

31^e Rapport d'activités 2023/24
Préposé fédéral à la protection
des données et à la transparence



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2023/2024

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

Le PFPDT remet annuellement un rapport sur son activité à l'Assemblée fédérale. Il transmet simultanément ce rapport au Conseil fédéral. Le rapport est publié (art. 57 LPD).

Le présent rapport couvre la période du 1^{er} avril 2023 au 31 mars 2024 pour le domaine de la protection des données. Pour le domaine du principe de la transparence il correspond à l'année civile du 1^{er} janvier au 31 décembre 2023.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra



Avant-propos

Depuis l'entrée en vigueur de la nouvelle loi sur la protection des données le 1^{er} septembre 2023, notre autorité a poursuivi la publication des guides et feuillets thématiques destinés au grand public, aux entreprises et aux autorités. Nos travaux visant à assurer le passage de l'ancien au nouveau droit seront bientôt clos de sorte que les postes supplémentaires approuvés par le Parlement pourront être assignés principalement aux enquêtes.

Malgré la portée pratique majeure des nouveautés techniques induites par la nouvelle législation, nous ne saurions perdre de vue les principes de base de la protection des données qui nous incitent à traiter les données en respectant les personnes concernées. J'ai donc décidé d'encourager cette compréhension fondamentale en répondant, dans la présente édition de notre rapport d'activités, à sept questions qui m'ont été posées à maintes reprises durant les deux premières législatures de mon mandat.

Adrian Lobsiger

Préposé fédéral à la protection des données et à la transparence



Berne, le 31 mars 2024

Défis actuels 6

Protection des données

1.1 Numérisation et droits fondamentaux 14

- Stratégie cloud de la Confédération : Projet CEBA de la Chancellerie fédérale
- Transformation numérique du système de santé : Identificateur de personnes
- Législation sur les épidémies : Utilisation du numéro AVS
- Identité électronique : Participation active du PFPDT à la finalisation du projet de loi sur l'e-ID
- Législation : Droit d'exécution de la loi sur la sécurité de l'information

Accent 20

La nouvelle loi sur la protection des données

1.2 Justice, police, sécurité 26

- Enquêtes contre fedpol, l'OFDF et Xplain : Accès à RIPOL et violation de la sécurité des données
- Piratage informatique : Enquêtes préliminaires concernant Concevis
- Banque de données de police : Le PFPDT demande que la numérisation de l'assistance administrative en matière de police ait lieu en conformité avec la protection des données

1.3 Économie et société 31

- Campagne en ligne « Pfarrer-Check » : Enquête sur l'association Forum Civique Suisse
- Formulaire d'inscription pour candidats locataires : Enquête préliminaire auprès d'une gérance immobilière
- Plateforme d'enchères Ricardo : Rapport final et recommandations
- Données clients : Enquête auprès de Digitec Galaxus
- Application de rencontre : Clôture de la procédure d'établissement des faits concernant Once Dating SA
- Technologies de traçage : Les inquiétudes suscitées par Oracle America ont été dissipées : les personnes résidant en Suisse ne sont pas concernées par les traitements de données en cause
- Transparence des personnes morales : Introduction d'un registre des ayants droit économiques
- Économie : Nouvelle loi sur l'examen des investissements étrangers

1.4 Santé 38

- Surveillance assurance-maladie : Échanges entre le PFPDT et l'OFSP
- Données de vaccination : Projet de sauvetage des données de mesvaccins.ch

- Pratique médicale : Signature d'une nouvelle déclaration de consentement par les patients
- Réutilisation des données : Rapports entre la loi sur la protection des données et la loi sur la recherche sur l'être humain
- Dossier électronique du patient : Révision complète de la Loi fédérale sur le dossier électronique du patient

1.5 Travail 44

- Droit du travail : Directives applicables à la gestion des dossiers personnels
- Droit du travail : Qualification des caisses de pension sous l'angle de la protection des données

1.6 Transports 46

- Projets divers : Conseils et consultations des offices dans le domaine de la mobilité
- Données PNR : Consultation des offices relative à la loi sur les données de passagers aériens

1.7 International 49

- Union européenne : Décision d'adéquation de l'UE
- Data Privacy Framework (DPF) : Cadre de l'échange de données vers les États-Unis
- Conseil de l'Europe : Ratification de la Convention 108+
- Europe : Réunion avec l'ICO et le CEPD
- European Case Handling Workshop : Rencontre internationale en Suisse
- Joint statement : Déclaration commune sur le moissonnage et sur la protection des données
- International : OCDE
- Schengen : BTLE et CEPD
- Schengen : Groupes de coordination du contrôle des systèmes d'information SIS II, VIS et Eurodac
- Schengen : Groupe de coordination Schengen des autorités suisses de protection des données
- Schengen : Activités relatives à Schengen au niveau national
- Rencontre internationale : Association francophone des autorités de protection des données personnelles
- Coopération internationale : Privacy Symposium de Venise
- Enjeux internationaux : Assemblée mondiale pour la protection de la vie privée
- Europe : Conférence européenne des commissaires à la protection des données à Budapest

Principe de la transparence

2.1	Généralités	62
2.2	Demandes d'accès – augmentation considérable en 2023	64
2.3	Procédures de médiation – Légère augmentation des demandes en médiation	68
	– Proportion des solutions amiables	
	– Durée des procédures de médiation	
	– Nombre de cas pendants	
2.4	Processus législatif	72
	– Finances : Transposition de l'ordonnance de nécessité du CS dans la loi sur les banques	
	– Archivage : Révision partielle de l'ordonnance sur l'archivage	
	– Criminalité financière : Nouvelle loi fédérale sur la transparence des personnes morales	
	– Réglementation des émoluments : La gratuité comme principe – Des émoluments en cas de charge de travail particulière	
	– Rapport de la CdG-E : Avis du Conseil fédéral	
2.5	Dispositions spéciales réservées au sens de l'art. 4 LTrans	78

Le PFPDT

3.1	Prestations et ressources	82
	– Prestations et ressources dans le domaine de la protection des données	
	– Prestations et ressources dans le domaine de la loi sur la transparence	
	– DPO et DSIO : Le PFPDT améliore son autocontrôle	
3.2	Communication	86
	– Nouveau site internet et portails de notification	
	– En chiffres	
	– Autres thèmes	
3.3	Statistiques	88
	– Statistiques des activités du PFPDT du 1 ^{er} avril 2023 au 31 mars 2024 (Protection des données)	
	– Vue d'ensemble des demandes d'accès selon la loi sur la transparence du 1 ^{er} janvier au 31 décembre 2023	
	– Statistique des demandes d'accès selon la loi sur la transparence du 1 ^{er} janvier au 31 décembre 2023	
	– Demandes d'accès 2023 liées au COVID-19	
	– Nombre de demandes en médiation	
	– Demandes d'accès de l'ensemble de l'administration fédérale du 1 ^{er} janvier au 31 décembre 2023	
3.4	Organisation du PFPDT	98
	– Organigramme	
	– Personnel du PFPDT	
	Liste des abréviations	100
	Table des illustrations	101
	Impressum	102
	Dans le pli	
	– Chiffres-clé	
	– Préoccupations relatives à la protection des données	

Défis actuels

I Protection des données

La dynamique de la numérisation a mené à une certaine focalisation du débat public sur des phénomènes technologiques, pour l'évaluation desquels les connaissances technologiques sont certes utiles, mais s'avèrent généralement insuffisantes sans une compréhension des principes de base de la protection des données. Dans ce contexte, il nous semble utile de répondre à sept questions de compréhension qui nous ont été fréquemment posées :

1) Quelles données la « protection des données » protège-t-elle ?

La protection des données protège la personnalité et les droits fondamentaux des personnes physiques en réglant le traitement des données personnelles et en protégeant les personnes concernées contre les traitements par lesquels l'État porte atteinte à leurs droits fondamentaux ou encore lorsque des entreprises privées empiètent sur leur sphère privée et l'autonomie de leur vie.

En ce sens, la protection des données ne vise pas directement la « protection » des données, puisque celles-ci ne peuvent être détentrices de droits. Elle ne protège pas non plus la propriété des données, ni les droits exclusifs sur les données, qui ressortent du droit des biens immatériels. De la même manière, les informations protégées par le secret

de fabrication ou d'affaires d'entreprises privées ou les secrets de l'État en matière militaire ou policière ne relèvent généralement pas de la protection des données, car l'intérêt lié au maintien du secret concerne typiquement le contenu matériel de l'information, par exemple une recette de bière ou une technologie en matière d'armement.

2) Qu'est-ce que la « personnalité » humaine et contre quoi est-elle protégée ?

La personnalité humaine, qui est au cœur de la protection des données, est ce que l'enfant désigne par MOI à peine a-t-il appris à dire son nom. Donner une définition juridique du JE humain demeure un grand défi. La Constitution fédérale, le code civil et la loi sur la protection des données disent certes que la personnalité est protégée par la loi, mais n'en donnent pas de définition. Il ressort toutefois de la doctrine juridique et de la jurisprudence que par « personnalité », l'on entend les particularités individuelles – le tréfonds de l'être humain qui le caractérise en tant que tel et qui le distingue de tous les autres.

3) Où commencent la sphère privée et l'intimité et jusqu'où s'étendent-elles ?

Le MOI humain se définit en référence au corps, au visage, à la voix, au comportement. En termes médicaux, ce MOI est abrité dans des organes internes tel le cerveau à partir duquel la zone centrale de la sphère privée et de l'intimité humaines s'étend à l'enveloppe corporelle extérieure et aux espaces personnellement habités par l'individu. Dans cette zone centrale, la protection des données empêche ou limite l'impact de moyens intrusifs de collecte de données tels que les détecteurs de mensonges ou les implants neuronaux. Mais les appareils disposant de caméras tels que les drones, les téléobjectifs et les capteurs qui épient le comportement des individus à l'intérieur de cette zone sont également soumis à une interdiction de principe.

Dans une vie quotidienne dominée par le numérique, les individus produisent ou laissent – comme consommateurs, passants, passagers ou patients – une multitude de traces électroniques qui permettent de recueillir des informations concrètes sur leur personne. Ainsi, leur sphère privée et intime ainsi que la protection des données s'étendent du corps à l'appartement en passant par le smartphone, et le « cloud », où les opérateurs privés des centres de données traitent une quantité incalculable de messages écrits et vocaux, d'images et de métadonnées de pages internet visitées, de conversations téléphoniques ou de dialogues en

« La personnalité humaine est au cœur de la protection des données. »

ligne. Dans cette zone élargie de la sphère privée et intime, la protection des données impose aussi des limites à leur traitement et à leur interconnexion.

4) Les adultes majeurs peuvent-ils renoncer à leurs droits en matière de protection des données ?

La protection de la sphère privée est un droit fondamental garanti par la Constitution (art. 13 Cst.). Lors de traitements de données personnelles effectués par l'État, un citoyen ne peut pas renoncer volontairement à ses droits en matière de protection des données. En effet, le but, l'étendue et l'intensité des traitements de données effectués par l'État sont régis par des bases légales contraignantes pour les organes publics qui, dans un cas concret d'application, ne peuvent être juridiquement libérées de cette obligation.

Par contre, un citoyen peut donner son consentement à des traitements de données effectués par des privés portant atteinte à sa personnalité. Mais cette renonciation n'est valable, en droit de la protection des données, que si cette personne a été informée au préalable de manière complète et compréhensible et que sa renonciation découle réellement de sa volonté libre. Ce sont les circonstances de vie qui déterminent si un consentement à se soumettre à un traitement concret peut

être considéré comme volontaire ou non. Prenons l'exemple de la capacité financière des utilisateurs d'offres numériques : pour des raisons économiques, ils ne peuvent pas tous se permettre de renoncer aux rabais importants que certains fournisseurs privés de biens et de services offrent en contrepartie de la divulgation d'informations personnelles dans le cadre de « programmes clients numériques ». De même, dans le cadre de dossiers de candidatures en vue d'un emploi, d'une location ou d'une assurance, une forte demande ne doit pas être la porte ouverte à des atteintes excessives à la vie privée des candidats, par exemple en priant ceux-ci de donner de manière faussement volontaire des informations sur leur sphère privée. Le consentement des personnes concernées peut alors s'avérer non valable du point de vue de la protection des données.

5) La protection des données est-elle une notion dépassée ? Sur les réseaux sociaux, de plus en plus de personnes dévoilent tout sur elles.

On compte par millions les personnes qui documentent chaque jour leur vie en postant des messages textuels, visuels ou vocaux, en les partageant sur internet avec leurs amis ou avec une clientèle payante. Parfois même, elles les rendent accessibles au grand public. Ces adultes qui prétendent s'exposer librement devant un large public sont pour la plupart soucieux de se présenter eux-mêmes et de présenter leur vie dans

un contexte qu'ils mettent personnellement en scène. Dans leur très grande majorité, ils sont offusqués et protestent avec énergie lorsque des données de leur sphère privée réelle sont collectées et diffusées.

Il existe donc bien un besoin croissant d'une protection des données qui requiert entre autres que les exploitants de réseaux sociaux respectent leurs conditions d'utilisation, ne traitent pas à des fins propres les données personnelles que les internautes ne partagent pas ou alors de manière sélective, et surtout ne les vendent pas à des tiers.

6) Existe-t-il des traitements de données interdits ?

Chargé d'établir les règles qui régissent les traitements de données personnelles effectués par les organes publics, le Parlement dans sa fonction législative s'engage au respect du droit fondamental protégeant la sphère privée et l'autodétermination en matière informationnelle – droit grâce auquel la Constitution fédérale garantit aux citoyens le respect de leur vie privée et de leur autonomie de vie. Il serait anti-constitutionnel que des lois introduisent des traitements de données étatiques

conduisant à une érosion des normes fondamentales telles que la liberté d'expression ou le droit de participation politique.

Malheureusement, les promoteurs de la transformation numérique des administrations n'en saisissent pas toujours très bien les enjeux constitutionnels et démocratiques. Lors de la surveillance de ces projets, les autorités de protection des données doivent en permanence veiller à ce que les mécanismes de freins des pouvoirs de l'État de droit démocratique – tels que la répartition du pouvoir administratif entre des services spécialisés, la séparation des pouvoirs ou le fédéralisme – ne soient pas éliminés les yeux fermés comme des concepts obsolètes, mais soient intégrés à temps à l'automatisation des données.

La situation est tout autre quant aux traitements de données personnelles effectués par des privés. Dans leur principe, ils sont autorisés en Suisse et le droit de la protection des données, défini par des principes de base, ne répond que de manière générale et abstraite à la question de savoir à partir de quand les atteintes à la personnalité des personnes concernées, provoqués par ces traitements privés, atteignent

un niveau que ne peuvent justifier ni un consentement ni des intérêts prépondérants.

Le droit de la protection des données fixe un seuil plutôt graduel de ce qui est admissible. En effet, il refuse de donner un caractère juridiquement contraignant aux consentements à la collecte de données personnelles lorsque, profitant de l'ignorance ou d'un rapport de dépendance, ils dépassent la mesure de ce que requiert le traitement.

Une limite absolue est atteinte lorsque, par son consentement, une personne aliène sa liberté ou s'en interdit l'usage dans une mesure contraire à l'ordre juridique dans son ensemble ou aux mœurs, ainsi que l'exprime le code civil.

7) Dans quelle mesure la protection des données est-elle politique ?

Du point de vue historique, la protection des données peut être considérée comme découlant du modèle étatique fondamental du libéralisme.

Dans les États de droit libéraux comme la Suisse, la protection des données et de la personnalité confère à l'individu un droit au respect de sa sphère privée et de son autonomie de vie qui va au-delà d'un simple droit à l'existence. D'une part, cette prémisse distingue la société libérale des modèles de gouvernement et de société totalitaires qui font de l'individu l'objet d'une domination fondée sur la collectivité. D'autre part, un modèle de société axé sur la revendication du vivant individuel par l'épanouissement personnel contraste avec les structures organisationnelles performantes d'autres espèces (comme celle des fourmis) ou avec une technique dénuée de vie (comme l'intelligence artificielle).

Un modèle de société étatique et économique qui ferait de l'humain le simple objet de desseins collectifs telle que l'atteinte d'une sécurité policière, économique et sanitaire absolue et peut-être aussi d'une durabilité écologique absolue par « l'automesure » permanente et la surveillance continue, aboutirait à une érosion totale de la liberté et marquerait la fin de la protection des données.

Indépendamment de cette déduction historique de la protection des données, les autorités de protection des données s'acquittent de leurs tâches légales dans un État de droit démocratique de manière apolitique.

« Ces adultes qui prétendent s'exposer librement devant un large public sont pour la plupart soucieux de se présenter dans un contexte mis en scène par eux-mêmes. »

II Principe de la transparence

Durée de traitement des demandes d'accès et des procédures de médiation

Le principe de transparence suscitant un intérêt croissant, le nombre de demandes d'accès à des documents administratifs ne cesse d'augmenter. Dans certains cas, cette affluence de demandes se répercute négativement sur leur durée de traitement – de sorte que le temps d'attente pour obtenir l'accès souhaité se prolonge. Bien que la LTrans contienne des dispositions légales claires à propos des différentes étapes de la procédure, la pratique montre que les services administratifs ne parviennent pas toujours à respecter les délais.

Il en va de même des procédures de médiation : durant l'année sous revue, le PFPDT n'a pu respecter la durée légale de traitement de 30 jours que dans un peu plus de 25 % des procédures (cf. ch. 2.3). Souvent, ce sont les demandes volumineuses, nécessitant un échange de courriels sur une longue période, et les questions juridiques complexes qui entraînent un allongement des procédures. Ainsi les ques-

tions de délimitation concernant l'application de la loi sur la transparence requièrent parfois des clarifications détaillées en amont d'une appréciation de la question sur le fond.

De même, lorsqu'un représentant légal est impliqué dans la procédure de médiation (tant du côté des demandeurs ou des tiers que de l'administration), la procédure est plus longue dans la majorité des cas. Étant donné l'intérêt croissant des demandes d'accès aux informations de l'administration, donc l'augmentation de leur nombre, la durée des procédures de médiation devrait donc rester une préoccupation.

Augmentation du nombre des exceptions à la LTrans en vertu de lois spéciales

Au cours de l'exercice sous revue, l'administration s'est de nouveau employée à soustraire du principe de transparence certains domaines de son activité ou certaines catégories de documents. Dans le cadre des consultations menées par les offices concernés, le PFPDT s'est exprimé à ce sujet de manière critique ; en effet, introduire de telles réserves contribue à affaiblir le principe de transparence ainsi que la transparence administrative visée par celui-ci. Chaque cas concret doit être examiné à la lumière des normes concernées ; cet examen permet ensuite de déterminer si une disposition légale prime en tant que disposition spéciale au sens de l'art. 4 LTrans.

Face à l'augmentation du nombre des exceptions à la LTrans en vertu de lois spéciales, le PFPDT en publie un état récapitulatif, comme dans son précédent rapport d'activités (cf. ch. 2.5) ; ce tableau peut également être consulté sur le site internet du PFPDT.

III Coopération nationale et internationale

International

À la mi-janvier 2024, la Commission européenne a confirmé que le niveau de protection des données garanti par la Suisse était adéquat. Une décision attendue depuis longtemps. Le transfert vers la Suisse de données personnelles provenant d'États membres de l'Union européenne (UE) ou de l'Espace économique européen (EEE) peut donc se poursuivre sans garanties supplémentaires. Cette décision revêt une importance économique considérable pour les entreprises de tous les États concernés.

Au cours du dernier exercice, les spécialistes du PFPDT ont, comme chaque année, participé à des groupes de travail pertinents au niveau international et profité de ces occasions pour entretenir des échanges personnels avec leurs partenaires étrangers. Le PFPDT

a en outre organisé début novembre à Berne le European Case Handling Workshop (ECHW), qui rassemble chaque année 80 professionnels représentant 37 autorités de protection des données en vue de partager leur savoir-faire.

Le PFPDT a par ailleurs participé aux réunions régulières des organes de protection des données du Conseil de l'Europe (comité consultatif de la convention 108) et de l'Organisation de coopération et de développement économiques (Groupe de travail sur la

gouvernance des données et la protection de la vie privée dans l'économie numérique), aux conférences européenne et internationale sur la protection des données, et à la conférence de l'Association francophone des autorités de protection des données personnelles. Il était aussi présent au Privacy Symposium, conférence internationale privée, qui a consacré une journée à la convention 108 modernisée du Conseil de l'Europe. Les échanges directs entre autorités de protection des données sont d'autant plus importants que les flux transfrontières de données à caractère personnel continuent de soulever des questions juridiques délicates à l'échelle internationale. Plusieurs de ces autorités ont d'ailleurs conclu des mémorandums d'accord juridiquement non contraignants dans l'intention d'intensifier leur coopération.

Collaboration avec les cantons

Les autorités de protection des données de la Confédération et des cantons ont intensifié leur collaboration dans le but de garantir une surveillance efficace et intégrale (cf. 30^e RA, ch. III). Ainsi, au cours de l'année sous revue, le PFPDT s'est entretenu avec les autorités cantonales partenaires à propos de l'externalisation de données personnelles vers des centres de calcul exploités par

la société privée Microsoft, projet soutenu par les administrations fédérales et cantonales.

La délimitation des compétences en matière de protection des données, notamment la question de savoir quand la législation fédérale et quand les législations cantonales sont appliquées, a été aussi abordée. Certains cas de figure ont nécessité une analyse juridique plus approfondie : lorsque des organes publics cantonaux ou communaux font appel au secteur privé pour traiter des données, lorsque des organismes privés ou publics agissent à la fois en vertu du droit privé et à titre souverain, ou lorsque le droit cantonal désigne la loi fédérale sur la protection des données en tant que droit applicable.

Protection des données

1.1 Numérisation et droits fondamentaux

STRATÉGIE CLOUD DE LA CONFÉDÉRATION

Projet CEBA de la Chancellerie fédérale

Comme durant l'exercice précédent, le PFPDT a été étroitement associé aux projets d'informatique en nuage de l'administration fédérale. Outre diverses consultations des offices, le projet TNI « Cloud Enabling Büro-automation » (Bureautique permettant l'accès au nuage), en abrégé CEBA, a occupé une position centrale dans ce contexte.

En 2022, le projet CEBA a été classé comme projet informatique-clé de la Confédération en raison de son impact considérable sur le fonctionnement de la majeure partie de l'administration fédérale. Le secteur Transformation numérique et gouvernance de l'informatique (secteur TNI) de la Chancellerie fédérale a associé le PFPDT à l'introduction du logiciel en mode cloud du groupe américain Microsoft (Microsoft 365). Au mois d'avril 2023, le Préposé fédéral a pris position sur la directive d'application de Microsoft 365, qui lui avait été soumise, ainsi que sur le projet d'analyse d'impact relative à la protection des données (AIPD), rédigé à sa demande. Une fois encore, il a demandé que tous les risques figurent de manière transparente dans l'AIPD, y compris ceux qui, en raison de la dépendance concrète vis-à-vis du fournisseur, ne

pourraient se révéler qu'à une date ultérieure au cours de l'intégration progressive aux services en nuage.

Par ailleurs, le PFPDT estime que l'évaluation de solutions de remplacement à Microsoft 365 Cloud constitue un aspect important du projet CEBA. Il a analysé en détail les activités du secteur TNI en la matière et a exprimé, auprès de l'équipe de projet, son souhait d'une approche large, ouverte et dénuée de subjectivité. Il est primordial que les responsables des offices puissent choisir entre différentes solutions en ayant une connaissance complète des faits (cf. notre brève du 7.3.2023, ainsi que le communiqué de presse du Conseil fédéral du 15.2.2023).

Examen par le CDF

Classé comme projet-clé TNI, le projet CEBA a été soumis à un audit du Contrôle fédéral des finances (CDF), dans le cadre duquel le PFPDT a également été consulté. Cet audit avait pour but d'évaluer si l'organisation du projet était en adéquation avec ses objectifs et si les dispositifs de pilotage et de gouvernance



nécessaires avaient été mis en œuvre et étaient opérationnels. Le CDF a estimé que le projet n'avait pas suffisamment pris en compte les remarques émises par le PFPDT lors de l'audit et il a recommandé au secteur TNI de mieux harmoniser sa démarche avec ce dernier quant à la protection des données et à la sécurité de l'information.

Principes relatifs à l'informatique en nuage

Dans le contexte de la stratégie d'informatique en nuage de la Confédération et au cours d'une consultation des offices, le secteur TNI a soumis au PFPDT – après remaniement profond – les « Principes relatifs à l'informatique en nuage ». Outre leur aspect stratégique, ils constituent des jalons supplémentaires sur la voie de la mise en œuvre de la stratégie d'informatique en nuage. Le PFPDT a porté un regard critique sur certaines modifications effectuées par rapport à la version précédente ; il estime qu'elles ont pour effet de réduire le caractère contraignant de ces principes et de les transformer de normes minimales en informations et recommandations.

Toujours dans le contexte de la mise en œuvre de la stratégie d'informatique en nuage, le PFPDT s'est exprimé au sujet de la note de discussion et de l'arrêté fédéral de l'Office fédéral de l'informatique et de la télécommunication (OFIT), dans le cadre d'une consultation des offices relative au projet Swiss

Government Cloud (SGC). Dans ces documents, l'OFIT propose au Conseil fédéral de remplacer l'actuelle solution de nuage privé Atlantica par une infrastructure hybride multicloud à trois niveaux : le niveau I inclurait les nuages publics fournis par l'OFIT via des fournisseurs de nuages publics ; le niveau II les solutions de grands fournisseurs de nuages publics installées dans les locaux de la Confédération ; et le niveau III le nuage privé de l'OFIT, intégralement hébergé au sein du réseau de centres de calcul de la Confédération. L'OFIT a adopté nos propositions de modification et apporté des précisions sur des points importants relatifs à la protection des données.

Le PFPDT souligne l'importance d'intégrer la question de la protection des données à un stade très précoce des projets lorsque des traitements de données sont prévues. Dans le cadre de ses compétences, il continuera à accompagner de ses conseils les initiatives d'informatique en nuage et à vérifier la mise en œuvre des normes et critères requis.



Identificateur de personnes

Dans le cadre du programme DigiSanté visant à promouvoir la transformation numérique du système de santé, le PFPDT s'est prononcé sur les travaux menés au sein du « Groupe gestion des données dans le système de santé » visant à faciliter la réutilisation de données par les chercheurs. Il a en particulier rappelé les aspects de protection des données

Le Département fédéral de l'intérieur (DFI) a lancé le programme DigiSanté qui vise à promouvoir la transformation numérique du système de santé. De nombreux projets touchent à l'utilisation des données de santé. Dans le volet portant sur l'utilisation des données pour la planification, le pilotage et la recherche, le Conseil fédéral a chargé le DFI de mettre sur pied un groupe spécialisé Gestion des données dans le système de santé (GGDS). Le Conseil fédéral a également thématiqué la création des conditions nécessaires à une utilisation multiple des données de santé par les institutions de recherche, notamment en ce qui concerne la forme du consentement des personnes concernées à l'utilisation de leurs données ou la préservation de la protection et de la sécurité des données grâce à un concept étendu de protection des données.

Dans le cadre des travaux sur l'identificateur de personnes, le PFPDT a rappelé les discussions menées lors de l'élaboration des dispositions concernant l'utilisation systématique du numéro AVS en dehors du domaine des assurances sociales ayant été concrétisées par l'introduction de dispositions sur les analyses de risques périodiques (art. 153e Loi fédérale sur l'assurance-vieillesse et survivants, LAVS) et la mise en place de mesures techniques et organisationnelles spécifiques (art. 153d LAVS).

Le PFPDT a également rappelé dans le cadre des réflexions de ce groupe de travail que la création d'un identificateur unique doit certes être envisagé sous l'angle de sa faisabilité et de ses aspects techniques, mais qu'il doit également faire l'objet d'un concept de protection des données dès la conception et par défaut au sens de l'art. 7 LPD et d'une analyse d'impact relative à la protection des données personnelles au sens de l'art. 22 LPD en cas de nouveaux projets ou développements envisagés.

Utilisation du numéro AVS

La loi sur les épidémies et les ordonnances d'application sont en cours de révision. Du point de vue de la protection des données, l'une des principales nouveautés est l'introduction du numéro AVS du patient parmi les données devant être communiquées avec l'annonce d'un cas.

Durant l'année sous revue, le PFPDT a dû se prononcer sur un projet de révision des ordonnances d'exécution de la loi sur les épidémies (LEp). Pour rappel, cette législation prévoit une obligation pour les médecins, laboratoires et autres institutions sanitaires d'annoncer aux cantons et à l'Office fédéral de la santé publique (OFSP) le diagnostic de certaines maladies, afin d'éviter ou de lutter plus efficacement contre les épidémies. Du point de vue de la protection des données, l'une des principales nouveautés amenées par ces révisions est l'introduction du numéro AVS du patient parmi les données qui doivent être envoyées lors d'une annonce. Selon l'OFSP, l'utilisation de ce numéro permet de faciliter le traitement des annonces par l'usage d'un numéro spécifique à chaque individu et aussi d'éviter d'éventuels doublons.

L'usage du numéro AVS est certainement un moyen permettant d'atteindre les buts visés par l'OFSP. En soi, il s'agit cependant d'une donnée relativement délicate, dans la mesure où ce numéro est utilisé pour passablement d'activités. Si ce numéro venait à être

IDENTITÉ ÉLECTRONIQUE

compromis, cela pourrait avoir des conséquences assez importantes pour la personne concernée. Pour cette raison, la loi sur l'AVS (LAVS) prévoit que l'utilisation de ce numéro en dehors du domaine de l'AVS est soumise à des mesures de sécurité renforcées (art. 153d LAVS). En outre, les institutions qui y recourent doivent procéder à des analyses de risque régulières (art. 153e LAVS) – indépendamment de l'analyse de risque à réaliser selon l'art. 22 LPD. Dans ses prises de position, le PFPDT a notamment souligné ces points.

À noter enfin que la LEp est aussi en cours de révision. Le PFPDT a également pris position sur ce projet. L'usage du numéro AVS dans la procédure d'annonce n'y était cependant pas encore prévu ; il n'a été introduit qu'ultérieurement, dans le projet de révision des ordonnances qui a suivi. De l'avis du PFPDT ainsi que d'autres Offices, il serait néanmoins préférable que cet usage soit ancré dans la loi formelle. L'OFSP a ainsi procédé à cette adaptation.

Participation active du PFPDT à la finalisation du projet de loi sur l'e-ID

Le PFPDT a accompagné, sur le plan de la surveillance, les travaux relatifs au nouveau projet de loi sur l'identité électronique, qui prévoit une solution étatique et suit l'approche de l'identité souveraine.

Suite au rejet du premier projet de loi sur l'identité électronique en 2021, le Département fédéral de justice et police (DFJP) a élaboré un nouveau projet de loi et l'a envoyé en consultation. Le PFPDT a fait part de ses préoccupations (cf. RA 29 et 30, ch. 1.1). La publication du projet de loi et de son message a eu lieu le 22 novembre 2023. Ce projet de loi règle d'une part l'identité électronique (l'e-ID) établie par l'État et d'autre part l'exploitation d'une infrastructure technique permettant d'émettre et de vérifier toutes sortes de preuves électroniques. Cette dernière pourra être utilisée par les autorités cantonales ou communales ainsi que par les acteurs du secteur



privé souhaitant établir et /ou utiliser des documents tels que des diplômes, des billets de concert ou des extraits de poursuite. L'e-ID sera émise par fedpol, sur demande de son titulaire. Pour le stockage et la gestion des preuves électroniques dont ils sont titulaires, les citoyens pourront utiliser une application fournie par la Confédération qui fonctionnera comme un portefeuille électronique. Avec cette application, le titulaire pourra contrôler la transmission de ses données, stockées localement sur son smartphone. Il aura

ainsi la maîtrise de ses données (identité souveraine), qui seront enregistrées de manière décentralisée, et il pourra limiter les flux de données à celles nécessaires (principe de la minimisation des données). Le système devra être conçu selon le principe de protection des données dès la conception et par défaut, c'est à dire que la protection des données sera assurée par le système lui-même.

Dans le cadre de la révision de la loi, le PFPDT avait fait part de son inquiétude que la création de l'e-ID n'engendre des prélèvements excessifs de données personnelles dans le monde numérique. Ainsi, il a salué l'introduction d'un devoir de diligence des vérificateurs afin d'empêcher la « sur-identification » et des mesures en cas de violation de ce devoir. Il a toutefois insisté afin que le message contienne des exemples concrets d'applications pour délimiter les demandes de données légitimes et les demandes de données excessives. Ainsi, le message adapté contient les scénarios concrets dans lesquels les organes de contrôle peuvent demander des données personnelles à partir de l'e-ID : Une demande de l'ensemble des données de l'e-ID d'un client pour vérifier son âge lors d'un simple achat en ligne serait considérée comme excessive et donc abusive étant donné que pour confirmer la majorité d'une personne, il n'est pas nécessaire



d'obtenir son identité ou sa date de naissance, mais seulement l'information selon laquelle cette personne a plus de 18 ans.

Pour lutter contre les cas d'abus, le PFPDT a recommandé de prévoir dans la loi la publication des cas d'utilisation abusive de l'infrastructure de confiance ou des soupçons fondés à ce sujet. Il a donc salué l'ajout d'un registre de confiance intégré à l'infrastructure dans le but de garantir la fiabilité des organes émetteurs et vérificateurs. Il a également exigé que certaines obligations de révocation s'appliquent à tous les émetteurs de preuves électroniques (et non seulement à fedpol, qui émet l'e-ID), dans le sens de leurs obligations de garantir l'exactitude des données. Le message a été modifié à cet effet de manière à ce que l'obligation de supprimer les données inexactes figurant sur les preuves électroniques découle directement de la LPD.

Le PFPDT en a profité pour soulever la problématique de l'utilisation des données marginales générées lors de la consultation du registre de base, qui ne devraient selon lui pouvoir être exploitées que dans le but d'assurer le maintien de la sécurité de l'information, la maintenance technique de l'infrastructure électronique ou pour tracer l'accès au registre. Il a par ailleurs insisté sur l'importance de réglementer le traitement de ces données marginales. Cette demande de réglementation a été adoptée.

LEGISLATION

Le PFPDT est en définitive satisfait de son implication dès le début dans l'accompagnement de ce projet sur le plan de la surveillance et de l'intégration de nombre de ses demandes au projet final de loi et à son message. Il regrette toutefois que le message n'informe pas des résultats de l'examen ou de l'analyse d'impact en matière de protection de données, comme le prévoit la lettre 4.1 des Directives du Conseil fédéral concernant l'examen préalable des risques et l'analyse d'impact relative à la protection des données personnelles en cas de traitement de données personnelles par l'administration fédérale du 28 juin 2023, qui concrétisent les obligations des organes fédéraux conformément à l'art. 22 LPD.

Sur demande des Commissions des affaires juridiques des deux conseils, le PFPDT a participé à leurs délibérations sur le projet entre janvier et avril 2024. En cas d'approbation par le Parlement, le PFPDT continuera à suivre la mise en œuvre de l'e-ID et de l'infrastructure de confiance et à apporter sa contribution, par exemple lors des consultations des offices relatives aux ordonnances du Conseil fédéral, afin de garantir la protection des données dès la conception et par défaut.

Droit d'exécution de la loi sur la sécurité de l'information

Les ordonnances d'application de la loi sur la sécurité de l'information sont entrées en vigueur le 1^{er} janvier 2024. Le DDPS a tenu compte d'une grande partie des remarques formulées par le PFPDT lors des différentes consultations. À la fin 2020, le Parlement a adopté la loi sur la sécurité de l'information (LSI). Dans le cadre de l'exécution de cette loi, plusieurs ordonnances ont été modifiées : l'ordonnance sur la sécurité de l'information, l'ordonnance sur les contrôles de sécurité relatifs aux personnes, l'ordonnance sur la procédure de sécurité relative aux entreprises et l'ordonnance sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération.

Lors des différentes consultations des offices, le PFPDT a formulé plusieurs remarques et questions. Dans le domaine des contrôles de sécurité relatifs aux personnes, il a constaté que la base légale au sens formel dans la LSI ne couvrait pas la totalité des données sensibles traitées prévues par l'ordonnance. Cette base légale sera complétée lors de la prochaine révision de la loi. Le Préposé a également demandé des précisions dans l'ordonnance sur la sécurité de l'information. Les autorités administratives en charge de la sécurité de l'exploitation doivent surveiller l'utilisation de leur infrastructure informatique et l'examiner régulièrement à la recherche de menaces et de vulnérabilités techniques. Le PFPDT a proposé de compléter la disposition en indiquant que la surveillance de l'utilisation de l'infrastructure informatique doit être effectué avec des moyens techniques et organisationnels appropriés et que l'examen régulier se fasse de manière automatisée.

Le DDPS a refusé la demande du PFPDT qui a fait l'objet d'une divergence lors de la dernière consultation des offices. Le Conseil fédéral n'a également pas tenu compte de sa position et les ordonnances d'exécution de la LSI sont entrées en vigueur le 1^{er} janvier 2024.

La nouvelle loi sur la protection des données

Entrée en vigueur de la nouvelle LPD

La nouvelle loi sur la protection des données et ses ordonnances sont entrées en vigueur le 1^{er} septembre 2023. Le PFPDT a organisé de nombreuses séances d'information, rédigé guides et feuillets thématiques et mis à jour les contenus de son site internet.

À la veille de l'entrée en vigueur de la nouvelle loi sur la protection des données, le PFPDT a particulièrement mis l'accent sur la sensibilisation de la population et sur l'information des professionnels du secteur privé et de l'administration fédérale.

Séances d'information

Durant l'année sous revue, le PFPDT a présenté la nouvelle loi au cours de diverses séances d'information organisées sur invitation par des offices fédéraux et des départements. En août, il a tenu à l'Université de Fribourg une journée d'information destinée à tous les conseillers à la protection des données des organes fédéraux. Plus de 80 participants issus de nombreuses unités administratives ont discuté de sujets pratiques tels que l'analyse d'impact relative à la protection des données, la journalisation des traitements automatisés ou les nouvelles règles de procédure.

Le PFPDT a aussi participé à de nombreuses rencontres avec les milieux économiques privés et répondu à des questions pratiques sur le passage de l'ancienne à la nouvelle LPD. Il a porté une attention particulière aux échanges avec les conseillers à la protection des données d'entreprises et, à cet égard, a pris en considération les différentes régions linguistiques. En Suisse alémanique, outre les contacts réguliers avec le Verein Unternehmens-Datenschutz, il a participé à la réunion d'automne de l'association Data Privacy Community ainsi qu'à plusieurs événements et manifestations universitaires. À Lausanne, le PFPDT a donné une conférence devant l'Association Suisse des Délégués à la Protection des Données (ASDPO) et participé à la masterclass organisée

pour les futurs délégués à la protection des données. Sur invitation de l'autorité chargée de la protection des données de la Principauté de Liechtenstein, il a présenté le nouveau droit suisse aux responsables de la protection des données de diverses entreprises de la Principauté. Enfin, sur invitation de la Fédération des Entreprises Romandes, il a abordé directement avec des entrepreneurs diverses questions pratiques relevant de la protection des données à Genève, dans le Jura et en Valais.

Par ailleurs, grâce à sa hotline ou par courriel, le PFPDT a pu répondre directement à des questions concrètes sur la nouvelle loi sur la protection des données. Par rapport aux mois précédents, le doublement du nombre des questions posées par téléphone durant les mois d'août et de septembre a témoigné du vif intérêt suscité par le nouveau droit.

Site internet du PFPDT

Au cours de l'année sous revue, le PFPDT a profondément remanié son site internet afin de pouvoir répondre aux besoins croissants d'informations écrites dans la perspective des nouvelles dispositions sur la protection des données.

Il a adapté à la nouvelle loi les textes pertinents et apporté des explications à toutes les nouveautés législatives. Il a consigné et commenté sur une page les plus importantes de ces nouveautés, dont le droit d'accès, le devoir d'informer, les dispositions pénales, les règles concernant les émoluments ou encore les certifications en matière de protection des données. Il a en outre publié une page consacrée aux questions fréquentes (FAQ), page appelée à être régulièrement complétée.

Guides et feuillets thématiques

Sur son site internet, le PFPDT met aussi à disposition des outils pratiques concernant la LPD.

Portails en ligne pour la transmission numérique et sécurisée des notifications au PFPDT

Avant l'introduction de la nouvelle loi sur la protection des données, le PFPDT a publié, sur son nouveau site internet, des portails permettant aux responsables de traitement de remplir de manière numérique et sécurisée leurs obligations de notification.

Registre des activités de traitement (portail DataReg)

Les organes fédéraux déclarent leurs activités de traitement au PFPDT en utilisant l'application DataReg. Ce nouveau portail d'annonce remplace l'ancien système de déclaration et ne contient plus d'annonces de fichiers du secteur privé, comme l'exigeait l'ancienne loi sur la protection des données. Outre la migration des entrées des organes fédéraux, il existe désormais un grand nombre de nouvelles entrées de responsables et de registres, dont notamment les entrées des caisses de pension et des fondations collectives qui sont qualifiées d'organes fédéraux et représentent une grande partie des trois mille entrées enregistrées jusqu'ici dans le portail d'annonce. Le DataReg est accessible au public. (www.datareg.edoeb.admin.ch)

Notification des violations de la sécurité des données (portail DataBreach)

En cas de violation de la sécurité des données (data breach) susceptible de présenter un risque élevé pour les personnes concernées, les responsables disposent désormais d'un portail dédié leur permettant de notifier cette violation au PFPDT. Le formulaire de notification recouvre toutes les informations nécessaires.

Depuis l'introduction de ce portail, le PFPDT reçoit une grande majorité de ces notifications sous forme électronique. Leurs auteurs couvrent un large éventail de branches, allant des hôtels aux fondations collectives. Le PFPDT s'est particulièrement intéressé aux cas impliquant des sous-traitants

(p. ex. les entreprises d'hébergement), car sur ce point, un grand nombre de notifications était attendu et le PFPDT souhaite coordonner son action dans toute la mesure du possible.

(www.databreach.edoeb.admin.ch)

Données de contact des conseillers à la protection des données (portail DPO)

Les entreprises privées peuvent nommer une conseillère ou un conseiller à la protection des données (data protection officer, DPO) et communiquer cette nomination au PFPDT si elles veulent bénéficier des facilités prévues en matière d'analyse d'impact relative à la protection des données.

En revanche, les organes fédéraux sont tenus de nommer un conseiller à la protection des données et, conformément à l'art. 27, al. 2, OPD, de publier ses coordonnées en ligne et de les communiquer au PFPDT. Le portail DPO leur offre la possibilité de communiquer au PFPDT par voie électronique les coordonnées de leur conseiller à la protection des données.

À ce jour, plus de deux mille responsables de traitement ont saisi un ou plusieurs conseillers à la protection des données sur le portail DPO.

(www.dpo-reg.edoeb.admin.ch)

Portail DataBreach

Total de 245 notifications depuis l'introduction du formulaire en ligne le 9 mai 2023.

Pour 57 d'entre elles, il a été fait usage de la possibilité de fournir des informations supplémentaires par le biais d'une notification de suivi, que ce soit à l'initiative du responsable du traitement ou à la demande du PFPDT.

Il est à noter le nombre de notifications où la violation de la sécurité des données s'est produite en rapport avec un sous-traitant (Xplain, Concevis, Booking.com...). Dans ces cas, il convient toujours de constater qu'un très grand nombre de personnes concernées ont été exposées à un risque élevé en raison de la violation constatée.

Nouvelle ordonnance sur les certifications en matière de protection des données

La nouvelle ordonnance sur les certifications en matière de protection des données (OCPD) est entrée en vigueur le 1^{er} septembre 2023, en parallèle à la nouvelle loi sur la protection des données. Ces deux entrées en vigueur ont été l'occasion de réviser les directives sur les exigences minimales qu'un système de gestion doit remplir et d'établir des directives sur les autres critères en matière de protection pour l'évaluation des exigences relatives à la certification des produits, des services et des processus

En collaboration avec l'Office fédéral de la justice (OFJ) et le Service d'accréditation suisse (SAS), le PFPDT a examiné l'adaptation de l'ordonnance sur les certifications en matière de protection des données (OCPD) à la nouvelle loi sur la protection des données (LPD). En effet, les services eux aussi peuvent être désormais certifiés, en plus des systèmes de gestion (à savoir l'organisation et les procédures) et des produits.

Bien que n'étant pas explicitement prévue, la possibilité de certifier des traitements de données personnelles est dorénavant prise en compte, notamment dans le cadre de la certification des produits ou des services, ce qui permet

de rapprocher le système de certification suisse du droit européen. De ce fait, les certifications suisses portant sur le traitement de données personnelles devraient pouvoir être reconnues par les autorités européennes de protection des données.

Toutes les certifications bénéficient désormais de la même durée de validité, à savoir trois ans, assortie d'un contrôle annuel obligatoire.

La nouvelle LPD introduit une exception à l'obligation de procéder à une analyse d'impact relative à la protection des données au bénéfice des responsables privés de traitements lorsque leurs traitements de données sont dûment certifiés. Cette nouvelle règle remplace la dispense du devoir de déclaration des fichiers qui existait dans la législation précédente. Les dispositions sur ce point ont été adaptées en conséquence dans l'OCPD.

Toutes les informations relatives aux certifications en matière de protection des données sont disponibles sur le site internet du PFPDT.

De nouveaux modèles pour les règlements de traitement

Certains traitements de données nécessitent un règlement de traitement. Ce règlement a pour but de fournir une vue d'ensemble des traitements de données, ce qui peut s'avérer essentiel notamment pour remédier aux violations de la sécurité des données (data breaches). Des modèles de règlement sont disponibles sur le site internet du PFPDT.

La nouvelle ordonnance sur la protection des données (OPD) est entrée en vigueur le 1^{er} septembre 2023, en parallèle à la nouvelle loi sur la protection des données (LPD). Comme dans l'ancien droit, certains traitements de données nécessitent un règlement de traitement. Les conditions en sont définies aux art. 5 OLP (pour les personnes privées) et 6 OLP (pour les organes fédéraux).

Désireux d'aider les responsables de traitements à établir leur règlement de traitement, le PFPDT a mis des modèles à leur disposition. Il existe deux modèles différents : l'un pour les organes fédéraux, l'autre pour les personnes privées. Chacun de ces modèles fournit une liste des contenus requis et une table des matières type.

Par exemple, le règlement de traitement fixe les flux d'informations : ceux-ci doivent indiquer quelles informations sont échangées par l'organe exploitant le système avec d'autres organes, quand, comment et de quelle manière. Ainsi, en cas de violation de la sécurité des données (data breach), un règlement de traitement soigneusement élaboré et régulièrement actualisé revêt une importance centrale car il permet d'obtenir rapidement une vue d'ensemble des données et des systèmes concernés. Il est également possible d'en déduire les premières mesures propres à réduire les risques.

Journalisation

La journalisation est l'une des mesures techniques et organisationnelles visant à assurer la sécurité des données.

Réglé à l'art. 4 OPDo, le processus décrit comme standard continue pourtant à soulever des questions.

Durant l'année sous revue, le PFPDT a régulièrement répondu à des demandes relatives à la journalisation. Le concept existait déjà sous l'ancien droit (art. 10 OLPD) et n'a fondamentalement pas changé : son but est de permettre de retracer l'historique de l'utilisation des données. Cela participe à la sécurité des données, non seulement en inscrivant les traitements de données dans un cadre (celui qui manipule des données sait qu'il laisse une trace), mais aussi en permettant de mieux comprendre ce qu'il s'est passé en cas d'incident. Le nouvel article 4 de l'ordonnance est cependant plus complet. Il rend également la journalisation obligatoire pour les organes fédéraux, qui disposent d'un délai de trois ans pour se mettre à jour (art. 46 al. 1 OPDo) ; jusqu'alors, et comme c'est toujours le cas pour les privés, la mesure n'était obligatoire qu'en présence de traitements caractérisés (en substance traitement de données sensibles et le profilage) et lorsque d'autres mesures préventives s'avéraient insuffisantes pour garantir la protection des données.

La thématique continue toutefois à poser un certain nombre de questions ou de difficultés pratiques, sur lesquelles le PFPDT a été amené à se pencher (notamment définition du « traitement automatisé » ; détournement de la journalisation, p. ex. à des fins de surveillance ; nécessité de générer des fichiers de journalisation effectivement exploitables ; vieilles applications sans fonction de journalisation ; problématique des ressources informatiques nécessaires à la journalisation limitant la puissance de calcul disponible lors d'analyses sur un nombre important de données ; nouvelles technologies tels les développements de l'IA).

Nouveau guide relatif aux mesures techniques et organisationnelles (TOM)

[Avec l'entrée en vigueur de la nouvelle loi sur la protection des données, le PFPDT a mis à jour le guide relatif aux mesures techniques et organisationnelles de la protection des données au niveau juridique et technique.](#)

L'objectif de ce guide est de permettre aux responsables de traitement de données personnelles d'avoir une vue d'ensemble de ce que la loi leur demande, ainsi que de leur fournir une explication compréhensible des différents éléments et des outils ou des références pour les aider à mettre en place les mesures nécessaires. Pour ce faire, il était nécessaire de reprendre l'entier du contenu, en prenant en compte des changements importants dans la nouvelle loi sur la protection des données (LPD) et de l'évolution de l'état actuel (state-of-the-art) de la technique et des normes.

L'ouvrage détaille notamment les nouvelles définitions des termes tels qu'utilisés dans la LPD comme par exemple l'importance des concepts de « risque élevé » et de « profilage » ou encore l'existence des nouveaux outils que sont le code de conduite et la certification. Il met l'accent sur les outils importants de la nouvelle loi que sont l'analyse d'impact sur la protection des données (AIPD) et le rôle du conseiller

à la protection des données dessus. Il détaille également le registre des activités de traitement et finalement que faire en cas de violation de la sécurité des données personnelles. Le guide tient également compte des besoins spécifiques lors du traitement de données par les organes fédéraux, qui ont des spécificités propres.

Les principaux thèmes de la protection des données sont présentés sous l'angle des mesures techniques et organisationnelles envisageables, comme la protection dès la conception et par défaut, ainsi que l'anonymisation, la pseudonymisation mais aussi les mesures concernant l'infrastructure de travail, avec des conseils sur la sécurité des locaux et des salles de serveurs, ainsi que sur l'usage du cloud dans les traitements de données personnelles. La politique de gestion des accès, les mesures d'identification et d'authentification et les accès à distance (home office) sont également expliqués tout comme le cycle de vie des données, avec des mesures sur la saisie, la sauvegarde et la destruction des données, mais aussi leur chiffrement et leur journalisation quand nécessaire.

Le guide sur les mesures techniques et organisationnelles est avant tout destiné aux personnes qui sont en charge des systèmes d'information, techniciens ou non, et qui sont confrontés directement au problème de la gestion des données personnelles. Il est disponible dans les trois langues nationales ainsi qu'en anglais sur le site du PFPDT.

Analyse d'impact relative à la protection des données

Les responsables des traitements de données, qu'ils soient privés ou publics, doivent effectuer une analyse d'impact relative à la protection des données (AIPD) lorsqu'un traitement de données personnelles est susceptible d'entraîner un risque potentiellement élevé pour la personnalité ou les droits fondamentaux des personnes concernées.

L'aide-mémoire du PFPDT sur l'AIPD s'adresse en particulier aux responsables privés de traitements de données. Il donne une définition du risque élevé, une description de l'examen préalable du risque et précise le contenu et la structure d'une AIPD. La procédure à suivre une fois l'AIPD établie et les mesures incombant au PFPDT y sont également présentées. Le PFPDT examine les AIPD qui lui sont soumises et communique son avis au responsable du traitement. Cet avis a valeur de recommandation et ne constitue ni une approbation, ni une autorisation du traitement prévu. Le PFPDT peut toutefois ouvrir une enquête sur la base de sa mission de surveillance et ordonner à l'intention du responsable les mesures requises.

De son côté, l'Office fédéral de la justice a mis au point les instruments nécessaires à la gestion de l'AIPD au sein de l'administration fédérale, notamment une directive du Conseil fédéral concernant l'évaluation préliminaire des risques et l'analyse d'impact relative à la protection des données lors de traitements de données effectués par l'administration fédérale, ainsi qu'un guide consacré à l'AIPD.

Procédures d'enquête

La nouvelle loi sur la protection des données renforce les compétences de surveillance du PFPDT et déclare la loi fédérale sur la procédure administrative applicable aux enquêtes que le PFPDT ouvre d'office ou sur dénonciation à la suite d'une violation des prescriptions de protection des données. Selon la nouvelle loi, le PFPDT dispose également de la compétence d'ordonner des mesures administratives pour imposer ces prescriptions.

Dans certaines conditions, le PFPDT a non seulement la compétence, mais aussi l'obligation d'enquêter. Il a publié une analyse détaillée des dispositions pertinentes de la loi sur son site internet et l'a en outre résumée dans un aide-mémoire.

Le PFPDT met un formulaire de dénonciation à la disposition des personnes concernées par une violation de la protection des données. Les personnes qui ne sont pas directement concernées peuvent également faire une dénonciation auprès du PFPDT.

Les responsables disposent d'un formulaire de contact spécifique s'ils souhaitent obtenir un conseil du PFPDT ou solliciter son avis sur des affaires spécifiques, par exemple en vue de l'approbation d'un code de conduite ou à propos de la communication de données personnelles à l'étranger.

1.2 Justice, police, sécurité

ENQUÊTES CONTRE FEDPOL, L'OFDF ET XPLAIN

Accès à RIPOL et violation de la sécurité des données

[Les enquêtes relatives aux accès à RIPOL et aux violations présumées de la sécurité des données chez Xplain SA ont bien avancé.](#)

Le 13 avril 2023, le PFPDT a ouvert une procédure d'enquête préalable concernant les questions soulevées par l'Aargauer Zeitung dans son édition du 11 avril 2023 au sujet de la licéité des accès de collaborateurs de l'Office fédéral des douanes et de la sécurité des frontières (OFDF) au répertoire suisse des signalements de personnes RIPOL, exploité par l'Office fédéral de la police (fedpol). Au cours de cette procédure, les deux offices fédéraux ont pris position par écrit. Après avoir pris connaissance de ces avis, le PFPDT a ouvert contre chacun des deux offices une enquête formelle concernant les accès à RIPOL. Tous deux ont répondu à un questionnaire du PFPDT et exposé les traitements de données douteux au sens de l'art. 27, al. 3, de l'ancienne LPD.

Ces deux procédures ont été suspendues jusqu'à la clôture de la procédure décrite ci-après relative à la violation présumée de la sécurité des données concernant la société Xplain SA.

Début juin 2023, fedpol et l'OFDF ont informé le PFPDT qu'une violation de la sécurité des données présentant des risques potentiellement élevés pour les personnes concernées avait eu lieu du fait de la collaboration avec le fournisseur de logiciels Xplain SA. Le 20 juin 2023, le PFPDT a ouvert de nouvelles enquêtes formelles contre les deux offices à propos de cette violation de la sécurité des données (cf. communiqué de presse du 21 juin 2023).



Ces procédures ont été étendues à l'entreprise Xplain le 13 juillet 2023 (cf. communiqué de presse du 14 juillet 2023). Dans le sillage des enquêtes, l'OFDF et fedpol ont répondu à des questionnaires relatifs à la violation de la sécurité des données. Les parties à la procédure ont édité des documents. Le PFPDT a par ailleurs procédé à l'audition des parties et de l'Office fédéral de la cybersécurité (OFCS), ce qui lui a permis d'examiner les faits de plus près. Il traite les procédures impliquant Xplain SA en priorité et entend les clore dans un délai rapproché.

PIRATAGE INFORMATIQUE

Enquêtes préliminaires concernant Concevis

[Suite à la cyberattaque dont a été victime la société Concevis, le PFPDT a ouvert deux enquêtes préliminaires visant respectivement la société et l'Office fédéral de la statistique \(OFS\). Ces enquêtes sont encore en cours.](#)

En novembre 2023, la société Concevis a été victime d'une cyberattaque par rançongiciel. Cette société fournit notamment des solutions logicielles destinées aux administrations publiques. Parmi les données concernées par cette attaque se trouvent des données de l'Office fédéral de la statistique (OFS). Mi-novembre, le PFPDT a donc ouvert deux enquêtes préliminaires visant la société Concevis et l'OFS. Le but de ces enquêtes préliminaires est de faire un premier examen sous l'angle de la LPD, afin d'évaluer s'il peut y avoir eu des manquements et, cas échéant, leur ampleur.



Le PFPDT demande que la numérisation de l'assistance administrative en matière de police ait lieu en conformité avec la protection des données

Durant l'hiver 2023/24, la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) a mené une consultation sur un projet de convention relative à l'échange de données policières impliquant la Confédération. Tant lors de la consultation que dans les médias, le Préposé s'est montré critique à l'égard de ce projet. Il demande que la modernisation de l'échange de données personnelles par la police soit proportionnée et compatible avec les droits des citoyens à la protection juridique.

Ce projet de convention a pour objectif de créer un espace commun de données policières reposant sur une plateforme de recherche. D'une part, cette plateforme devrait permettre aux corps de police cantonaux d'accéder sans condition par une consultation en ligne aux informations concernant des personnes enregistrées par les polices cantonales, mais non encore introduites dans les systèmes de police nationaux. Aujourd'hui, cet accès exige un examen au cas par cas dans le cadre d'une assistance administrative partiellement automatisée. Ainsi, selon le texte de la convention faisant foi au moment où

mettons sous presse, les autorisations et les mesures de police administratives ou encore les cas mineurs tels que les troubles à l'ordre public seraient directement consultables au niveau intercantonal. D'autre part, du fait de la participation de la Confédération prévue par la convention, ces mêmes informations seraient directement accessibles aux organes de police de la Confédération. Aujourd'hui, ces derniers traitent principalement les délits et les menaces complexes et graves pour la sécurité.

Étant donné que le champ d'application de ce projet de convention englobe tout l'éventail des tâches préventives et répressives de la police et ne lie pas l'utilisation du traitement des données personnelles entre corps de police à des objectifs suffisamment concrets, la nouvelle plateforme entraînerait une transformation systémique des flux de données de la police et des compétences de traitement à tous les niveaux de l'État fédéral (communes, cantons, Confédération). Cela concernerait aussi la protection des données, puisque le texte du projet

prévoit que le traitement des données sur la plateforme de consultation soit effectué conformément à la loi fédérale sur la protection des données et, dans le cas de la participation prévue de la Confédération, sous la surveillance du PFPDT.

Du fait que l'architecture globale du projet, visant une participation fédérale, tend par certains traits vers une structure de police unifiée, cette convention présente un potentiel élevé d'atteintes graves à la sphère privée et à l'autodétermination informationnelle de la population. L'assistance administrative, aujourd'hui partiellement automatisée via l'index national de police, est liée à une obligation générale de documentation permettant aux personnes dont les données sont transmises de défendre leurs droits. En revanche, la disponibilité en ligne sans condition de toutes les données policières fait courir le risque d'une large érosion de cette protection juridique.

Au moment de la mise sous presse, nous ne savons pas si les limitations et précisions nécessaires du point de vue de la protection des données seront intégrées au texte de la convention. Il en va de même de la participation prévue de la Confédération qui, en l'absence des limitations et précisions nécessaires, suscite en outre des réserves du point de vue du droit public et du droit constitutionnel.

La numérisation ne doit pas donner carte blanche à des superautorités monolithiques

Assistance administrative

La doctrine et la jurisprudence déduisent de la Constitution fédérale une obligation générale, pour les autorités de la Confédération et des cantons, de soutenir d'autres autorités dans l'accomplissement de leurs obligations légales par le biais de l'assistance administrative. Aujourd'hui, le premier champ d'application de l'assistance administrative est l'échange d'informations réciproque et au cas par cas. S'il s'agit de données personnelles, cet échange est régi, sous réserve de réglementations de droit spécial, par les dispositions du droit de la Confédération et des cantons en matière de protection des données.

Accès en ligne aux données personnelles

Actuellement, il est d'usage que les législateurs de la Confédération et des cantons demandent aux autorités de leur collectivité d'accorder à d'autres autorités de leur propre collectivité ou d'une autre collectivité un accès en ligne à certains segments sélectionnés des volumes de données qu'elles traitent (mais jamais à la totalité de ces volumes).

Selon la pratique actuelle du PFPDT, pour être conformes à la législation sur la protection des données, les accès en ligne aux données personnelles d'autres autorités doivent répondre à plusieurs critères :

- Tout d'abord, du point de vue **qualitatif**, il doit ressortir des bases légales que l'accès de l'autorité étrangère est limité, dans le respect du principe de proportionnalité, à des catégories de données choisies, circonscrites au soutien d'objectifs de traitement suffisamment précis de l'autorité étrangère.

- Deuxièmement, du point de vue **quantitatif**, il doit être établi, sur la base d'une grille de quantités, qu'il est approprié et nécessaire d'accorder un accès en ligne. Tel est le cas lorsque sans cet accès en ligne, chacune des tâches de l'autre autorité qu'il convient d'aider entraîne une accumulation de demandes d'assistance administrative manuelles ou partiellement automatisées ayant des motifs similaires ou identiques. En outre, le cercle des personnes autorisées doit être limité aux membres du personnel de l'autre autorité qui ont les compétences et la formation requises pour exécuter les tâches en question conformément au droit.
- Troisièmement, il convient de mener une analyse d'impact relative à la protection des données en présence de projets de grande envergure qui, compte tenu de l'ampleur et de l'intensité du partage de données en ligne ainsi que de la nature particulièrement sensible des données partagées, sont susceptibles de porter gravement atteinte aux droits fondamentaux, à la personnalité et aux intérêts de protection juridique de nombreux citoyens.

Réseautage en ligne des autorités publiques

Au cours de l'exercice sous revue, dans le cadre de diverses procédures de consultation, le Préposé a reçu un grand nombre de projets d'actes législatifs prévoyant le partage en ligne de données personnelles sensibles sous la responsabilité ou avec la participation déterminante d'organes fédéraux.

À cet égard, il est apparu que les responsables de projet ont de plus en plus de difficultés à justifier une mise en réseau en ligne des autorités dans le sens des exigences posées. Par contre, ils invoquent en substance l'argument selon lequel cette mise en réseau des autorités répond à la nécessité actuelle de numériser les administrations publiques, sur la base de ce qui est techniquement faisable, et que par le seul fait de cette nécessité, cette numérisation ne requiert ni justification particulière ni restriction quant à sa finalité ou à sa portée.

« Superautorités monolithiques »

Le PFPDT s'oppose aux arguments qui débouchent sur un diktat du « technique-ment faisable » car ces arguments entrent en conflit avec le principe de précision de la législation et avec les principes de légalité et de proportionnalité du droit de la protection des données. Il met vivement en garde contre le risque de voir des autorités, dont les tâches se recoupent en tout ou en partie, partager toutes les données qu'elles détiennent sur leurs citoyens et se mettre ainsi en réseau sans se soucier des limites de compétences d'un État de droit organisé en fonction du lieu et de l'objet. Une telle évolution devrait aboutir en définitive à ce qu'une administration publique compétente au service des citoyens soit absorbée par de superautorités monolithiques se posant comme omniscientes face aux citoyens.



1.3 Économie et société

CAMPAGNE EN LIGNE « PFARRER-CHECK »

Enquête sur l'association Forum Civique Suisse

Le mouvement *Bürgerforum Schweiz* (Forum Civique Suisse) a lancé une opération en ligne intitulée « Pfarrer-Check ». Son but est de déterminer, sur la base d'un questionnaire, quels sont les prêtres, pasteurs et autres agents pastoraux qui partagent ses opinions religieuses. Une banque de données, publiée sur Internet, indique qui a reçu le questionnaire et comment il ou elle y a éventuellement répondu. Le PFPDT a ouvert une enquête à ce propos durant le dernier trimestre 2023.

Au cours de l'exercice sous revue, le PFPDT s'est penché sur les traitements de données effectués par le Forum civique suisse dans le cadre de sa campagne en ligne « Pfarrer-Check » (contrôle des prêtres et pasteurs), cela à la suite d'une demande du Forum Civique lui-même et de signalements émanant de citoyennes et citoyens. Le Forum civique collecte les données de personnes actives dans un contexte ecclésial (prêtres, pasteurs, membres d'un conseil d'église ou d'un synode, employés des universités, animatrices et animateurs jeunesse, etc.) dont les adresses sont en libre accès, pour ensuite leur adresser un questionnaire

dont le but est d'établir si ces personnes partagent les convictions religieuses de ce même Forum. Cette collecte d'informations pose un problème en ce sens que le Forum civique a utilisé ces données pour créer une base de données accessible au public. Le Forum civique ayant refusé de tenir compte des demandes d'effacement des personnes dont les données sont publiées sur le site Internet de Pfarrer-Check, le PFPDT est intervenu dans un premier temps de manière informelle : il a requis que les demandes d'effacement de personnes concernées soient prises en compte et que les réponses au questionnaire ne soient publiées qu'avec leur consentement explicite.

Le Forum civique a accepté notre requête de ne publier que les réponses des personnes ayant donné au préalable leur consentement explicite. Mais il a estimé qu'en l'occurrence, ses traitements de données personnelles pouvaient se justifier par un intérêt public prépondérant et qu'en conséquence, même si une personne s'opposait au traitement de ses données parce qu'elle ne souhaitait pas figurer dans la banque de données, il n'entendait pas effacer les données en question.

Désireux d'étudier de plus près le traitement en cause quant à sa conformité avec la législation sur la protection des données, le PFPDT a ouvert une enquête formelle en décembre 2023. Selon le nouveau droit, il établissait d'abord les faits juridiquement contraignants dans le cadre d'une procédure administrative et concluait ensuite la procédure par une décision.

FORMULAIRE D'INSCRIPTION POUR CANDIDATS LOCATAIRES

Enquête préliminaire auprès d'une gérance immobilière

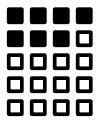
Lors d'une enquête préalable informelle, le PFPDT a signalé à une gérance immobilière que son formulaire d'inscription relatif à la location d'un appartement contenait des critères douteux du point de vue du droit de la protection des données. La gérance concernée a rectifié le formulaire sans délai.

Un formulaire d'inscription en vue de la location d'un appartement contenait, outre les questions prévisibles et admissibles relatives à l'identité et à la situation financière des futurs locataires, une injonction à produire la preuve d'une éventuelle grossesse.

Le bailleur défendait le point de vue selon lequel il fallait examiner la question à la lumière de la pénurie de logements en ville et estimait de ce fait avoir le droit d'attribuer des appartements de grande taille à des candidats sans enfants mais prévoyant d'en avoir, afin de ne pas les défavoriser vis-à-vis des candidats avec enfants. Il a précisé que lorsqu'un dossier n'était pas retenu, les données étaient effacées.

Le PFPDT a établi clairement que les gérances immobilières doivent, lorsqu'elles traitent des données, respecter les principes de proportionnalité et de finalité visés à l'art. 6 LPD.

La collecte et le traitement de données personnelles par une gérance immobilière sont admissibles pour autant qu'ils soient objectivement appropriés et nécessaires à la sélection d'un locataire approprié et qu'ils ne portent pas démesurément atteinte à la vie privée



des personnes concernées. Le traitement de données relatives à la grossesse d'une future locataire ne relève évidemment pas de cette catégorie. De plus, il n'apparaît pas clairement comment un intérêt prépondérant de la gérance ou le consentement de la personne concernée permettrait de justifier un tel traitement, ce consentement

devant être libre et éclairé, ce qui est loin d'être évident dans le contexte d'une recherche de location, vu la pénurie de biens disponibles.

La gérance immobilière a été invitée à mettre en conformité son traitement de données avec la législation, à rectifier son formulaire en conséquence et à effacer immédiatement les données éventuellement recueillies.

Elle s'est exécutée dans le délai imparti.

Enquêtes du PFPDT

Le PFPDT ouvre d'office ou sur dénonciation une enquête formelle si des indices suffisants font penser qu'un traitement de données pourrait être contraire à des dispositions de protection des données et que cette violation supposée n'est pas que de peu d'importance.

Avant d'ouvrir une enquête, il peut effectuer une première analyse informelle de la situation.

L'action du PFPDT a pour principe d'être orienté solution et économe en ressources, le but étant de remédier rapidement aux atteintes éventuelles à la personnalité. Aujourd'hui, les personnes concernées ont conscience des droits de

la personnalité qui sont les leurs, et les entreprises savent que la bonne mise en œuvre de la protection des données est un élément central de leur relation avec leur clientèle.

Lorsqu'il a connaissance d'une atteinte potentielle à la protection des données, le PFPDT commence souvent par adresser un courrier informel au responsable du traitement pour lui signaler une éventuelle irrégularité. L'expérience a montré que dans bien des cas, l'intéressé est disposé à procéder dans les temps aux modifications nécessaires.

Il va de soi que dans sa réponse au PFPDT, le responsable du traitement peut

réagir aux reproches qui lui sont adressés et exposer son point de vue sur les faits et sur la situation juridique. Dans ce cadre informel, rien ne l'oblige à donner suite aux observations du PFPDT.

Si l'échange informel ne produit pas de solution satisfaisante conforme au droit, le PFPDT se réserve le droit d'ouvrir à tout moment une enquête formelle dans le cadre de laquelle il examinera en détail les faits et la légalité du traitement des données personnelles conformément à la loi fédérale sur la procédure administrative, et prendra si nécessaire des mesures administratives après audition des responsables tenus de collaborer.

Rapport final et recommandations

Au cours de l'année sous revue, le PFPDT a clos par des recommandations la procédure d'établissement des faits lancée en 2017 à l'encontre de la plateforme d'enchères Ricardo. Selon ses conclusions, les traitements effectués par Ricardo et par TX Group – notamment la transmission et le suivi multiplateforme aux fins de ciblage publicitaire – doivent être justifiés au cas par cas par le consentement explicite des personnes concernées. Le PFPDT a également demandé que la déclaration de protection des données soit améliorée. Dans son 28^e Rapport d'activités, le PFPDT avait déjà fait part de certaines de ses constatations concernant l'état de fait examiné (cf. 28^e RA, ch. 1.4). À la suite de l'introduction d'une plateforme de gestion du consentement sur le site internet de Ricardo et de la création du Swiss Marketplace Group (SMG), le PFPDT a examiné les répercussions de ces modifications techniques et organisationnelles sur les traitements de données analysés dans la présente procédure (cf. 29^e RA, ch. 1.3).

Sur la base des précisions fournies par Ricardo et TX Group – à savoir que les traitements de données, les flux de données et les responsables des données étaient restés inchangés même après la restructuration et que les nouveaux protagonistes (les sociétés du groupe SMG et leurs actionnaires)

n'étaient pas impliqués dans l'échange de données –, le PFPDT a établi en 2022 qu'il ne fallait ni adapter ni étendre l'examen de l'état de fait sous l'angle de la procédure. Au cours de l'année sous revue, le PFPDT a toutefois appris qu'en plus de l'échange de données entre Ricardo SA et TX Group SA faisant l'objet de son examen, un échange de données a aussi lieu désormais à l'intérieur du SMG. La procédure étant déjà avancée, le PFPDT a estimé qu'il n'était pas opportun de l'étendre formellement au groupe SMG pour clarifier les faits concernant le dernier échange de données en question. Si cela s'avérait nécessaire, le PFPDT ouvrirait une nouvelle enquête sur la base de la nouvelle loi.

Afin que ses conclusions correspondent à l'état actuel des faits, le PFPDT a tenu compte de la mise en ligne d'une nouvelle déclaration de protection des données et de l'utilisation d'une plateforme de gestion du consentement sur le site internet de Ricardo. Il a complété sa constatation des faits. Ricardo et TX Group ont été

priés de vérifier l'exactitude de ce complément. C'est sur cette base que le PFPDT a élaboré son appréciation juridique de l'affaire.

Du point de vue matériel, le PFPDT a conclu que les traitements de données effectués par Ricardo et TX Group à des fins de publicité ciblée constituent des atteintes à la personnalité que ne justifient pas les intérêts des deux responsables de traitement des données. La divulgation de données par Ricardo et le traçage multiplateforme de TX Group devraient être justifiés au cas par cas par un consentement librement



donné après une information appropriée. Estimant que le traitement des données peut aboutir à un profil de personnalité,

le PFPDT a émis une recommandation selon laquelle les utilisateurs devraient être informés au préalable de cette divulgation de données au TX Group et de l'appariement multiplateforme de données à des fins de publicité ciblée ; ils devraient en outre donner leur consentement exprès. Le PFPDT demande également une amélioration des informations figurant sur la plateforme d'enchères et dans la déclaration de protection des données.

Le PFPDT a soumis son rapport final à Ricardo et au TX Group pour examen et prise de position.

DONNÉES CLIENTS

Enquête auprès de Digitec Galaxus

Le PFPDT a ouvert au printemps 2021 une procédure de vérification du traitement des données clients effectuée par Digitec Galaxus, l'un des plus grands magasins en ligne de Suisse. Dans son rapport final, il constate que les principes de transparence et de proportionnalité ne sont pas respectés et formule des recommandations à ce sujet.

À l'issue d'une enquête préliminaire informelle, le PFPDT a ouvert au printemps 2021 une procédure contre Digitec Galaxus afin de vérifier que son traitement des données clients était conforme à la législation sur la protection des données (cf. 28^e RA, ch. 1.4, et 29^e RA, ch. 1.3). L'enquête a été ouverte suite aux constats de personnes concernées selon lesquelles elles devaient accepter tous les traitements de données décrits dans la déclaration de confidentialité de l'exploitant. Toute opposition ultérieure à ces traitements était rejetée au motif que la déclaration de confidentialité s'appliquait également à tous sans exception. Dans le cadre d'une vaste procédure d'établissement des faits, la responsable a expliqué que certains traitements

n'étaient jamais effectués. Elle estimait par ailleurs que le droit du client de s'opposer à la communication de ses



données était suffisamment respecté dans la mesure où l'intéressé pouvait s'abstenir de passer une commande ou demander la suppression de ses données personnelles. Selon la responsable toujours, les traitements effectués sur le site, notamment l'obligation de créer un compte client et l'exploitation du comportement d'achat étaient conformes à la législation sur la protection des données et ne nécessitaient aucune justification.

Le PFPDT a vérifié si les informations contenues dans la déclaration de confidentialité étaient conformes aux exigences légales en matière de transparence. Il a en outre cherché à établir dans quelle mesure certains traitements de données sont proportionnés au but poursuivi s'ils sont effectués contre la volonté des personnes concernées.

Les faits ayant été jugés selon l'ancien droit en vertu de la disposition transitoire visée à l'art. 70 LPD, le Préposé a fondé ses recommandations sur l'art. 29, al. 3, de la LPD de 1992 (cf. 30^e RA, encadré p. 20).

À l'issue d'un examen approfondi, le PFPDT a notamment conclu dans son rapport final que l'exploitant viole les principes de transparence et de proportionnalité, et formulé plusieurs recommandations pour remédier aux manquements constatés

Dans sa prise de position, Digitec Galaxus a précisé que certaines des recommandations visant à accroître la transparence avaient déjà été anticipées par l'introduction d'une nouvelle déclaration de protection des données pendant la procédure en cours. Elle a rejeté certaines recommandations. Dans l'une des recommandations, le Préposé a suggéré d'adapter le traitement des données de manière à ce qu'il n'empiète pas plus que nécessaire sur l'autodétermination informationnelle de ses clients. Selon le PFPDT, une possibilité consisterait à proposer une alternative, à savoir un achat en tant que visiteur, c'est-à-dire un achat qui peut être effectué sur la plateforme en ligne sans enregistrement. Digitec Galaxus a accepté cette recommandation et soumettra au PFPDT des propositions de mise en œuvre.

Dès que ces dernières seront disponibles, le PFPDT examinera si et dans quelle mesure il interviendra contre les traitements qui font l'objet de recommandations rejetées ou éventuellement mises en œuvre de manière non conforme au droit.

APPLICATION DE RENCONTRE

Clôture de la procédure d'établissement des faits concernant Once Dating SA

Le PFPDT a clos la procédure relative à l'exploitant de la plateforme de rencontre Once, domicilié en Suisse et opérant à l'international. Après avoir vendu la plateforme, la société a confirmé au PFPDT avoir au préalable procédé au transfert ou à l'effacement des données de ses anciens clients, conformément au droit de la protection des données. Au printemps 2021, le PFPDT a ouvert une procédure d'établissement des faits concernant le traitement de données par l'application de rencontre Once. L'objectif était notamment de vérifier que la gestion des demandes de suppression et la transmission de données personnelles à des tiers étaient conformes à la législation sur la protection des données (cf. 28^e et 29^e RA, ch. 1.1, 30^e RA, ch. 1.3).

Dans son rapport final du 17 mai 2023, le PFPDT a formulé plusieurs recommandations visant à combler les lacunes constatées et à garantir le respect des principes de traitement définis dans la loi sur la protection des données. La

société Once Dating SA a accepté ces recommandations et annoncé au PFPDT qu'entre-temps, la plateforme avait été vendue à une société étrangère (cf. communiqué de presse du 13 juin 2023). Once Dating SA a précisé au PFPDT les éléments suivants : toutes les données de clients inactives ont été effacées avant la vente ; les clients actifs ont été informés de la vente et ont eu la possibilité de passer sur la plateforme exploitée par l'ayant-droit de Once Dating SA ; l'acquéreur a pris connaissance des recommandations du PFPDT concernant l'application Once. Compte tenu de ces informations, le PFPDT a clos son enquête.

TECHNOLOGIES DE TRAÇAGE

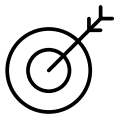
Les inquiétudes suscitées par Oracle America ont été dissipées : les personnes résidant en Suisse ne sont pas concernées par les traitements de données en cause

Les traitements de données à l'origine de la poursuite civile d'Oracle America, Inc. aux États-Unis ne concernent pas la population suisse. Le PFPDT a donc cessé ses investigations et décidé de ne pas ouvrir de procédure formelle.

Dans sa brève du 27 septembre 2022, le PFPDT avait informé le public qu'il avait pris connaissance d'une plainte collective déposée contre Oracle America, Inc. (ci-après : Oracle America) aux États-Unis et qu'il examinerait l'éventualité d'atteintes à la personnalité dans le contexte suisse aussi. Selon la plainte en question, Oracle America aurait collecté les données de cinq milliards d'internautes grâce à des technologies de traçage et les aurait rassemblées dans une base de données.

Cette entreprise aurait ainsi analysé et évalué les informations collectées afin de créer un fichier de données sur chacune de ces personnes (cf. 30^e RA, ch. 1.3).

Le PFPDT a analysé les griefs formulés dans la plainte et a contacté Oracle Suisse GmbH et Oracle America pour leur poser certaines questions. Plus précisément, il voulait savoir comment Oracle America mettait en œuvre le ch. 7 de l'Oracle Advertising Policy afin de s'assurer qu'aucune information concernant des personnes résidant en Suisse ne soit traitée à des fins publicitaires. Oracle America a assuré qu'elle n'offrait plus ses services



de courtier de données aux fournisseurs de données en Suisse et qu'elle avait résilié, depuis des années, tous les contrats avec les fournisseurs de données concernant spécifiquement des personnes résidant en Suisse. Elle a en outre expliqué de manière crédible avoir pris des mesures techniques pour empêcher l'utilisation à des fins publicitaires d'informations sur des personnes résidant en Suisse et a confirmé

que les services de publicité d'Oracle ne procédaient à aucun traitement de données sur des personnes en Suisse, à l'exception de leur anonymisation et de leur suppression pour empêcher toute utilisation à des fins publicitaires. L'entreprise a également confirmé qu'elle ne traitait pas d'informations sur des personnes résidant en Suisse en relation avec le service Oracle ID Graph, ni d'informations hors ligne les concernant. En outre, le PFPDT a pris note du fait qu'Oracle America a mis fin à tous les services AddThis au 31 mai 2023.

Pour toutes ces raisons, le PFPDT a cessé ses investigations et informé le public, par une brève en date du 6 octobre 2023, qu'aucune procédure formelle ne serait ouverte.

Introduction d'un registre des ayants droit économiques

L'introduction d'un registre fédéral des ayants droit économiques des personnes morales et autres mesures ciblées a pour but de lutter efficacement contre le blanchiment d'argent, le financement du terrorisme et la criminalité économique. Dans le même temps, elle vise à tenir compte de l'évolution des normes internationales. Le PFPDT a accompagné ce projet législatif. Il a été partiellement tenu compte de ses critiques.

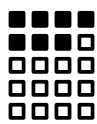
Le 12 octobre 2022, le Conseil fédéral a chargé le Département fédéral des finances (DFF) d'élaborer d'ici l'été 2023, en collaboration avec le Département fédéral de justice et police (DFJP), un projet de loi sur la transparence des personnes morales (LTPM) visant à faciliter notamment l'identification des ayants droit économiques, et ainsi à renforcer et moderniser des aspects importants du système de lutte contre la criminalité financière. La procédure de consultation relative à la LTPM a duré du 30 août 2023 au 30 novembre 2023.

Le PFPDT a exprimé ses points de vue dans le cadre de la consultation des offices. Le projet a pu être amélioré quant à la protection des données, entre autres par la précision apportée au contenu du nouveau registre fédéral des personnes réputées ayants droit économiques.

Toutefois, les préoccupations du PFPDT sur divers autres éléments de la LTPM n'ont été que partiellement éliminées lors de la mise au point du projet législatif. Le fait que l'objet et le

ÉCONOMIE

but de la loi ne soient décrits, en raison de la formulation « en particulier », que par une énumération non exhaustive a été critiqué par le PFPDT ; de même à propos du champ d'application qui, à ses yeux, n'est pas assez précis. Le PFPDT a par ailleurs souligné à plusieurs reprises que tout accès d'une autorité au registre doit être proportionné et répondre à un but identifiable. Pour cette raison, tout accès en ligne d'une autorité telle que l'Office



fédéral de la statistique ou le Service de renseignement doit être dûment motivé. Nous avons également critiqué la réglementation du profilage comme étant insuffisante.

Par ailleurs, au cours de la consultation des offices, le PFPDT a requis en vain du DFF que ce département effectue au moins un examen préliminaire en vue d'une AIPD (analyse d'impact relative à la protection des données) avant l'introduction du registre avec accès en ligne pour diverses autorités, et que les résultats de cet examen soient consignés dans un rapport explicatif. Les offices compétents n'ont pas mené les travaux requis dans ce but. En l'absence d'une AIPD, il manque certains éléments qui seraient nécessaires à une réglementation précise dans la loi.

Lors de la deuxième consultation des offices (mars 2024), le PFPDT a constaté que les risques associés étaient potentiellement élevés et que les accès en ligne n'étaient pas suffisamment justifiés, que ce soit d'un point de vue quantitatif ou qualitatif. (cf. aussi ch. 2.4)

Nouvelle loi sur l'examen des investissements étrangers

Le 15 décembre 2023, le Conseil fédéral a approuvé le message relatif à la loi fédérale sur l'examen des investissements étrangers. Lors de la consultation des offices, le PFPDT a concentré son attention sur les impératifs de la protection des données.

L'introduction d'un contrôle des investissements vise à empêcher les acquisitions d'entreprises nationales par des investisseurs étrangers lorsque ces acquisitions menacent ou compromettent l'ordre public ou la sécurité du pays. À cette fin, le projet de loi fédérale sur l'examen des investissements étrangers prévoit de soumettre les acquisitions d'entreprises suisses à l'approbation du SECO. Cette mesure cible les entreprises qui sont actives dans un domaine particulièrement critique et que des investisseurs placés sous le contrôle d'un État étranger souhaitent acquérir.

Plus de transparence

Au cours de la consultation des offices organisée à propos du message relatif à la loi fédérale sur l'examen des investissements étrangers, le PFPDT a souligné la nécessité de prendre en compte les impératifs de la protection des données, tout comme il l'avait déjà fait lors de la consultation des offices sur l'avant-projet. Ainsi, en ce qui concerne la collaboration du SECO avec les autorités suisses, le PFPDT a obtenu que soit défini plus clairement qui communique quelles données, à qui, dans quel but et de quelle manière.

Droit de recours élargi

Le PFPDT a aussi porté un regard critique sur la réglementation de la protection juridique, qui limitait initialement le droit de recours à l'investisseur étatique étranger et à l'entreprise suisse. Désormais, selon le projet de loi, cette restriction de la qualité pour recourir ne s'applique pas en cas d'ordonnance d'édition ou de renseignements du SECO. Ainsi, outre l'investisseur étatique étranger et l'entreprise suisse, les tiers prenant part à l'acquisition peuvent à présent également saisir la justice lorsqu'elles souhaitent contester une ordonnance de renseignements du SECO.

1.4 Santé

SURVEILLANCE ASSURANCE-MALADIE

Échanges entre le PFPDT et l'OFSP

Le PFPDT et l'OFSP ont mis en place des échanges réguliers dans le cadre de la mise en œuvre des recommandations de coordination émises par le Contrôle fédéral des finances concernant la surveillance des assurances maladie.

Suite à un audit effectué auprès de l'Office fédéral de la santé publique (OFSP) concernant la surveillance dans le domaine des assurances, le Contrôle fédéral des finances (CDF) a relevé qu'une clarification des rôles et la mise en place d'échanges et de coordination s'imposaient entre le PFPDT et l'OFSP (Audit CDF-20424). Dans le cadre de leurs activités, les assureurs-maladie doivent en effet respecter les dispositions relevant des assurances sociales et de la protection des données. Ils sont ainsi soumis à la surveillance tant de l'OFSP que de celle du PFPDT.

Se déclarant favorable à une coordination des activités de surveillance de l'OFSP et du PFPDT dans le domaine de l'assurance-maladie compte tenu du chevauchement des compétences

ainsi qu'à la clarification des rôles et des responsabilités, le PFPDT a rappelé que l'indépendance du PFPDT vis-à-vis des efforts de coordination dans le domaine de l'assurance-maladie devait rester garantie et qu'il continuera notamment à assumer sa fonction de surveillance vis-à-vis de l'OFSP. Dans une première étape de mise en œuvre des recommandations du CDF, le PFPDT et l'OFSP ont collaboré à l'adaptation de la circulaire numéro 7.1 de l'OFSP concernant la surveillance dans le domaine de l'assurance maladie (cf. 29^e RA, ch. 1.6).

Pour atteindre l'objectif visé par le CDF selon lequel la surveillance auprès des assureurs-maladie doit tirer profit de l'expérience et de la proximité de l'OFSP via ses interventions sur site et des compétences légales renforcées du PFPDT avec la LPD révisée, l'OFSP et le PFPDT ont, dans une deuxième étape, établi des échanges réguliers périodiques. Les deux premiers ont permis de coordonner les sujets suivants :

- Mise en place de nouvelles apps ou plateformes dans le domaine des assurances,
- développement de nouveaux modèles d'assurances,
- externalisation de données de santé,
- réactions suites à l'entrée en vigueur de la circulaire révisée numéro 7.1 sur la surveillance,
- mise en œuvre de l'obligation pour les fournisseurs de prestation de transmettre une copie de leurs factures aux assurés,

- demandes d'assurances d'accéder aux contrats de travail des employés dans le cadre des services d'aide et de soins à domicile,
- accessibilité des médecins conseil des assurances pour les médecins traitants,
- aspects de protection des données dans le cadre du développement de centres de soins réunissant différents acteurs de la santé
- ou encore problématique des attestations des assurances à l'attention des autorités fiscales. Sur ce dernier point, il a été ainsi rappelé que les autorités fiscales n'ont pas besoin de recevoir les détails sur les prestations de santé mais uniquement les montants des primes et des frais médicaux.

Le PFPDT et l'OFSP ont également échangé sur leurs activités de contrôle respectives en cours dans le domaine des assurances.

Projet de sauvetage des données de mesvaccins.ch

Après la reprise des données de l'ancienne plateforme mes vaccins.ch par la communauté de référence eHealth Argovie, le PFPDT a apporté son assistance administrative à la préposée à la transparence et à la protection des données du canton d'Argovie, désormais en charge du dossier. Le projet de restitution au moins partielle des données de vaccination, financé entre autres par l'OFSP, devrait être réalisé au plus tôt à partir du printemps 2024.

Exploitée par une fondation de droit privé et largement subventionnée par la Confédération, la plateforme mesvaccins.ch présentait de graves lacunes en matière de protection des données, ce qui amena en mars 2021 le PFDT à entamer à son encontre une procédure formelle qu'il clôtura en août de la même année par des recommandations également formelles. La fondation n'avait pu remédier ni aux lacunes ni aux manquements en matière d'intégrité des données, de sorte qu'en novembre 2022, il fallut se résoudre à prononcer sa faillite. Face au risque imminent de vente de gré à gré des données tombées dans la masse de la faillite, le PFPDT, accompagné du préposé à la protection des données du canton de Berne, enjoignit l'Office des faillites Berne-Mittelland de supprimer ces données. Le Département

de la santé et des affaires sociales du canton d'Argovie et l'Office fédéral de la santé publique s'étant engagés par écrit à respecter les dispositions légales en matière de protection des données, le PFPDT est ensuite revenu sur sa requête de suppression des données. Les données en question ont alors été transférées au canton d'Argovie, chargé d'examiner la possibilité de les restituer aux personnes concernées. (Le PFPDT a fourni des informations détaillées à ce sujet dans ses deux derniers rapports, cf. 29^e et 30^e RA, ch. 1.4).

Dans le cadre d'un avant-projet, la communauté de référence eHealth Argovie, chargée de « sauver » les données par le canton d'Argovie, a tout d'abord estimé qu'il était possible de restituer les données de vaccination aux anciens utilisateurs de la plateforme. Ainsi que l'indiquaient les responsables en mai 2023, les conditions techniques permettant une restitution des données conforme à la protection des données devaient être créées dans le projet ultérieur.

Le 11 décembre 2023, eHealth Argovie a annoncé que le projet, soutenu financièrement par l'OFSP entre autres, ne pourrait être réalisé avant le printemps 2024 au plus tôt. Cela signifiait un nouveau retard dans la restitution aux personnes concernées de leurs données de vaccination qui dataient désormais de presque trois ans et demi.

Depuis le transfert des données au canton d'Argovie, l'autorité responsable de la surveillance du traitement des données en question est la préposée argovienne à la transparence et à la protection des données. Par voie d'entraide administrative, le PFPDT a transmis à son homologue cantonale ses propres constatations établies dans le cadre de la procédure relative à la plateforme mesvaccins.ch.

Se fondant sur les faits établis et les conclusions concernant la plateforme mesvaccins.ch, le PFPDT a également



précisé à d'autres reprises que lorsque des mandats ou des subventions sont attribués à des personnes privées qui fournissent des prestations numériques à la Confédération, il est impératif de convenir des normes de sécurité de la Confédération, de les mettre en œuvre et de les contrôler.



PRATIQUE MÉDICALE

Signature d'une nouvelle déclaration de consentement par les patients

Au cours de l'année sous revue, le PFPDT a été fréquemment sollicité sur le formulaire de consentement remis pour signature par les professionnels de la santé à leurs patients depuis l'entrée en vigueur de la nouvelle LPD. Ce nouveau procédé et plus particulièrement la nécessité de signer un tel document suscitent de nombreuses interrogations de la part de patients

Plusieurs organisations et faitières des médecins mettent à disposition un modèle de déclaration de consentement à l'intention de leurs membres et partenaires. Ces formulaires visent en général un double but. D'une part, celui d'informer de manière claire et transparente le patient sur le traitement de ses données conformément aux exigences de la LPD ; notamment sur les finalités du traitement de données et sur les communications de données à des tiers qui sont envisagées (p. ex. : communication à un autre médecin, à une société de facturation, etc.) de

façon à ce qu'il comprenne les traitements de données le concernant et qu'il soit en mesure d'y consentir valablement. D'autre part, ils permettent au professionnel de recueillir le



consentement exprès du patient lorsque celui-ci est nécessaire comme dans le cas de la communication de données sensibles, dont font partie les données relatives à la santé d'une personne. À noter que, selon la loi, ni l'information ni le consentement ne nécessitent, en soi, la forme écrite mais la déclaration de volonté de la personne concernée doit être suffisamment claire. Dans la pratique, la forme écrite est cependant souvent privilégiée pour des raisons de preuves ou documentaires. En signant ce document, le patient atteste donc qu'il a été informé et qu'il consent à ce que ses données soient traitées dans la mesure décrite. En vertu du principe de proportionnalité, seules les données personnelles dont ces tiers ont besoin pour atteindre leurs objectifs légitimes de traitement seront toutefois communiquées en évitant toute transmission en bloc.

Parallèlement, les données de santé sont également soumises au secret médical, ce qui implique que toute communication à des tiers sur un patient implique son consentement préalable, sous peine d'être sanctionné pénalement

(art. 321 du Code pénal) et sous réserve également d'obligations légales de communication à des autorités ou des tiers.

Le patient est libre de signer ou non le formulaire. Il faut toutefois être conscient que le professionnel a besoin d'un consentement pour communiquer des données sur la santé à des tiers et qu'il a un intérêt compréhensible à disposer d'un document écrit, attestant également que l'information a été donnée. Aussi, un refus de signer ou la suppression de certaines clauses peut conduire le professionnel à refuser une prise en charge en raison de l'insécurité juridique dans laquelle il peut se retrouver.

En conséquence, si des éléments du formulaire ne sont pas clairs, semblent excessifs ou que des questions demeurent, le PFPDT recommande d'en discuter avec la personne qui a remis ce document pour y apporter les précisions appropriées.

RÉUTILISATION DES DONNÉES

Rapports entre la loi sur la protection des données et la loi sur la recherche sur l'être humain

[La loi sur la recherche sur l'être humain \(LRH\) et la loi sur la protection des données \(LPD\) traitent chacune de la réutilisation des données à des fins de recherche. L'articulation entre ces deux lois est ainsi une question récurrente.](#)

Durant l'année écoulée, le PFPDT a régulièrement dû examiner la question de l'articulation entre la LRH et la LPD, que ce soit dans le cadre de consultations d'office ou de conseils aux particuliers comme aux organes fédéraux.

De fait, la LRH et la LPD traitent de questions parfois similaires. Tel est en particulier le cas des régimes de réutilisation à des fins de recherches de données collectées antérieurement, à d'autres fins (par exemple un médecin souhaite envoyer les résultats d'examens d'un patient à des chercheurs). Ces situations sont visées par les art. 31 al. 2 let. e et 39 LPD (applicables aux personnes privées, respectivement aux organes fédéraux) et art. 32 ss LRH.

La LRH est une loi spéciale par rapport à la LPD. Elle a donc le pas sur la LPD pour ce qui tombe dans son champ d'application : en substance, la recherche sur des maladies humaines ou sur le corps humain, sur des personnes

(y compris décédées, des embryons ou des foetus), sur du matériel biologique ou sur des données de santé. À noter que la LRH ne règle que certains aspects du traitement de données ; pour ce qui n'y est pas spécifiquement réglé, la LPD continue à s'appliquer.

Concrètement, l'une des principales différences entre ces régimes est la base légitimant la réutilisation : un intérêt prépondérant du responsable de traitement (art. 31 al. 2 LPD) ou la loi elle-même (art. 39 LPD) pour la LPD, le consentement (à des degrés divers) pour la LRH.

D'une manière générale, le régime LRH peut paraître plus complexe que celui de la LPD. Cela se justifie cependant par l'objet considéré – la recherche sur l'être humain, sujet par définition sensible. Dans ce contexte, le mécanisme standard de l'art. 31 al. 2 LPD serait en effet peu adéquat, dès lors qu'il est basé sur une pesée des intérêts réalisée par le responsable de traitement lui-même (soit le médecin, celui-ci étant alors « juge » et partie). Le cadre plus précis défini par la LRH permet donc une meilleure prise en compte de la volonté de la personne, une meilleure information et, globalement, une plus grande sécurité juridique, tant dans l'intérêt des personnes concernées que des chercheurs.

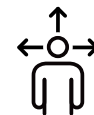
Révision complète de la Loi fédérale sur le dossier électronique du patient

Le Conseil fédéral entend poursuivre le développement et promouvoir la diffusion et l'utilisation du dossier électronique du patient à l'aide de diverses mesures ciblées. Il a donc soumis en consultation un projet de révision complète de la loi en juin 2023 prévoyant plusieurs adaptations importantes. Le PFPDT a pris position sur certains éléments clés.

Le projet de révision induit un changement de paradigme. Alors que la loi sur le dossier électronique du patient (LDEP) actuelle prévoit le libre consentement à l'ouverture d'un dossier électronique du patient (DEP), le projet de révision vise à passer du modèle du consentement explicite (opt-in) à celui du droit d'opposition (opt-out) dans la mesure où toute personne domiciliée en Suisse et au bénéfice d'une assurance obligatoire de soins devra désormais disposer d'un dossier électronique, à moins qu'elle ait expressément

refusé la constitution d'un tel dossier après information préalable. Dans un tel cas, le refus sera consigné dans un registre des oppositions. En l'absence d'opposition, le DEP sera ouvert et pourra être rempli ou géré par des professionnels de la santé et le patient qui déterminera qui y a accès. La révision de la loi a également pour effet d'obliger tous les prestataires de soins de santé à s'affilier à une communauté ou à une communauté de référence certifiée ainsi qu'à enregistrer les données pertinentes pour le traitement des patients dans le DEP afin de les rendre disponibles aux autres professionnels de la santé.

En tant qu'autorité de surveillance en matière de protection des données, le PFPDT considère que le modèle actuel, à savoir le consentement préalable à l'ouverture d'un dossier électronique, garantit davantage le droit à l'autodétermination des personnes concernées qui se traduit par le droit pour chaque



personne de pouvoir déterminer elle-même si elle souhaite ou non disposer d'un dossier électronique et dans quel but des

informations à son sujet (par ex. santé) peuvent être traitées. Si le modèle de l'opposition était toutefois retenu, sa mise en œuvre devrait être garantie de manière uniforme et sans formalisme excessif dans tous les cantons.

La révision prévoit également d'autres nouveautés qui modifient ou étendent les traitements de données personnelles sur lesquels se fonde le DEP actuel et intensifient les risques pour la personnalité et l'autodétermination informationnelle qui en découlent pour les personnes concernées : Par conséquent, le PFPDT a invité l'Office fédéral de la santé publique à procéder à une évaluation de ces risques supplémentaires et à effectuer si nécessaire une analyse d'impact relative à la protection des données, ainsi qu'à présenter les résultats de ses réflexions sur ce point. Si les données sont généralement accessibles aux seules personnes autorisées, le patient doit être informé de la signification de chaque autorisation et de sa hiérarchie ainsi que de la possibilité de limiter les accès. De plus, il faut généralement garantir, conformément au principe de la protection des données par défaut, que les paramètres correspondent au niveau de confidentialité le

plus élevé et qu'aucun accès par des professionnels de la santé n'est possible sans l'intervention active des personnes concernées. En cas d'entrée ou de sortie dans un groupe de professionnels de la santé, le patient devrait en être informé systématiquement, sauf s'il ne le souhaite pas.

Le PFPDT salue le fait que le droit d'accès des assureurs-maladie se limite à l'enregistrement dans le DEP de certaines données administratives définies avec l'accord des patients. Quant à la possibilité d'exploiter les données du DEP à des fins de recherche, le PFPDT prend positivement acte que la révision de la loi permettra la mise à disposition des données médicales non anonymisées uniquement moyennant le consentement explicite des patients.

Il juge cependant plus problématique l'accès au DEP par des applications de santé tierces telle qu'envisagé par la révision. Avec le consentement du patient, les applications de santé auront accès au DEP et leur permettront d'enregistrer et/ou de consulter des données médicales, p. ex. via un smartphone ou un appareil médical. Ainsi, le PFPDT estime que, pour toutes les applications, la protection et la sécurité des données des patients doivent être garanties de manière globale. Par conséquent, l'accès au DEP par des applications de

santé tierces dont la fiabilité et le niveau de sécurité ont été préalablement évalués et qui doivent être certifiées ne constitue pas un risque pour les données des patients, ni pour la sécurité opérationnelle du DEP lui-même. La mise à disposition d'une interface n'est acceptable que dans la mesure où une analyse approfondie des risques a été effectuée et que des mesures ont été mises en œuvre pour les réduire. En outre, le transfert des données de l'application vers le DEP doit être suffisamment sécurisé et crypté.

Compte tenu du nombre de personnes concernées et de la nature sensible de ces données, le PFPDT considère qu'il convient de définir encore plus clairement dans la loi les compétences et les responsabilités en matière de traitement des données.

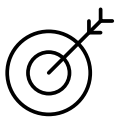
1.5 Travail

DROIT DU TRAVAIL

Directives applicables à la gestion des dossiers personnels

L'obligation d'effacer les données à caractère personnel qui ne sont plus nécessaires, et leur conservation dans le dossier personnel, soulèvent maintes questions auprès des employeurs. Pour y répondre, il est essentiel de considérer le principe de proportionnalité.

Durant l'année sous revue, le PFPDT a de nouveau été contacté à de nombreuses reprises sur la manière de gérer les dossiers du personnel en conformité avec le droit de la protection des données, notamment quant aux délais et aux formes de conservation, mais aussi à propos de l'effacement des données personnelles. Dans le cadre des rapports de travail, le traitement de données personnelles est autorisé si les principes généraux de traitement des données (en particulier les



principes de proportionnalité et de finalité) et selon le code des obligations sont respectés. Plus précisément, l'employeur ne peut traiter que les données personnelles nécessaires à l'exécution du contrat de travail (en termes d'aptitude et de réalisation). Cela signifie que les données personnelles doivent être effacées lorsqu'elles ne sont pas ou plus nécessaires ou que le but du traitement des données est atteint. Des informations détaillées sur les délais de conservation avant, pendant et après les rapports de travail, ainsi que sur les formes de conservation, peuvent être consultées sur le site Internet du PFPDT.

DROIT DU TRAVAIL

Qualification des caisses de pension sous l'angle de la protection des données

Désireuses de s'informer sur les dispositions de la LPD auxquelles les caisses de pension sont soumises, de nombreuses institutions de prévoyance et associations professionnelles se sont adressées au PFPDT. De l'avis de ce dernier, les caisses de pension agissent en tant qu'organes fédéraux dans le cadre du régime obligatoire de la prévoyance professionnelle (LPP), tandis que dans le régime surobligatoire, ce sont les dispositions concernant les personnes privées qui s'appliquent. La question est pertinente dans le sens où les organes fédéraux doivent déclarer au PFPDT leur registre des activités de traitement conformément à l'art. 12 LPD et leur conseiller à la protection des données au sens de l'art. 10 LPD.

L'application du régime de prévoyance professionnelle obligatoire (régime obligatoire LPP) constitue une tâche publique de la Confédération (tâche fédérale au sens de l'art. 5 let. i LPD). Selon la jurisprudence du Tribunal administratif fédéral, les caisses de pension enregistrées participant à la mise en œuvre de l'assurance obligatoire sont considérées comme des personnes

morales chargées d'une tâche fédérale (TAF, A-4467-2011, consid. 4.2). Pour remplir leurs obligations légales dans le cadre du régime obligatoire LPP, les caisses de pension doivent impérativement traiter les données personnelles des assurés. Elles traitent donc des données personnelles pour l'accomplissement de cette tâche fédérale et agissent en tant qu'organe fédéral dans le cadre du régime obligatoire LPP.

Par contre, dans le régime surobligatoire, les caisses de pension sont soumises aux dispositions spécifiques de la LPD pour les personnes privées, à la condition toutefois que le traitement des données n'ait rien à voir avec les tâches publiques et relève exclusivement du domaine surobligatoire. C'est le cas des institutions de prévoyance qui fournissent des prestations exclusivement en dehors du régime obligatoire et qui ne sont donc pas enregistrées (art. 48 LPP a contrario). C'est également le cas de la prévoyance individuelle facultative du pilier 3A/3B. Lorsqu'une séparation des domaines n'est pas possible ou s'avère difficile, les dispositions applicables aux organes fédéraux s'appliquent à l'ensemble de l'activité.

Les caisses de pension qui agissent en tant qu'organes fédéraux pour la partie obligatoire ou en tant que personnes privées pour la partie surobligatoire sont soumises à la surveillance du PFPDT. Cela vaut également pour les caisses de pension dites enveloppantes, à savoir les institutions de prévoyance actives à la fois dans le domaine obligatoire et dans le domaine surobligatoire, selon que le traitement de données en question est effectué dans le cadre du régime obligatoire LPP ou dans le cadre du régime surobligatoire.

Les caisses de pension agissant en tant qu'organes publics cantonaux ou communaux

Les caisses de pension des employés cantonaux, communaux et municipaux dont les tâches sont liées à la prévoyance professionnelle et qui, à ce titre, procèdent à des traitements de données personnelles, ne sont en principe pas des organes fédéraux. Ces caisses constituent des organes publics cantonaux ou communaux et sont soumises, dans le cadre de la LPP obligatoire, à la législation cantonale sur la protection des données ainsi qu'à la surveillance cantonale ou municipale.

Les sociétés de services des caisses de pension agissant en tant que sous-traitantes

Il arrive, dans la pratique, que des institutions de prévoyance confient une partie ou la totalité de leurs activités opérationnelles à une entreprise extérieure. Ce type de société de services agit sur mandat de l'institution de prévoyance, en qualité de sous-traitante de données au sens de l'art. 9 LPD.

Pour les caisses de pension, la qualification d'organe fédéral au sens de la LPD est une question pertinente, car tout organe fédéral doit déclarer ses activités de traitement au PFPDT conformément à l'art. 12 LPD. Au cours de l'année sous revue, les institutions de prévoyance ont ainsi procédé à plus de 10 00 inscriptions dans le registre des activités de traitement des organes fédéraux (Datareg).



1.6 Transports

PROJETS DIVERS

Conseils et consultations des offices dans le domaine de la mobilité

Dans le cadre de conseils de projet et de consultations d'offices, le PFPDT s'est exprimé à plusieurs reprises sur des questions liées aux transports et à la mobilité. Il demande aux entreprises de transports publics à concession étatique que le voyage anonyme et le paiement en liquide demeurent possibles et ne soient entravés ni par la privation de rabais, ni par d'autres obstacles administratifs.

Au cours de l'année sous revue, le PFPDT a conseillé des particuliers et des organes fédéraux sur le thème de la mobilité. Il est essentiel à ses yeux que les entreprises chargées du transport de passagers – tâche de l'État régie par la loi – continuent de garantir aux voyageurs la possibilité de voyager de manière anonyme à l'intérieur du pays. En outre, les fournisseurs de services ayant un impact en matière de données doivent continuer à accepter l'argent liquide comme moyen de paiement.

Plateforme informatique NOVA pour les transports publics

Dans le contexte de la faille constatée en février 2022 sur la plateforme centrale de distribution NOVA – que les CFF exploitent sur mandat d'Alliance SwissPass (ASP), organisation de la branche des transports publics (cf. 29^e RA, ch. 1.7) –, le PFPDT a notamment attiré l'attention des CFF sur l'exigence de proportionnalité en matière de conservation des données. Le respect des délais d'effacement n'était pas entièrement mis en œuvre au début de l'année sous revue. Vers la fin de cette

même année, l'équipe en charge de la protection des données auprès des CFF a effectué un audit afin de déterminer si les règles d'effacement étaient entièrement appliquées dans NOVA. Si cet audit révèle des lacunes, le PFPDT veillera à ce qu'il y soit entièrement remédié.

De plus, au 1^{er} janvier 2024, la branche des transports publics a mis en place des normes en matière de sécurité de l'information, contraignantes notamment pour les entreprises de transport affiliées à NOVA. Les entreprises déjà affiliées à NOVA bénéficient d'un délai de transition unique : elles doivent prouver au plus tard fin juin 2024, sur la base d'une auto-évaluation, qu'elles respectent les directives. Si des lacunes sont constatées, les entreprises concernées sont tenues de les documenter et d'y remédier d'ici fin 2024.

Système de mesure de l'affluence des CFF

Le nouveau système de mesure de l'affluence 2.0 des CFF (KFMS 2.0) avait donné lieu à des spéculations en raison du manque de clarté de l'appel d'offres initial (cf. 30^e RA, ch. 1.6), les CFF ont présenté depuis au PFPDT une analyse d'impact relative à la protection des données (AIPD), comme convenu dans le cadre de la consultation du PFPDT. Sur la base de cette AIPD et des précisions fournies par les CFF, le PFPDT a établi qu'il n'y avait en aucun cas génération de données personnelles susceptibles d'être utilisées de manière abusive au sens d'un risque théorique.

Il a donc estimé que la mesure de l'affluence des passagers dans sa conception actuelle est conforme à la protection des données.

Projet pilote de SwissPass pour la collecte des clés de répartition

Alliance SwissPass nécessite certaines données pour pouvoir répartir correctement entre les entreprises de transport qu'elle rassemble les recettes tirées des titres de transport forfaitaires tels que les abonnements généraux (AG). L'objectif du projet pilote est de recueillir la clé de répartition de façon numérique, en invitant le client à participer à un relevé en ligne de l'utilisation de son AG. Pour y participer, il doit installer sur son téléphone mobile une application de traçage d'un partenaire externe mandaté (par ex. un institut d'études de marché) qui saisit à intervalles réguliers la position de l'appareil. Celui-ci envoie les données de localisation enregistrées à l'institut d'études de marché qui calcule alors les itinéraires. Puis les voyages ainsi enregistrés sont envoyés sous forme anonymisée à l'Alliance SwissPass (ASP), qui les évalue et effectue ultérieurement le calcul de la clé de répartition de l'AG. L'institut d'études de marché efface par la suite les données personnelles.

Le PFPDT a attiré l'attention des CFF sur le fait que la mise en œuvre de ce projet doit accorder toute l'attention requise à la sécurité des données car le relevé numérique des données engendre de nouveaux risques. Le choix de l'institut d'études de marché devra se faire en fonction de l'aspect particulier de la conservation des données (p. ex. emplacement du serveur en Suisse). Les

DONNÉES PNR

principes de finalité et de transparence attachés à la protection des données doivent aussi être toujours respectés.

Conduite automatisée

Le PFPDT est également intervenu à plusieurs reprises sur la conduite automatisée, notamment lors de la consultation organisée par l'OFROU sur l'ordonnance y relative. Il a demandé que les objectifs soient atteints sans traitement de données personnelles sensibles et sans profilage à risque élevé. Il a souligné en outre que les projets législatifs requièrent que l'on examine suffisamment tôt s'il faut procéder à une AIPD. L'OFROU a informé le PFPDT que ses suggestions avaient été largement intégrées au projet d'ordonnance.

Vidéosurveillance dans les transports publics

Plusieurs entreprises concessionnaires de transport par autobus ainsi que des fabricants de véhicules de transport public ont voulu savoir comment mettre en place une vidéosurveillance intégrale à l'intérieur et à l'extérieur des nouveaux autobus dans le respect de la protection des données. Selon la réponse du PFPDT, une base légale suffisamment concrète doit exister, le principe de proportionnalité doit être respecté et les personnes concernées doivent clairement percevoir qu'elles sont filmées. Elles doivent aussi savoir à qui elles peuvent s'adresser pour obtenir des informations afin d'exercer leurs droits de personnes concernées.

Consultation des offices relative à la loi sur les données de passagers aériens

Le DFJP a remanié son projet législatif concernant l'utilisation par la Suisse des données de passagers recueillies par les compagnies aériennes (passenger name records [PNR]) et organisé une deuxième consultation des offices à son propos. Le PFPDT a pris position dans ce cadre.

Les données PNR sont communiquées à la compagnie aérienne ou à l'agence de voyage lors de la réservation d'un vol par le passager. Ces informations doivent servir à prévenir le terrorisme et la grande criminalité, par exemple en les comparant aux bases de données des organes de poursuite pénale. De nombreux pays européens ont déjà mis en place des services correspondants (appelés Unités Informations Passagers [UIP]) chargés de recueillir, d'enregistrer et de traiter les PNR.

Le PFPDT également pris position lors de la deuxième consultation des offices, organisée pendant l'année sous revue (à propos de la première consultation, cf. 29^e Rapport d'activités, chap. 1.7, et 28^e Rapport d'activités, chap. 1.8). Il a notamment fait remarquer qu'à partir de l'entrée en vigueur de la LPD révisée le 1^{er} septembre 2023, il fallait, pour tout projet législatif, vérifier en temps utile s'il implique un traitement de données présentant un risque potentiellement élevé pour la personnalité ou les droits fondamentaux des personnes concernées, et s'il y a lieu d'effectuer une analyse d'impact relative à la protection des données personnelles. Celle-ci doit être soumise au PFPDT pour avis avant la consultation des offices.

Pour le PFPDT, il était également essentielle que le projet législatif et sa mise en œuvre respectent à aussi insisté sur la nécessité de respecter à tout moment, lors de la mise en œuvre du p les principes de traitement des données prévus par la LPD, en particulier le principe de proportionnalité. Il faut notamment veiller à ce qu'en cas de faux positif, les personnes dont les critères correspondent au profil de risque ne soient pas enregistrées comme suspectes et que leurs données soient immédiatement pseudonymisées puis effacées. Les demandes du PFPDT concernant l'AIPD ont été prises en compte et mentionnées dans le message.



1.7 International

UNION EUROPÉENNE

DATA PRIVACY FRAMEWORK

Décision d'adéquation de l'UE

Le 15 janvier 2024, la Commission européenne a confirmé que le niveau de protection des données garanti par la Suisse était adéquat.

Dans son rapport du 15 janvier 2024, la Commission européenne a reconnu que la législation suisse continue d'offrir un niveau de protection suffisant en matière de traitement des données personnelles. Le transfert vers la Suisse de données personnelles provenant d'États membres de l'Union européenne (UE) ou de l'Espace économique européen (EEE) va donc pouvoir se poursuivre sans garanties supplémentaires, ce qui revêt une importance économique considérable.

La Suisse disposait depuis l'an 2000 d'une décision d'adéquation de l'UE adoptée sous la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Cette directive a été remplacée en 2016 par le règlement (UE) 2016/679 (règlement général sur la protection des données [RGPD], cf. 30^e RA 2022/2023, p. 11).

La décision de la Commission européenne revêt une importance capitale pour la place économique suisse, en particulier pour sa compétitivité.

Cadre de l'échange de données vers les États-Unis

Durant l'été 2023, l'UE et les États-Unis se sont accordés pour créer un nouveau cadre applicable au transfert de données de l'UE vers les États-Unis, à la suite de quoi la Commission européenne a adopté sa décision d'adéquation. De son côté, la Suisse a aussi mené des discussions avec les États-Unis.

En septembre 2020, dans le contexte de l'arrêt Schrems II rendu par la Cour de Justice de l'Union européenne (CJUE), le PFPDT avait constaté que le bouclier de protection Suisse-États-Unis (Swiss-US Privacy Shield) ne fournissait pas un niveau de protection suffisant en cas de transfert de données de la Suisse vers les États-Unis, malgré l'octroi de droits de protection particuliers aux personnes concernées en Suisse (cf. 28^e RA, Accent II.). Depuis lors, les transferts de données personnelles de la Suisse vers les États-Unis nécessitent des garanties supplémentaires au sens de l'art. 16, al. 2, LPD telles que des clauses de protection des données, des clauses type de protection des données ou des règles d'entreprises contraignantes.

En juillet 2023, l'UE et les États-Unis se sont accordés sur un nouveau cadre de protection des données UE/États-Unis (Data Privacy Framework, ci-après DPF UE/US), à la suite duquel la Commission européenne a adopté une nouvelle décision d'adéquation concernant le transfert de données vers les États-Unis. Le niveau adéquat de protection des données fixé dans cette décision ne s'applique toutefois qu'aux données personnelles transmises à des entreprises américaines certifiées qui participent au DPF UE-US. Selon la Commission européenne, le DPF répond aux préoccupations exprimées par la CJUE dans l'arrêt Schrems II, en premier lieu parce qu'il limite l'accès des services de renseignement américains aux données personnelles de l'UE et a créé une nouvelle cour chargée du contrôle de la protection des données (Data Protection Review Court, DPRC) auquel les citoyens de l'UE auront accès. De son côté, le Royaume-Uni a également adopté une décision d'adéquation en faveur des États-Unis, le UK-US Data Bridge, sur la base d'une extension du DPF UE-US.

La Suisse a aussi mené de son côté des discussions avec les États-Unis en vue d'établir un cadre parallèle. Depuis l'entrée en vigueur de la nouvelle loi sur la protection des données le 1^{er} septembre 2023, la tâche d'évaluer si un État étranger ou une organisation internationale offre un niveau de protection des données adéquat incombe

au Conseil fédéral et non plus au PFPDT. Les États et organisations internationales jugés adéquats par le Conseil fédéral sont listés dans l'annexe de l'ordonnance sur la protection des données (OPDo). De ce fait, des garanties supplémentaires au sens de l'art. 16, al. 2, LPD sont nécessaires pour les transferts de données de la Suisse vers les États-Unis jusqu'à l'entrée en vigueur de la décision d'adéquation du Conseil fédéral sur ces transferts et l'ajout des États-Unis sur la liste des États à l'annexe 1 OPDo. En cas d'accord sur un nouveau cadre juridique de protection des données entre la Suisse et les États-Unis, la décision d'adéquation du Conseil fédéral ne devrait s'appliquer qu'aux transferts de données vers des entreprises américaines participant au cadre de protection des données et ayant certifié leur adhésion aux principes de ce cadre (comme dans le contexte du DPF UE-US et de l'ancien bouclier de protection Suisse-États-Unis), tandis que les transmissions à des entreprises américaines non certifiées devraient demeurer liées à d'autres garanties appropriées au sens de l'art. 16, al. 2, LPD.

Ratification de la Convention 108+

Le comité consultatif de la convention du Conseil de l'Europe sur la protection des données a adopté, lors de ses réunions plénières, les deux premiers modules des clauses contractuelles types pour le transfert de données à caractère personnel. La Suisse a ratifié la convention modernisée (Convention 108+) juste après l'entrée en vigueur de la LPD révisée. La Convention 108+ devrait entrer en vigueur en 2024.

Le PFPDT participe régulièrement aux réunions plénières bisannuelles et aux réunions du bureau du comité consultatif de la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108, dite C108). Lors de sa réunion plénière de juin 2023, le comité consultatif a adopté le premier module des clauses contractuelles types pour le transfert de données à caractère personnel. Ce premier module traite le transfert de données entre deux responsables de traitement. Le deuxième module traite le transfert de données du responsable de traitement à un sous-traitant en tant qu'importateur. Il a été adopté lors de la réunion plénière de novembre 2023. Un troisième et dernier module dédié au transfert de données de sous-traitant à sous-traitant est en cours d'élaboration. La représentante du PFPDT participe à ces travaux en tant que rapporteure.

Le comité consultatif s'intéresse aussi au traitement de données dans le cadre de votations et d'élections et dans le contexte des neurosciences. Tous les documents s'appuient déjà sur la Convention 108 modernisée, dite C108+ ou Convention 108+. Le protocole d'amendement de la C108 a été adopté par le Comité des ministres le 18 mai 2018, mais il n'entrera en vigueur que lorsque 38 États parties l'auront ratifié. La convention étant ouverte aux États non membres du Conseil de l'Europe, elle déploie ses effets au-delà de l'Europe. En Suisse, la LPD révisée met en œuvre la C108+ à l'échelle fédérale. La Suisse fut donc le 28^e État membre à remettre à la secrétaire générale du Conseil de l'Europe, le 7 septembre 2023, l'instrument de ratification de la C108+. Fin décembre, 31 États avaient ratifié la convention, et 15 l'avaient signée sans l'avoir encore ratifiée. Il est probable que de nouvelles ratifications suivront dans les prochains temps, et que la C108+ entrera en vigueur au cours de l'année 2024.

EUROPE

Réunion avec l'ICO et le CEPD

Au cours d'une réunion informelle, le PFPDT a évoqué avec ses homologues du Royaume-Uni et de l'Union européenne la possibilité d'intensifier la collaboration du CEPD avec les États non membres de l'UE et de l'EEE présentant un niveau de protection des données équivalent.

En septembre 2023, le PFDPT, son homologue britannique de l'Information Commissioner's Office (ICO) et la présidente du Comité européen de la protection des données (CEPD) se sont retrouvés à Bruxelles pour une réunion informelle afin d'évaluer leur collaboration future. Les échanges se poursuivent sur le plan bilatéral dans le cadre des organes internationaux officiels.

Par ailleurs, la Commission européenne a organisé une rencontre de haut niveau à début mars avec toutes les autorités concernées par une décision d'adéquation afin de favoriser le partage d'expériences et les échanges d'informations. Les discussions ont notamment porté sur la coopération entre les autorités en matière d'application des dispositions relatives à la protection des données.

EUROPEAN CASE HANDLING WORKSHOP

Rencontre internationale en Suisse

L'édition annuelle du ECHW a été organisée à Berne par le PFPDT. Axée sur la pratique, elle a permis aux représentants de 37 autorités de protection des données de 27 États européens et de la Suisse de discuter des dernières avancées technologiques et des questions qui en découlent pour la protection des données. Le but était d'analyser la jurisprudence en la matière et de débattre des solutions aux problèmes du quotidien.

Le PFPDT a organisé l'édition 2023 du European Case Handling Workshop (ECHW, atelier européen de gestion de cas) à Berne les 8 et 9 novembre derniers. Cette manifestation axée sur la pratique, qui se déroule sous l'égide de la conférence des autorités européennes de protection des données (Spring Conference), a réuni plus de 80 représentants de 37 autorités de protection des données de 27 États européens et de la Suisse, dans le but de favoriser les échanges.

L'ECHW a donné lieu à 13 ateliers dirigés par différentes autorités de protection des données et consacrés aux défis suscités par le maniement des dernières technologies et aux questions en suspens d'importance nationale ou internationale liées à la protection des données en Europe et en Suisse. Parmi les sujets traités figuraient le recours aux techniques numériques de détection de visages ou de reconnaissance faciale et l'influence de celles-ci sur la protection des données, ou la définition des données personnelles par rapport aux dernières technologies (intelligence artificielle, suivi analytique et publicitaire, etc.). Les participants ont aussi abordé la loi américaine appelée Cloud Act, qui autorise les autorités américaines de poursuite pénale à accéder aux données personnelles traitées par des filiales de sociétés américaines en Europe, y compris en relation avec des projets dans le secteur public utilisant des applications en nuage (Microsoft 365, p. ex.).

Les débats féconds et la participation active de tous ont produit des échanges constructifs et des enseignements précieux pour le travail quotidien des autorités suisses et européennes de protection des données.

Déclaration commune sur le moissonnage et sur la protection des données

Le PFPDT a publié, avec onze autres autorités nationales de protection des données, une déclaration commune à l'attention des plateformes de réseaux sociaux concernant la protection des données personnelles contre le moissonnage, qui consiste à extraire automatiquement des données d'un site web.

En août 2023, le PFPDT a publié, avec onze autres autorités nationales de protection des données, une déclaration commune à l'attention des plateformes de réseaux sociaux concernant la protection des données personnelles contre le moissonnage de données. Aussi appelée data scraping, cette pratique consiste à extraire automatiquement des données de la toile.

Cette déclaration commune enjoint aux entreprises de réseaux sociaux et aux exploitants de sites web de prendre des mesures pour protéger les données personnelles contre cette pratique. En effet, le moissonnage de données peut entraîner une violation de la sécurité des données (data breach). La LPD révisée entrée en vigueur le 1^{er} septembre 2023 oblige les entreprises à annoncer au PFPDT les cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 24, al. 1, LPD).



La déclaration commune énumère par ailleurs les précautions que les particuliers peuvent prendre pour réduire au maximum le risque de moissonnage de leurs données. Les entreprises de réseaux sociaux et les exploitants de sites web sont tenus de communiquer activement sur la manière dont ils protègent leurs clients contre le data scraping et sur les mesures que chacun peut prendre pour contribuer à la protection de ses données.

INTERNATIONAL

OCDE

L'OCDE mène des recherches et des analyses approfondies sur la gouvernance des données afin de contribuer aux discussions internationales. Dans le même temps, elle insiste sur la nécessité de renforcer la confiance dans les échanges transfrontières de données. À cette fin, les travaux de l'OCDE entendent contribuer à la création d'un environnement numérique mondial qui permette la circulation des données au-delà des frontières, tout en garantissant que lorsqu'elles franchissent ces frontières, ces données bénéficient de la surveillance et de la protection souhaitées.

Notamment du fait de sa diversité géographique – ses pays membres vont de l'Europe aux États-Unis, en passant par le Japon et l'Australie – l'OCDE est une organisation internationale qui œuvre au premier plan mondial pour promouvoir la protection de la sphère privée. Même si la plupart des instruments de l'OCDE ont un caractère de « droit persuasif », ils posent souvent les bases de futures négociations sur des instruments juridiquement contraignants. Dans le domaine de la protection des données, l'action de l'OCDE est considérée comme une

source d'inspiration pour d'importants instruments internationaux, tels que le RGPD ou le DPF UE-US.

Le PFPDT est représenté au sein du Groupe de travail de l'OCDE sur la gouvernance des données et la protection de la vie privée dans l'économie numérique (Data Governance and Privacy Working Party, DGP). Le DGP est rattaché au Comité des politiques de l'économie numérique (CPEN) de l'OCDE. Il est composé de délégués des 38 pays membres de l'OCDE, dont des représentants des gouvernements et des autorités de protection des données. Le DGP coopère avec les autres groupes de travail du CPEN et d'autres organes de l'OCDE ; il élabore et promeut des stratégies de gestion des données et de protection de la vie privée reposant sur des données étayées. L'objectif de ces stratégies est de maximiser les avantages sociaux et économiques d'une utilisation plus large et plus efficace des données, tout en gérant les risques et défis qu'elle pose face à la protection de la sphère privée. Dans ce contexte, mentionnons par exemple la révision de la Recommandation de l'OCDE sur la coopération transfrontière dans l'application des législations protégeant la vie privée, les nouvelles connaissances et analyses sur la libre circulation des données dans la confiance (DFFT), ou encore l'analyse des approches politiques et réglementaires actuelles sur les technologies renforçant la protection de la vie privée (Privacy Enhancing Technologies / PETs).

SCHENGEN

BTLE et CEPD

Le sous-groupe de travail Border, travel and law enforcement (BTLE) du Comité européen de la protection des données (CEPD) traite aussi de thèmes relatifs à l'acquis de Schengen. La Suisse, en tant qu'État associé à Schengen, a participé à cette partie de ses travaux, dont l'élaboration et l'achèvement des grandes lignes de l'art. 37 de la directive (UE) 2016/680 et la formulation de nouveaux principes directeurs sur les droits des personnes concernées dans cette même directive.

Au cours de l'année sous revue, le sous-groupe de travail BTLE a élaboré à l'intention du CEPD les grandes lignes de l'art. 37 « Transferts moyennant des garanties appropriées » de la directive (UE) 2016/680 de l'UE (dite « Law Enforcement Directive, LED »), qui règle la protection des données dans le domaine des poursuites pénales. Ces grandes lignes décrivent notamment les conditions légales que doivent remplir les garanties appropriées lorsque des données sont transférées vers un pays tiers (extérieur à l'UE et à l'EEE). À cet égard, le PFPDT a déclaré que la Suisse,

SCHENGEN

en tant qu'État associé à Schengen, n'est pas un pays tiers, ce qui a été pris en compte dans la mesure où au sens de l'art. 37, la Suisse n'est pas un pays tiers. À l'issue des travaux, le document final a été mis à la disposition du public pour avis du 27 septembre au 8 novembre 2023.

Les travaux qui viennent d'être entamés portent sur l'élaboration de nouveaux principes directeurs relatifs aux « droits des personnes concernées » dans la directive « police-justice », notamment dans ses art. 12 « Communication et modalités de l'exercice des droits de la personne concernée » et 15 « Limitations du droit d'accès ». Ils visent aussi à analyser et à commenter les aspects de l'accès direct (auprès du responsable du traitement lui-même) et indirect (par l'intermédiaire de l'autorité de protection des données, comme c'est le cas en Belgique, p. ex.) aux données personnelles.

Groupes de coordination du contrôle des systèmes d'information SIS II, VIS et Eurodac

Les traitements de données des systèmes d'information Schengen, dont le volume s'était effondré pendant la pandémie, ont retrouvé leur niveau d'avant le COVID-19. Certains États génèrent un nombre particulièrement élevé de demandes de renseignements. Des échanges intenses avec la société civile, représentée par des ONG triées sur le volet, ont été mis en place.

Le comité coordonné de surveillance du système d'information Schengen (SIS) et les groupes de coordination du contrôle du système d'information sur les visas (VIS) et du système européen de comparaison des empreintes digitales des demandeurs d'asile (Eurodac) sont des organes créés en vertu du droit de l'UE afin de surveiller la protection des données personnelles dans les systèmes d'information en question. Ils se composent de représentants des autorités nationales de protection des données et du Contrôleur européen de la protection des données (CEPD).

Le nouveau mécanisme d'évaluation et de contrôle soumet chaque État membre de Schengen à une évaluation non plus tous les cinq ans, mais tous les sept ans. Cette évaluation porte sur la protection des données, la coopération policière, les grands systèmes informatiques (supplément d'information requis à l'entrée nationale

[SIRENE], SIS), le retour, la protection des frontières et les pools d'experts en matière de visas. Le PFPDT a dépêché un expert en vue de l'évaluation de l'Estonie dans le domaine de la protection des données du 13 au 17 novembre 2023.

Le transfert du secrétariat du CEPD au Comité européen de la protection des données en mars 2023 a fait passer de deux à quatre le nombre de réunions annuelles consacrées au SIS. Lors de ces réunions, les autorités de protection des données ont constaté que certains États génèrent un nombre particulièrement élevé de demandes de renseignements Schengen, certains allant jusqu'à envoyer simultanément la même demande à des douzaines d'entre elles. L'évolution de la situation est en cours d'observation.

Dans le cadre de ses réunions, le comité coordonné de surveillance du SIS a lancé cette année des échanges intenses avec la société civile, en invitant de grandes ONG européennes à y participer.

Le volume des traitements de données, qui avait considérablement chuté pendant la pandémie, a retrouvé son niveau d'avant le COVID-19.

SCHENGEN

Groupe de coordination Schengen des autorités suisses de protection des données

Les autorités de protection des données de la Confédération et des cantons et celle de la Principauté de Liechtenstein se sont réunies à deux reprises dans le cadre du groupe de coordination Schengen, présidé par le PFPDT.

Le groupe de coordination Schengen des autorités de protection des données de la Confédération et des cantons s'est réuni en juin et en décembre 2023. Le PFPDT en assure la présidence. L'autorité de protection des données de la Principauté de Liechtenstein est membre du groupe avec un statut d'observateur. Lors des deux réunions, le PFPDT a

exposé les résultats des travaux des groupes européens de coordination du contrôle des systèmes d'information SIS et VIS à Bruxelles. Le PFPDT et ses homologues cantonaux ont ensuite partagé leur expérience concernant les contrôles qu'ils effectuent.

Les cantons ont rapporté que les contrôles réguliers des fichiers journaux des collaboratrices et collaborateurs dotés d'un droit d'accès aux systèmes d'information Schengen favorisent la prise de conscience relative à la protection des données.

Le groupe de coordination étant désormais régi par une loi fédérale formelle et non plus dans une simple ordonnance, il a adapté formellement son règlement d'organisation en conséquence.

Un sous-groupe de travail est en train d'élaborer à l'intention des autorités cantonales de protection des données un modèle de mise à jour des sites web qui leur permettra de mettre facilement en ligne des informations sur Schengen, lesquelles instruiront notamment les personnes concernées de leurs droits.

SCHENGEN

Activités relatives à Schengen au niveau national

Le contrôle auprès de fedpol en qualité de point d'accès central du C-VIS (système central d'information sur les visas) a été poursuivi et un contrôle des fichiers journaux (log files) a été entamé auprès du Corps des gardes-frontière.

Le PFPDT a poursuivi le contrôle qu'il avait initié au cours de l'exercice précédent auprès de fedpol en qualité de point d'accès central du C-VIS. Ce contrôle porte sur la consultation de données de visas Schengen à des fins de prévention, de détection ou d'enquête en matière d'infractions terroristes et autres infractions pénales graves. Le PFPDT a néanmoins dû suspendre ce contrôle en raison de l'élargissement du périmètre d'enquête à Xplain SA (cf. ch. 1.2).

De plus, au cours de l'exercice sous revue, le PFPDT a débuté un contrôle des fichiers journaux VIS auprès du Corps des gardes-frontière afin de vérifier la légalité des accès effectués. Pour ce faire, le PFPDT a demandé au conseiller à la protection des données du Secrétariat d'État aux migrations (SEM) d'extraire et d'analyser, sur la base d'un échantillonnage, les journaux d'accès (les log files) établis, sur une période définie, par les utilisateurs autorisés du Corps des gardes-frontière. Divers entretiens ont été menés avec ces personnes, au cours desquels elles devaient expliquer et démontrer au PFPDT la légalité de certaines demandes.

Les États membres de l'espace Schengen sont responsables du contrôle de la licéité du traitement des données à caractère personnel effectué par une autorité de contrôle nationale établie conformément au règlement (UE) 2016/679. En vertu du règlement (CE) no 767/2008, les États membres veillent, conformément à leur législation nationale, à ce que les transferts effectués à partir du C-VIS soient consignés dans des registres et que ces enregistrements puissent être consultés par les autorités nationales de la protection des données qui en font la demande. En Suisse, le SEM est l'autorité compétente en la matière.

Association francophone des autorités de protection des données personnelles

Les autorités membres de l'Association francophone des autorités de protection des données personnelles (AFAPDP), dont le PFPDT, se sont rencontrées à Tanger les 2 et 3 octobre 2023 pour les Rencontres francophones de la protection des données personnelles.

Pendant deux jours, les autorités indépendantes de 26 pays partageant une langue, une tradition juridique et des valeurs communes se sont réunies.

Cette année, le thème central de la conférence était le moissonnage des données (ou « data scraping ») qui consiste en l'extraction automatisée d'informations personnelles à partir d'Internet. Cette pratique comporte en effet un certain nombre de risques pour les données personnelles, dont notamment les cyberattaques ciblées,

l'usurpation d'identité, le profilage, les spams ou encore la prospection directe non autorisée. Le Commissariat à la protection de la vie privée du Canada, la Commission nationale pour le contrôle des données à caractère personnel (CNPD) du Maroc et le Préposé fédéral à la protection des données et à la transparence (Suisse) ont ainsi présenté la prise de position commune qu'ils ont publiée en août dernier avec 11 autres autorités de protection. Cette déclaration commune recommande ainsi aux entreprises du numérique de prendre un certain nombre de mesures.

Durant le tour de table des évolutions et actualités législatives en matière de protection des données personnelles dans l'espace francophone, le PFPDT a par ailleurs eu l'occasion de présenter la nouvelle LPD.

L'AFAPDP a également tenu sa 14^{ème} Assemblée générale annuelle qui a permis l'examen et l'adoption de ses rapports moral et financier. De plus, l'association a accueilli en son sein les autorités de Géorgie, du Kosovo et de la Mauritanie – représentés au sein de l'Organisation internationale de la Francophonie – portant le nombre de ses membres à 26.

COOPÉRATION INTERNATIONALE

Privacy Symposium de Venise

Le PFPDT a assisté au Privacy Symposium, une conférence internationale destinée à faciliter le dialogue, la coopération et la convergence parmi experts, chercheurs et autorités de protection des données du monde entier. L'édition 2023, placée sous le patronage de l'Autorité italienne de protection des données personnelles – le Garante – s'est tenue du 17 au 21 avril à Venise.

Le Privacy Symposium a donné lieu à des échanges sur les derniers développements et perspectives en matière de protection des données et de la vie privée. Accueillis par l'université Ca'Foscari, plus de 200 intervenants de haut niveau ont pris part à plus de 80 sessions sur des thématiques d'actualité telles que la coopération internationale, la technologie et la conformité, les perspectives socio-économiques et la recherche et l'innovation.

Sa journée d'ouverture a été consacrée à un programme spécial sur le traité du Conseil de l'Europe relatif à la protection de la vie privée et des données (Convention 108) et différentes sessions et ateliers ont traité de l'impact futur du protocole modernisant le

traité (Convention 108+) sur le renforcement de la protection des données au niveau mondial et sur la facilitation de la circulation des données entre les pays.

Le PFPDT a ainsi présenté la nouvelle loi fédérale sur la protection des données, son rôle au sein de la Convention 108 ainsi que la promotion de la coopération entre et avec les autorités de contrôle européennes non membres du CEPD.

La participation du PFPDT lui a également permis d'échanger de manière informelle avec ses homologues italien (Garante) et allemand (BfDI) ainsi qu'avec le contrôleur européen sur des sujets tels que ChatGPT, l'informatique en nuage ou encore le transfert des données à l'étranger.

ENJEUX INTERNATIONAUX

Assemblée mondiale pour la protection de la vie privée

Les nouvelles technologies et leurs incidences sur la vie privée étaient au cœur des préoccupations de l'Assemblée mondiale pour la protection de la vie privée. Lors de sa réunion annuelle, elle a adopté sept résolutions, dont deux sur l'intelligence artificielle.

L'Assemblée mondiale pour la protection de la vie privée (AMVP) a pour objectif de discuter des principaux enjeux en matière de protection de la vie privée et de la façon dont les organismes de réglementation peuvent travailler efficacement – tant individuellement que collectivement – pour protéger la vie privée dans un monde de plus en plus axé sur les données.

Les incidences sur la vie privée de technologies telles que l'intelligence artificielle (IA) et l'IA générative ont été au cœur de cette réunion annuelle qui a adopté deux résolutions à ce sujet

- L'une sur les systèmes d'intelligence artificielle générative : elle rappelle la nécessité de respecter les principes essentiels de la protection des données lors du développement, de l'exploitation et du déploiement de systèmes d'intelligence artificielle ;
- L'autre sur Intelligence artificielle et emploi : elle souligne l'importance des principes et des garanties en matière de protection des données et de la vie privée dans le développement et l'utilisation de systèmes d'intelligence artificielle dans le contexte de l'emploi (y compris le recrutement).

Lors de cette assemblée, l'AMVP a également adopté les cinq résolutions suivantes :

- Une résolution sur les principes mondiaux de protection des données visant à mettre à jour les principes adoptés par l'AMVP à Madrid en 2009 à la lumière des récents développements technologiques. La résolution inclut de nouveaux principes tels que la protection des données dès la conception et par défaut, le droit à la portabilité des données et un cadre pour le profilage et la prise de décision automatisée ;
- Une résolution sur la création d'une bibliothèque de ressources sur les principes clés de la protection des données ;

- Une résolution sur la création d'un groupe de travail sur une approche intersectionnelle du genre en matière de protection des données ;
- Une résolution sur les données de santé et la recherche scientifique ;
- Une résolution proposant un prix conjoint AMVP/Access Now sur la protection des données et les droits de l'homme.

Finalement, le plan stratégique 2023–2025 a également été adopté. Il mettra l'accent sur les domaines d'intérêt stratégique de l'AMVP, qui comprendra un accent sur les droits des personnes concernées et le renforcement de la capacité des autorités de protection des données.

L'Assemblée mondiale pour la vie privée – dont le PFPDT est membre – a été créée en 1979. Sa 45^e édition s'est tenue du 15 au 20 octobre 2023 à Hamilton (Bermudes).

EUROPE

Conférence européenne des commissaires à la protection des données à Budapest

La Conférence européenne des commissaires à la protection des données a notamment discuté des derniers développements et des points en suspens concernant la communication transfrontalière de données. Ils ont aussi évoqué la coopération entre autorités de protection des données, exemples à l'appui, et les moyens de sensibiliser le public à l'importance de la protection des données. Pour la première fois, une session ouverte a été organisée.

La session fermée de la Conférence européenne des commissaires à la protection des données a porté sur quatre sujets : les nouvelles technologies, le droit de la concurrence, les décisions de justice et les meilleures pratiques/études de cas en matière de coopération entre les pays de l'EEE et les pays hors EEE pour l'application de la législation. Le panel sur les nouvelles technologies a permis d'examiner les impacts de la technologie sur notre société, en particulier sur notre façon de penser et sur nos relations. Le panel sur le droit de la concurrence visait à explorer les liens entre le droit de la concurrence et la protection des données, en essayant d'identifier comment ces deux domaines du droit peuvent se soutenir l'un l'autre. En outre, le panel consacré aux meilleures pratiques/études de cas en matière de coopération entre les pays de l'EEE et les pays non membres de l'EEE a donné un aperçu de l'expérience

acquise en matière de coopération entre les pays en dehors de la coopération relative au RGPD. Enfin, le panel consacré aux décisions de justice a permis de faire le point sur les affaires les plus importantes de Strasbourg et de Luxembourg.

Pour la première fois, la Conférence de printemps proposait une session ouverte au grand public. Les panels proposés se sont concentrés sur les thèmes suivants : la relation délégués et autorité de protection des données, le réseau et la formation des délégués et le rôle du délégué au sein de l'organisation.

Par ailleurs, les membres ont adopté trois résolutions :

- Une résolution sur la nécessité d'une coopération renforcée dans le domaine de la protection des données et du droit de la concurrence ;
- Une résolution visant à accréditer l'autorité de protection des données de Saint-Marin
- Une résolution sur la révision des règles de procédure de la Conférence.

La 31^e Conférence européenne des commissaires à la protection des données s'est tenue du 10 au 12 mai 2023 à Budapest. La session fermée a rassemblé 138 membres des autorités de protection des données, la session ouverte a enregistré quant à elle plus de 350 personnes, provenant de 39 pays.



Principe de la transparence

2.1 Généralités

La loi sur la transparence (LTrans) vise à promouvoir la transparence quant à la mission, l'organisation et l'activité de l'administration en garantissant l'accès du public aux documents officiels (cf. art. 1 LTrans). En permettant la vérifiabilité de l'action administrative et, partant, son acceptation, le principe de la transparence favorise la confiance dans l'État et dans les autorités.

Les chiffres fournis par l'administration fédérale concernant les demandes d'accès à des documents officiels reçues en 2023 montrent que les besoins des médias et de la société en informations spécifiques et en transparence de l'administration (ou de l'activité administrative) non seulement ne faiblissent pas, mais ont même présenté un nouveau pic de demandes. Au cours de l'année sous revue, le nombre des demandes d'accès adressées aux autorités fédérales a augmenté de presque 50 % par rapport à l'année précédente. Selon les informations fournies par les autorités, cette augmentation a également eu des répercussions

sur la charge de travail requise par le traitement des demandes. Il est apparu d'une manière générale que la mise en œuvre du principe de la transparence demeure un grand défi. Les chiffres ci-après (cf. ch. 2.2) montrent que la tendance constatée des dernières années (forte proportion d'accès intégralement accordés) s'est confirmée durant l'année sous revue.

Si les demandeurs ou les tiers concernés ne sont pas d'accord avec l'accès que les autorités envisagent d'octroyer, la loi sur la transparence leur offre la possibilité de déposer une demande en médiation auprès du Préposé. Le Préposé a reçu au cours de l'année sous revue 132 demandes en médiation, ce qui représente une légère augmentation de 2 % par rapport

à l'année précédente. Le but de la procédure de médiation est de parvenir rapidement à un accord entre les parties. L'organisation de procédures de médiation orales a de nouveau fait ses preuves en 2023 : l'évaluation des demandes en médiation traitées au cours de l'exercice montre qu'une solution à l'amiable a été trouvée dans 55 % des cas où une médiation orale a pu être menée.

Les demandes en médiation, en nombre très élevé depuis plusieurs années, ainsi que les procédures menées par écrit en conséquence de la pandémie ont entraîné un allongement de la durée de traitement et, par contrecoup, un retard dans le règlement des procédures. Nous constatons en parallèle une complexité croissante des questions et des problèmes juridiques auxquels il convient de donner une réponse dont en particulier, durant l'année sous revue, les procédures de médiation liées aux contrats d'acquisition de vaccins COVID-19 et la reprise de Credit Suisse par l'UBS. Du fait des facteurs

mentionnés, le Préposé a dépassé le délai légal de 30 jours pour une grande part des procédures.

Cette année encore, le Préposé a observé une recrudescence des initiatives visant à exclure du principe de transparence des pans supplémentaires de l'activité administrative ou certaines catégories de documents (cf. ch. 2.4). Dans ce contexte, l'administration soutient régulièrement que le respect des obligations légales de collaborer

et de notifier ne peut être garanti que si la loi sur la transparence est exclue. Le Préposé fédéral estime par contre que dans un État de droit, il convient de considérer que les obligations légales de collaborer et de notifier sont respectées et appliquées. Les éventuelles violations de ces règles de droit par des assujettis – même si ou précisément parce qu'elles reposent sur le principe de transparence – ne peuvent en aucun cas justifier ces restrictions de la loi sur la transparence. Introduire de telles réserves se traduit par un affaiblissement du principe de transparence et, partant, de la transparence de l'administration. Un aperçu des dispositions spéciales réservées au sens de l'art. 4 LTrans figure au ch. 2.5.

2.2 Demandes d'accès – augmentation considérable en 2023

Selon les chiffres communiqués par les autorités fédérales, 1701 demandes d'accès ont été déposées au cours de l'année sous revue (contre 1153 en 2022), ce qui correspond à une augmentation de 48 % par rapport à 2022. À cela s'ajoutent 37 demandes déposées durant les années précédentes mais traitées en 2023. Les autorités ont accordé un accès intégral aux documents dans 830 cas (48 %), contre 624 (53 %) en 2022, et un accès limité ou différé dans 402 cas (23 %), contre 236 (20 %) en 2022. Dans 176 cas (10 %), l'accès a été totalement refusé, contre 99 (8 %) en 2022. Selon les indications des autorités, 73 demandes d'accès (4 %) ont été retirées, contre 53 (5 %) en 2022, 96 demandes étaient en suspens à la fin de 2023 et 161 cas ne correspondaient à aucun document officiel.

Nous estimons qu'au cours des années à venir, l'accès aux informations émanant de l'administration continuera de susciter un grand intérêt, même si le besoin d'information et de transparence, particulièrement marqué durant la pandémie, s'est tourné durant l'année sous revue vers d'autres aspects des affaires du monde. Les autorités ont procédé à une évaluation statistique

des demandes d'accès concernant les documents officiels liés au COVID-19 et l'ont transmise au Préposé avec les informations à communiquer annuellement (cf. Statistiques « Demandes d'accès liées au COVID-19 »). Selon les indications des autorités fédérales, sur 1738 demandes traitées, 39 (soi 2 %) concernaient le COVID-19, ce qui représente à nouveau une diminution considérable par rapport à l'année précédente (8 %). L'accès complet a été accordé dans 12 cas (31 %), soit moins souvent que dans la statistique générale. Toujours dans le domaine des demandes liées à la pandémie, les autorités ont accordé un accès partiel ou différé dans 17 cas (44 %), soit plus souvent, et un refus complet dans 1 cas (2 %), soit cinq

fois moins que par rapport à la statistique générale. 2 demandes d'accès liées à la pandémie étaient encore en suspens fin 2023 et dans 7 cas, la demande ne correspondait à aucun document officiel.

En résumé, le Préposé constate que durant l'année sous revue, pour la première fois depuis 2015, l'accès complet aux documents a été accordé dans un peu moins que la moitié des cas. Par contre, les refus complets qui se sont stabilisés au fil des ans à près de 10 % restent stables à un niveau bas.

Départements et offices fédéraux

En 2023, l'attention des médias et de la société s'est concentrée sur certaines unités administratives. Du fait de leur domaine d'activité, le DDPS (432), le DETEC (236) ainsi que le DFI (230) et le DFAE (228) ont reçu un grand nombre de demandes d'accès. Dans le cas du DFI, 15 % des demandes concernaient l'accès interdépartemental à des documents officiels liés au COVID-19 (38 % en 2022). Selon les autorités, certaines de ces demandes étaient à la fois très volumineuses et très complexes, et un

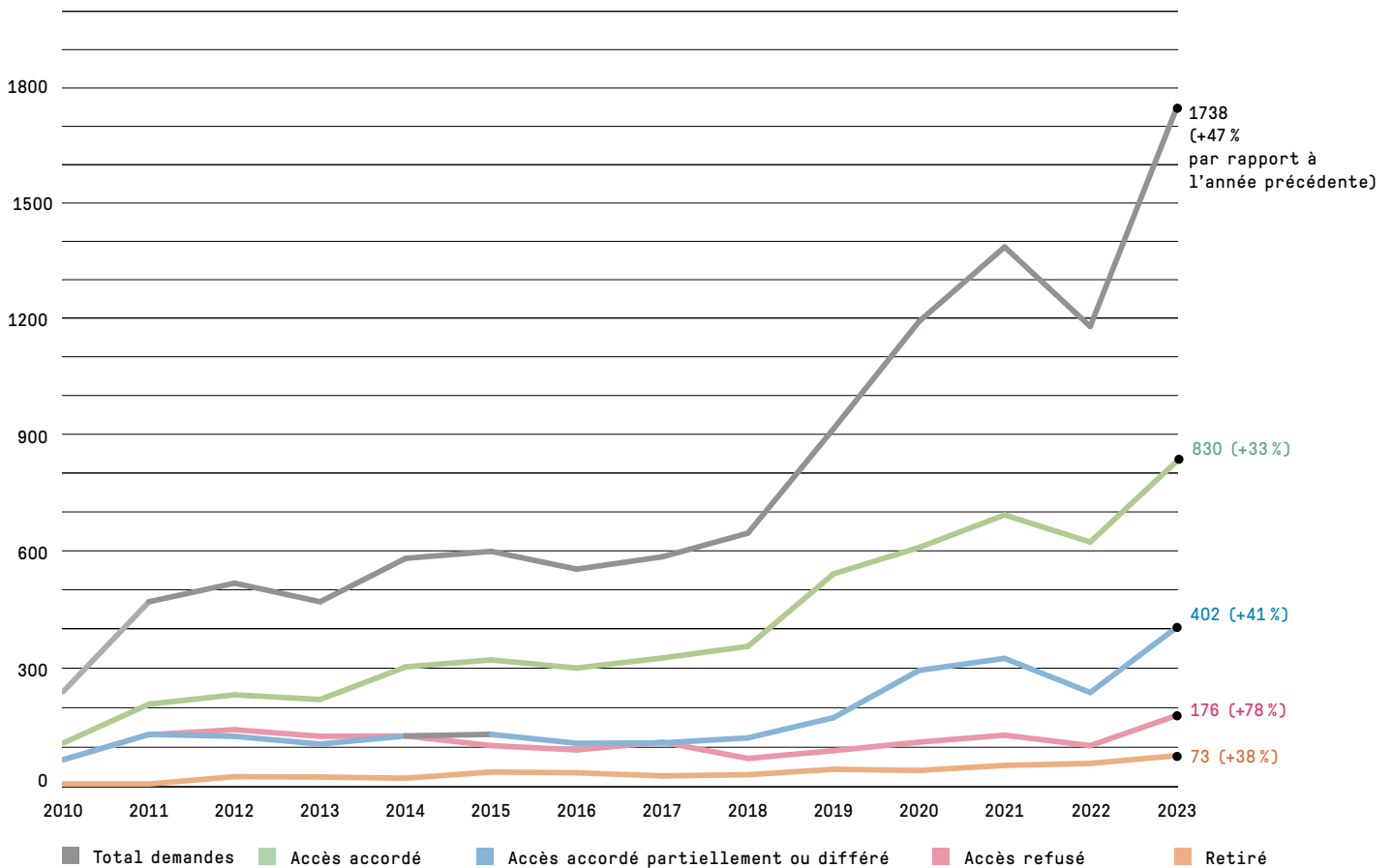
grand nombre de cas ont nécessité une coordination entre offices ou entre départements.

Au niveau des offices, c'est l'OFSPPO qui a signalé le plus de demandes d'accès (277) en 2023. Viennent ensuite l'OFEV (98), le SG-DFF (87) et le SG-DDPS (83). 14 autorités déclarent n'avoir reçu aucune demande d'accès en 2023. Le Préposé fédéral lui-même en a reçu 14, dont 10 pour lesquelles il a accordé un accès complet et 1 pour laquelle il a entièrement refusé l'accès. 3 demandes étaient en suspens fin 2023.

En 2023, les émoluments perçus pour l'accès à des documents officiels ont atteint un montant de 14 226 francs, inférieur de 42 % à celui de l'année précédente (24 582 francs). Alors que le DFAE, le DFJP, le DDPS, les Services du Parlement et le Ministère public de la Confédération n'ont prélevé aucun émolument, les quatre autres départements et la Chancellerie fédérale

ont facturé aux demandeurs une partie du temps consacré au traitement (DFI : 6 403 francs : DEFR : 4 498 francs : OFEV : 1 675 francs : DFI : 1 500 francs : ChF : 150 francs). Signalons que 19 seulement des 1 738 demandes traitées ont donné lieu à la perception d'émoluments. Par rapport à l'année précédente, au cours de laquelle des émoluments ont été perçus dans 29 cas, cela représente un recul considérable, tant pour le nombre de cas dans lesquels un émolument a été perçu que pour la

Graphique 1 : Demandes d'accès – évolution depuis 2010





somme totale des émoluments. En tout état de cause, la perception d'émoluments demeure une exception : près de 99 % des demandes d'accès n'en ont pas fait l'objet en 2023. La pratique de l'administration, qui permet sur le principe de consulter gratuitement les documents officiels, est inscrite depuis le 1^{er} novembre 2023 dans la loi sur la transparence. La perception d'émoluments demeure exceptionnellement possible lorsqu'une demande d'accès entraîne un surcroît de travail particulier pour les autorités. Le Conseil fédéral a décidé de baisser à huit heures le seuil de surcroît de travail requis, alors que le Préposé fédéral avait fait remarquer qu'un seuil trop bas ne respectait pas la volonté du législateur (à propos de la modification en question de l'ordonnance sur la transparence, cf. ch. 2.4).

S'agissant du temps consacré au traitement des demandes d'accès, le Préposé rappelle que les autorités ne sont pas tenues de le consigner et qu'il n'existe pas de directive de saisie uniforme pour l'ensemble de l'administration fédérale. Aussi, les indications qui lui sont fournies (sur une base volontaire) ne reflètent-elles que partiellement la réalité. Selon ces données, le temps consacré au traitement a sensiblement augmenté, passant de 5404 en 2022 à 6469 heures en 2023.

Les données fournies par l'OFSP montrent clairement que le temps de traitement déclaré par les autorités

ne correspond que partiellement à la réalité. En plus du temps de travail de 287,5 heures indiqué ponctuellement par les unités spécialisées compétentes de l'OFSP et du soutien juridique apporté par sa conseillère à la transparence à hauteur d'un poste à 80 %, l'OFSP a signalé une charge de travail toujours très élevée pour le traitement des demandes d'accès liées au COVID-19 (y c. les procédures de médiation et de recours), estimée à au moins 2,8 postes à plein temps. Il en va probablement de même pour d'autres unités de l'administration fédérale.

Il est à noter une diminution du temps consacré à la préparation des procédures de médiation : 730 heures par rapport à 1006 heures l'année précédente (cf. à ce propos 865 heures en 2021, 569 heures en 2020, 473 heures en 2019, 672 heures en 2018 et 914 heures en 2017).

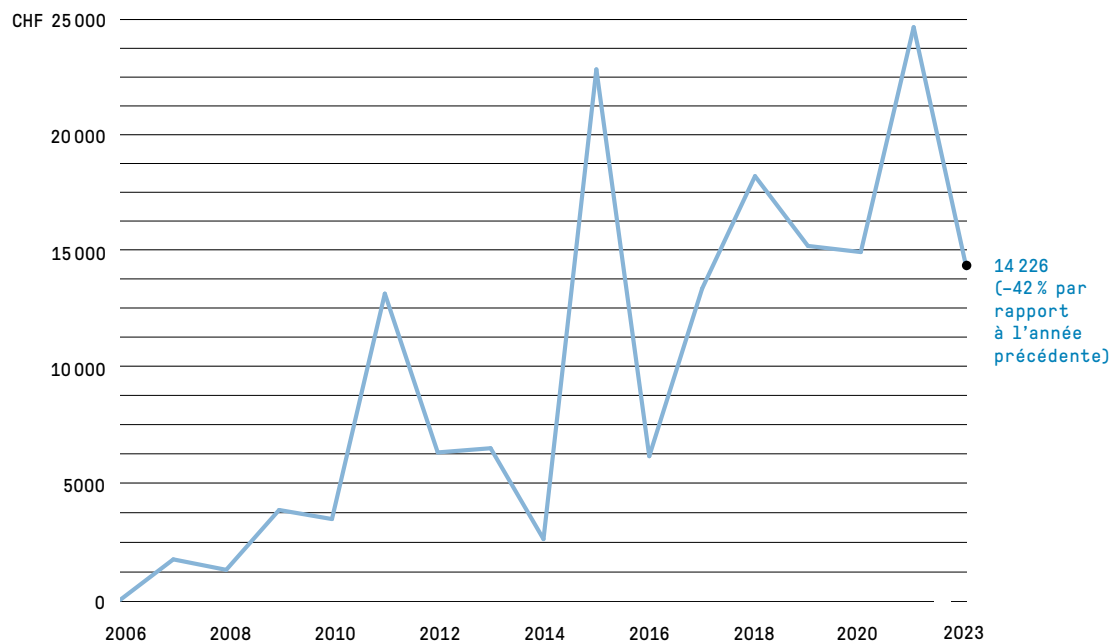
Services du Parlement

Les Services du Parlement ont déclaré avoir reçu 2 demandes d'accès au cours de l'année écoulée. Dans un cas, l'accès a été entièrement refusé, dans l'autre la demande ne correspondait à aucun document officiel.

Ministère public de la Confédération

Le Ministère public de la Confédération a déclaré avoir reçu 2 demandes d'accès en 2023. L'accès a été entièrement accordé dans un cas, dans l'autre la demande ne correspondait à aucun document officiel.

Graphique 2 : Émoluments prélevés depuis l'entrée en vigueur de la LTrans



2.3 Procédures de médiation – Légère augmentation des demandes en médiation

En 2023, le Préposé fédéral a reçu 132 demandes en médiation, ce qui correspond à une augmentation de 2 % par rapport aux 129 demandes reçues en 2022. La plupart de ces demandes émanaient de journalistes (74) et de particuliers (31). Ces chiffres permettent les constatations suivantes : sur les 739 cas dans lesquels l'administration fédérale a refusé entièrement ou partiellement la demande d'accès, l'a différée ou a invoqué qu'elle ne correspondait à aucun document officiel, 132 (18 % des cas) ont donné lieu au dépôt d'une demande en médiation.

En 2023, 142 demandes en médiation ont été réglées, dont 18 (14 %) concernaient des documents officiels en relation avec le COVID-19. Parmi ces

142 demandes, 105 avaient été déposées dans l'année, 34 en 2022 et 3 au cours des années précédentes. Dans 54 cas, un accord à l'amiable a été obtenu. Le Préposé fédéral a en outre émis 47 recommandations ayant permis de régler 61 cas dans lesquels aucun accord ne s'esquissait.

Aux cas terminés s'ajoutent aussi 12 demandes remises hors délai, 9 pour lesquelles les conditions d'application de la loi sur la transparence n'étaient pas remplies, et 6 qui ont été retirées.

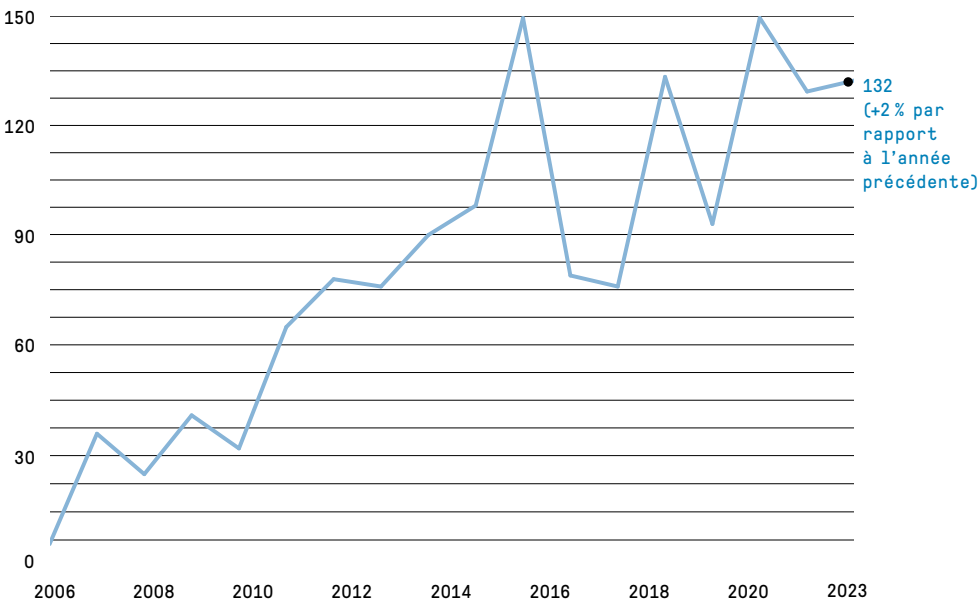
À la fin de l'année, 9 procédures de médiation étaient suspendues en accord avec les participants ou à la requête des demandeurs.

Proportion des solutions amiables

Les solutions à l'amiable présentent de nombreux avantages, dont ceux de clarifier la situation, d'accélérer la procédure d'accès aux documents et de faciliter une éventuelle future collaboration entre les personnes impliquées dans la séance de médiation.

L'efficacité des séances de médiation orales apparaît surtout dans le rapport entre les solutions amiables et les recommandations. Au cours de l'année

Graphique 3 : Demandes en médiation depuis l'entrée en vigueur de la LTrans



sous revue, 54 solutions amiables ont été trouvées et le Préposé a émis 47 recommandations écrites afin de régler 61 cas. Par rapport aux recommandations, les solutions amiables représentent donc 47 % des procédures de médiation. Il convient toutefois d'apporter quelques précisions à ce sujet : en général, pour aboutir à une solution amiable, il faut qu'une séance de médiation puisse avoir lieu. Ainsi, pendant l'année sous revue, sur les 62 procédures menées, 34 (55 %) ont permis d'aboutir à un accord. Dans les 58 cas pour lesquels la séance de médiation n'a pas pu avoir lieu en présence physique des participants (p. ex. en raison du grand nombre de participants à la procédure), la procédure n'a permis d'aboutir à une solution amiable que dans 20 cas (34 %).

En conclusion, nous pouvons dire que les procédures de médiation orales sont la base même des solutions amiables et profitent à tous les participants. De l'avis du Préposé fédéral, il conviendra de poursuivre dans cette voie, donc de les privilégier et de les promouvoir par rapport aux procédures écrites.

Note : toutes les recommandations émises durant l'année sous revue peuvent être consultées sur le site internet du Préposé fédéral (www.leprepose.ch)

Tableau 1 : Solutions amiables

2023	47%
2022 (impact du COVID-19)	51%
2021 (impact du COVID-19)	44%
2020 (impact du COVID-19)	34%
2019	61%
2018	55%

Durée des procédures de médiation

Le tableau ci-dessous compte trois parties correspondant à trois durées de traitement. Précisons que la durée pendant laquelle une procédure est suspendue à la demande des participants ou en accord avec eux n'est pas prise en compte. Il peut y avoir suspension notamment lorsque l'administration souhaite revoir sa position à l'issue d'une séance de médiation, ou lorsqu'elle doit procéder à la consultation de tiers concernés. Si la séance est reportée à la demande des participants (p. ex. pour cause de congés ou de maladie), la période qui s'étend entre la date initialement prévue et la nouvelle date – qui constitue la prolongation de la procédure en découlant – n'est pas non plus prise en compte dans la durée de traitement.

Le tableau montre que 27 % des procédures de médiation réglées en 2023 l'ont été dans le délai ordinaire de 30 jours, 35 % dans un délai compris entre 31 et 99 jours, et 38 % en 100 jours ou plus. À ce propos, il convient de relever que sur les 39 demandes en

médiation traitées dans les délais, 15 seulement (38%) ont abouti à un accord ou à une recommandation et ont donc donné lieu à un examen matériel de l'objet de la médiation. Dans les 24 autres cas (62%), il n'y a pas eu d'appréciation matérielle quant au fond, soit parce qu'il était évident que la loi sur la transparence ne s'appliquait pas, soit parce que les conditions formelles d'ouverture d'une procédure de médiation n'étaient pas remplies. Durant l'année sous revue, le retard dans le traitement des dossiers hérité des années précédentes s'est de nouveau traduit par un allongement de la durée des procédures. À cela s'ajoute le fait que le nombre des demandes entrantes est fluctuant. À titre d'exemple, durant les mois de mars (17), d'avril (15) et de novembre (15), de nombreuses demandes sont parvenues au Préposé, alors qu'en septembre il n'en a reçu que 5 et en août 2 seulement.

Avant la pandémie, le délai légal de 30 jours a été régulièrement respecté lorsque les séances de médiation se concluaient avec succès par un accord. Même si cela ne vaut pas pour l'année sous revue, nous constatons un taux légèrement supérieur à celui de l'année précédente : lorsque la procédure a abouti à un accord, le délai de 30 jours a pu être tenu dans 35 % des cas (contre 29 % l'année précédente). Cela est notamment dû au fait qu'en raison du personnel disponible pour le traitement des demandes en médiation et du retard dans le traitement des dossiers, les séances de médiation, dans 83 % des cas, ont dû être programmées de telle

sorte que le délai était déjà dépassé au moment où la séance a eu lieu. Lorsque le Préposé a été contraint, faute de solution amiable, de produire une recommandation, il a remis aux parties la recommandation écrite dans les trente jours ayant suivi la réception de la demande (délai légal) dans un cas seulement.

Les raisons les plus fréquentes pour lesquelles les délais ont été dépassés sont des demandes d'accès particulièrement volumineuses, un nombre important de tiers concernés impliqués dans la procédure ou la complexité juridique des questions. Ces motifs s'appliquent aux 54 cas dont le traitement a pris plus de 100 jours. Il s'agit par exemple des procédures de médiation concernant les contrats d'acquisition des vaccins COVID-19 ou la reprise de Credit Suisse par l'UBS (cf. à ce propos les recommandations du Préposé fédéral du 23 novembre 2023 et du 27 novembre 2023). Le traitement de ces cas nécessitant souvent un surcroît important de travail, le Pré-

Tableau 2 : Durée de traitement des procédures de médiation

Durée de traitement en jours	Période 2014 - août 2016*	Phase pilote 2017	Période 2018	Période 2019	Période 2020	Période 2021	Période 2022	Période 2023
30 jours maximum	11%	59%	50%	57%	43%	42%	25%	27%
de 31 à 99 jours	45%	37%	50%	38%	30%	51%	42%	35%
100 jours ou plus	44%	4%	0%	5%	27%	7%	33%	38%

*Source : présentation du Préposé, rencontre organisée pour les dix ans de la LTrans le 2 septembre 2016

posé peut – en vertu de l’art. 12a de l’ordonnance sur le principe de la transparence dans l’administration (OTrans ; RS 152.31) – prolonger le délai ordinaire d’une durée raisonnable. Un fait positif est à souligner : contrairement aux deux années précédentes, les demandes en médiation réglées en 2023 (142) ont été plus nombreuses que les demandes entrées (132).

Nombre de cas pendants

Les chiffres ci-dessous indiquent le nombre de cas pendants à la fin de chaque année. Au début du mois de

janvier 2024, il y avait 31 procédures de médiation pendants, dont 9 suspendues (1 de 2019, 1 de 2021, 2 de 2022 et 5 de l’année sous revue). 17 cas ont été clos avant la mise sous presse du présent rapport.

Tableau 3 : Procédures de médiation pendants

Fin 2023	31 (dont 17 terminées à la mise sous presse et 9 suspendues)
Fin 2022	41 (dont 16 terminées à la mise sous presse et 13 suspendues)
Fin 2021	27 (dont 14 terminées à la mise sous presse et 8 suspendues)
Fin 2020	17 (dont 9 terminées à la mise sous presse et 8 suspendues)
Fin 2019	43 (dont 40 terminées à la mise sous presse et 3 suspendues)
Fin 2018	15 (dont 13 terminées en février 2019 et 2 suspendues)

2.4 Processus législatif

FINANCES

Transposition de l'ordonnance de nécessité du CS dans la loi sur les banques

L'acquisition du Credit Suisse par l'UBS s'est faite en vertu du droit de nécessité du Conseil fédéral, qui a exclu de l'accès en vertu de la loi sur la transparence (LTrans) les documents officiels liés à cette acquisition. Au cours de la procédure législative ordinaire consécutive à l'acquisition, le Préposé fédéral s'est prononcé contre l'introduction d'une réglementation allant dans ce sens.

Face aux fortes turbulences des marchés auxquelles Credit Suisse a été confronté, le Conseil fédéral, s'appuyant directement sur la Constitution fédérale, a édicté le 16 mars 2023 l'ordonnance temporaire sur les prêts d'aide supplémentaires sous forme de liquidités et l'octroi par la Confédération de garanties du risque de défaillance pour les prêts d'aide sous forme de liquidités de la Banque nationale suisse (BNS) à des banques d'importance systémique. Sur cette base, le Conseil fédéral a adopté une série de mesures visant à stabiliser l'économie suisse et ouvrant la voie à l'acquisition de Credit Suisse par UBS. Ces mesures comprenaient des garanties de la Confédération et de la Banque

nationale pour un montant total de 209 milliards de francs. Conformément à cette ordonnance de nécessité, le droit d'accès des citoyens à ces informations et à ces données en vertu de la LTrans a alors été exclu. Le rapport explicatif précisait à ce sujet que la disposition mentionnée était une disposition spéciale primant sur la LTrans.

Dans le projet de modification de la loi sur les banques mis en consultation, le Secrétariat d'État aux questions financières internationales (SFI) a proposé, par le transfert du paquet d'urgence en une loi fédérale ordinaire, de maintenir l'exclusion de la LTrans. Le SFI justifiait le maintien de l'exclusion par le fait que les informations et les données fournies étaient de nature sensible et pourraient fréquemment contenir des secrets d'affaires ou de fabrication en vertu de la LTrans. En outre, l'exclusion de la LTrans entendait garantir, toujours selon le SFI, que les unités administratives chargées de l'exécution de l'ordonnance reçoivent rapidement

de la part des institutions financières concernées toutes les informations pertinentes. Pour des raisons identiques, le SFI envisageait d'introduire une autre exclusion de la LTrans à propos des informations relatives à l'octroi de garanties de risques de défaillance lors de transactions selon la loi sur la fusion.

Le PFPDT s'est opposé à toutes les exclusions de la LTrans proposées et a fait observer qu'outre les objections de droit intertemporel, la LTrans serait encore davantage vidée de sa substance si les citoyens se voyaient de nouveau privés, dans le domaine des aides financières, de l'accès général à des documents après l'avoir été déjà dans le cas de la loi sur le cautionnement solidaire COVID-19 (cf. 28^e RA, ch. 2.4), et du mécanisme de sauvetage du secteur de l'électricité (cf. 30^e RA, ch. 2.4).

Le Conseil fédéral a supprimé ces deux restrictions dans le projet mis en consultation ainsi que le demandait le Préposé fédéral. Ces exceptions au principe de transparence ne figurent plus dans le projet de modification de la loi sur les banques, actuellement entre les mains des commissions compétentes du Parlement fédéral.

Des développements plus détaillés sur l'exclusion du droit d'accès selon la LTrans par l'ordonnance d'urgence figurent dans les recommandations du PFPDT du 27 novembre 2023.

Révision partielle de l'ordonnance sur l'archivage

De l'avis des Archives fédérales, c'est au niveau de l'ordonnance que doit être réglée la coordination entre la loi sur l'archivage et la loi sur la transparence, ainsi que la question connexe de savoir lequel de ces deux actes législatifs doit être appliqué en cas de demande d'accès à des documents archivés en vertu de la loi sur la transparence. Le Préposé fédéral requiert pour sa part une adaptation de la loi sur l'archivage.

En 2022 déjà, dans le cadre de la consultation des offices sur la note de discussion concernant la nécessité d'une révision de la loi sur l'archivage, le Préposé fédéral avait souligné les vastes répercussions pratiques qu'ont la coordination entre la loi sur l'archivage (LAr) et la loi sur la transparence (LTrans), ainsi que la question – qui s'y rattache – du droit applicable durant le délai de protection en cas de demandes d'accès à des documents archivés selon la LTrans. Nous avons donc demandé que la coordination des deux lois fédérales soit réglée au niveau de la loi

(cf. 30^e RA, ch. 2.4). Les Archives fédérales ont tout d'abord rejeté cette demande comme étant prématurée.

Ensuite, bien que sachant que le Préposé avait opté pour une position contraire, le Conseil fédéral a décidé que la coordination devait se faire par une adaptation de l'ordonnance relative à la loi sur l'archivage (OLAr).

La réglementation élaborée par les Archives fédérales prévoyait l'introduction du principe de « l'application de la loi la plus favorable » selon lequel le régime d'accès le plus favorable au cas d'espèce (selon la LAr ou la LTrans) serait appliqué à l'examen de la requête. De l'avis des Archives fédérales, ce régime de coordination aurait dû être inscrit dans l'OLAr.

Au cours de la consultation préalable, le Préposé fédéral avait rappelé qu'il est parfois difficile, même impossible, d'analyser une demande et de déterminer la loi la plus favorable dans le cas concret. Les prescriptions formelles et matérielles de la LTrans et de la LAr présentant des différences importantes, une comparaison pourrait se heurter à des difficultés considérables. L'avant-projet ne précisait pas non plus si le requérant ou l'autorité déciderait quelle loi serait la plus favorable et quel droit régirait la procédure jusqu'à cette décision. Enfin, le libellé de la disposition proposée indiquait une simple application en alternance de la LTrans ou de la LAr, ce qui aurait probablement pour conséquence une limitation de l'une des deux lois.

De plus, le Préposé fédéral avait mis en doute la possibilité de refuser à un requérant, sur la base d'une disposition

d'ordonnance, l'examen en parallèle selon la LTrans et la LAr d'une décision de refus de l'autorité (dans le cadre de la procédure de recours). Pour conclure, il estimait que la disposition d'ordonnance proposée par les Archives fédérales serait impossible à appliquer dans la pratique et ne pourrait pas remplacer une coordination du droit sur l'archivage et du droit sur la transparence au niveau de la loi.

Par la suite, dans le projet de révision partielle de l'ordonnance relative à la loi sur l'archivage effectivement envoyé en consultation des offices, les Archives fédérales ont abandonné toute forme de réglementation de la coordination. En lieu et place, elles estiment que dans la poursuite de la pratique actuelle, il conviendra de recueillir des données fondées sur l'expérience quant à sa praticabilité et à son coût. Les Archives fédérales ont justifié leur position en invoquant les réactions au projet, dont celle du Préposé fédéral.

Ceci en dépit du fait que nous avons déclaré, au cours de la consultation des offices, que la poursuite de la pratique actuelle ne peut être considérée comme une solution de coordination appropriée car elle soulève un grand nombre de questions non résolues, de procédure et de fond.

Nouvelle loi fédérale sur la transparence des personnes morales

Avec une loi sur la transparence des personnes morales, un registre central doit être créé pour identifier les ayants droit économiques effectifs des personnes morales. Malgré l'intervention du PFPDT, le projet de loi prévoit une exclusion de la loi sur la transparence. Le 30 août 2023, le Conseil fédéral a mis en consultation le projet de loi fédérale sur la transparence des personnes morales et l'identification des ayants droit économiques (LTPM). Ce projet prévoit la création d'un registre fédéral regroupant des informations actuelles sur les ayants droit économiques des entités juridiques enregistrées, dans le but de renforcer le dispo-

sitif de lutte contre le blanchiment d'argent, le financement du terrorisme et la criminalité économique.

L'avant-projet du Secrétariat d'État aux questions financières internationales (SFI) détermine les autorités et les personnes qui auront accès à ce registre. Dans le rapport explicatif, le SFI explique que les tiers (non mentionnés) n'auront pas accès aux informations au motif qu'une plus grande ouverture du registre représenterait, compte tenu de son intérêt public limité, une atteinte disproportionnée au droit constitutionnel à une sphère privée et à la protection des données personnelles contre un emploi abusif. Le rapport explicatif initial précisait que les règles d'accès constitueraient des dispositions spéciales au sens de l'art. 4, let. b, de la loi sur la transparence, qui feraient que la LTrans ne s'appliquerait pas à l'accès à ces informations.

Lors de la consultation, le Préposé a défendu le point de vue selon lequel il ne s'agit pas là de dispositions spéciales réservées. L'objet de la réglementation serait bien plus le droit d'accès au registre et la communication des données qui s'y rattache, et donc, simplement, la création d'une base légale pour la communication de données au sens des art. 36 LPD et 57 rLOGA. De l'avis du Préposé, une remarque à ce sujet dans le rapport explicatif n'y change rien. Indépendamment de cela, le Préposé ne voit pas la nécessité de soustraire de manière générale et inconditionnelle les données du registre au

champ d'application de la LTrans puisque les exceptions prévues par celle-ci garantissent expressément la protection des intérêts privés des personnes concernées.

En fin de compte, la formulation selon laquelle les règles d'accès constituent des dispositions spéciales au sens de l'art. 4 LTrans a été abandonnée dans le rapport explicatif accompagnant le projet mis en consultation. Au grand regret du PFPDT, le Conseil fédéral a toutefois complété le projet de loi à la suite de la procédure de consultation par une exclusion explicite de la loi sur la transparence, selon laquelle celle-ci n'est pas applicable aux données du registre de transparence qui se rapportent à des personnes physiques ou morales. (cf. aussi ch. 1.3)

RÉGLEMENTATION DES ÉMOLUMENTS

La gratuité comme principe – Des émoluments en cas de charge de travail particulière

Le Parlement a adopté le principe de la gratuité de l'accès aux documents officiels et établi que des émoluments ne peuvent être perçus que si la demande d'accès nécessite un important surcroît de travail de la part de l'autorité. Le Conseil fédéral considère que plus de huit heures de travail constituent une charge de travail particulière. Le Préposé fédéral s'était prononcé en faveur d'un seuil de déclenchement plus élevé de l'obligation de redevance des émoluments.

En septembre 2022, le Parlement avait décidé que le principe de la gratuité de l'accès aux documents officiels remplace désormais le principe de la perception d'émoluments. Exceptionnellement une autorité peut percevoir des émoluments lorsqu'une demande d'accès nécessite un surcroît de travail important de sa part. Le législateur chargea alors le Conseil fédéral de régler, dans l'ordonnance sur la transparence, le nombre d'heures à partir duquel le traitement d'une demande d'accès nécessite un surcroît important de travail et peut donc donner lieu à la perception d'un émolument. Par ailleurs, le Conseil fédéral devait fixer le tarif des heures de travail fournies au-delà du seuil à partir duquel un émolument est demandé. De cette manière, la perception exceptionnelle d'un émolument

sera liée à un critère objectif – le temps de travail investi – et il devra être possible d'éviter des pratiques différentes en la matière au sein de l'administration fédérale.

Dans le cadre d'une consultation préalable du groupe de travail interdépartemental Transparence et de la consultation ultérieure des offices relative à la modification de l'ordonnance sur la transparence, l'Office fédéral de la justice proposa – outre des modifications rédactionnelles – un seuil de 30 heures de travail comme surcroît important de travail. Le Préposé fédéral souligna qu'avec le principe de l'accès gratuit, le législateur entendait réduire les litiges relatifs aux émoluments et favoriser la gratuité de la transparence de l'administration et qu'il considérait la modification de la loi comme un pas décisif vers le renforcement du principe de transparence. Il estimait acceptable le seuil de 30 heures. Tenant compte d'éventuelles demandes d'abaissement de ce seuil, il insista sur le fait que la solution du Conseil fédéral se devait de respecter la volonté du

législateur et que, par conséquent, l'abaissement de l'obligation de payer des émoluments ne devait pas entraîner une augmentation de la charge pour les requérants, les autorités et les tribunaux et, de ce fait, une transformation de la révision en son contraire.

Après réception des prises de position issues de la consultation des offices, l'OFJ a abaissé le seuil du surcroît de travail de 30 à 20 heures. Dans une prise de position ultérieure, le Préposé fédéral a fait remarquer que cet abaissement du seuil de surcroît de travail ne respectait pas la volonté du législateur.

En septembre 2023, le Conseil fédéral a choisi d'abaisser encore le seuil d'assujettissement à la redevance à 8 heures de travail. Au-delà de ce seuil, l'administration pourra facturer 100 francs par heure au requérant. Si un émolument est dû, le requérant devra en être informé au préalable.

L'émolument est réduit de 50 % si la demande d'accès émane d'un média. Dans le même temps, le Conseil fédéral a décidé que les autorités devront communiquer chaque année au Préposé fédéral à la protection des données non seulement le montant total des émoluments perçus au titre de l'accès aux documents officiels, mais aussi le nombre de cas où un émolument a été exigé. La nouvelle réglementation est entrée en vigueur le 1^{er} novembre 2023.

Avis du Conseil fédéral

Dans son rapport d'enquête sur les courriels introuvables au sein du Secrétariat général du Département fédéral de l'intérieur (SG-DFI), la Commission de gestion du Conseil des États (CdG-E) constate que les prescriptions en matière de classement et d'archivage ne sont pas uniformes à l'intérieur de l'administration fédérale et nécessitent une clarification. Selon ses conclusions, le droit de consulter les documents dont dispose le Préposé fédéral doit être renforcé. Elle estime par ailleurs que le Conseil fédéral devrait considérer la possibilité de conférer au Préposé fédéral dans la LTrans un droit d'intervention ou de décision lorsque son droit de consulter les documents n'est pas respecté. Le Conseil fédéral rejette un tel droit de décision, mais est prêt à examiner d'éventuels droits d'intervention.

Dans un article de presse du 14 juin 2022, il était fait état que dans le contexte de la tentative de chantage visant le conseiller fédéral Alain Berset, des courriels étaient introuvables ou auraient été effacés au sein du Secrétariat général du DFI (SG-DFI), et que cet état de fait faisait l'objet d'une procédure de médiation auprès du Préposé. La CdG-E a alors chargé sa sous-commission DFJP/ChF d'étudier, de manière générale et dans le cas concret, à quelles

règles obéissent la conservation et l'archivage des documents à l'intérieur de l'administration fédérale et quels documents doivent être rendus accessibles en application de la LTrans.

Dans son rapport d'enquête (« Archivage, classement de documents officiels et procédure à suivre en cas de demande d'accès selon la LTrans : Clarifications des prescriptions générales et dans le contexte des reproches des courriels introuvables au SG-DFI »), la CdG-E a examiné tout d'abord les bases légales de la conservation, du classement et de l'archivage des documents (en particulier loi sur l'archivage, LAr) et de l'accès aux documents officiels (loi sur la transparence, LTrans). Elle a relevé à cet égard que ces bases légales se distinguent non seulement par les termes utilisés, mais aussi par les objectifs, par l'objet de la réglementation et par le champ d'application, et qu'elles nécessitent donc une clarification.

Pour ce qui est du cas concret, la Commission relève qu'il n'a pas été possible de déterminer avec certitude dans quelle mesure les courriels introuvables ont existé et si une partie d'entre eux pourrait avoir été détruite.

Selon la Commission, il faut considérer que les courriels en question n'étaient pas seulement de nature privée, mais qu'ils avaient également un lien avec la fonction de chef de département.

Dans son rapport, la CdG-E est très claire sur le fait que la conservation et l'archivage de documents, ainsi que la garantie du droit d'accès aux documents de l'administration fédérale sont essentiels quant à la traçabilité et à la transparence de l'activité administrative. La Commission estime par ailleurs qu'en refusant au Préposé fédéral l'accès à ces documents, le SG-DFI n'a pas respecté les obligations légales qui lui incombent en vertu de la LTrans. Elle souligne qu'en procédure de médiation en vertu de la LTrans, le droit de consulter les documents qui revient au Préposé fédéral revêt un caractère central pour qu'il puisse évaluer si des documents ou des courriels ont valeur de documents officiels. Si les autorités lui refusent cet accès, le Préposé fédéral ne peut pas remplir correctement son mandat légal de médiation. De ce fait, la Commission estime nécessaire que le Préposé fédéral ait accès à tous les documents afin qu'il soit en mesure d'évaluer si les documents et les dossiers présentent un caractère officiel. La Commission estime que cette situation – dans laquelle le Préposé fédéral se voit refuser, dans une procédure de médiation, l'accès à des documents contestés – est insatisfaisante et demande expressément au Conseil fédéral d'examiner

une modification de la LTrans visant à conférer au Préposé fédéral un droit d'intervention ou de décision.

Le rapport de la CdG-E, publié en octobre 2023, renferme cinq recommandations au Conseil fédéral, dont trois présentent un lien direct avec la LTrans :

- Dans la recommandation 1, le Conseil fédéral est invité à examiner s'il est nécessaire de modifier les dispositions légales relatives au droit de consultation des documents qui ont un lien tant avec la fonction qu'avec la sphère privée, notamment en ce qui concerne les magistrats.
- Dans la recommandation 4, le Conseil fédéral est invité à examiner si la LTrans s'applique ou devrait s'appliquer aussi aux procédures closes et, le cas échéant, s'il y a lieu de préciser ce point lors de la prochaine révision de la loi.
- Dans la recommandation 5, le Conseil fédéral est invité à examiner l'opportunité d'une modification de la LTrans conférant au Préposé fédéral un droit d'intervention ou de décision lorsque son droit de consulter les documents n'est pas respecté.

La CdG-E a demandé au Conseil fédéral à se prononcer sur ce rapport. L'Office fédéral de la justice (OFJ) a procédé à la consultation des offices concernant la position du Conseil fédéral sur le rapport de la CdG-E. Le projet de réponse prévoyait que le Conseil fédéral donne pleinement suite aux recommandations 1-4, mais seulement en partie à la recommandation 5.

À propos de la recommandation 5, il a été proposé que le Conseil fédéral se déclare d'accord avec un examen du droit d'intervention du Préposé fédéral uniquement pour le cas où son droit de consultation est refusé, mais rejette le droit de décision. Selon le motif invoqué, la procédure de médiation selon la LTrans est une procédure informelle, qui ne crée pas de précédent et ne donne lieu à aucun procès-verbal, et de ce fait une compétence décisionnelle du Préposé fédéral n'est pas conforme au système. Le Préposé a rétorqué que le souhait explicite de la CdG-E était d'une part d'examiner l'octroi d'un droit d'intervention et d'autre part d'inclure, dans le cadre de cet examen, la question d'un droit de décision spécifique du PFPDT, au lieu de l'exclure d'emblée en anticipant des réponses matérielles.

Cette restriction injustifiée ne permettrait plus d'effectuer l'examen ouvert souhaité par la CdG-E. Pour ces raisons, le Préposé fédéral a proposé l'adoption sans condition de la recommandation 5.

L'OFJ a rejeté cette proposition et maintenu l'acceptation partielle de la recommandation 5 par le Conseil fédéral : les résultats de la consultation des offices ont confirmé cette position, car les autres participants étaient d'accord avec la procédure proposée par l'OFJ ou avaient même proposé de rejeter entièrement la recommandation 5.

Dans sa réponse du 10 janvier 2024 à l'intention de la CdG-E, le Conseil fédéral rejette l'octroi d'un droit de décision au Préposé fédéral : en revanche, il accepte pleinement les autres recommandations de la CdG-E. Il a en outre chargé le DFJP d'examiner ces recommandations d'ici la fin de l'année 2024 et de lui soumettre des propositions quant à la suite de la procédure.

2.5 Dispositions spéciales réservées au sens de l'art. 4 LTrans

La LTrans nécessite une coordination avec les dispositions spéciales d'autres lois fédérales, qui prévoient des règles particulières d'accès aux documents officiels. L'art. 4 LTrans précise que les dispositions spéciales d'autres lois fédérales qui déclarent certaines informations

secrètes (let. a) ou qui déclarent certaines informations accessibles, à des conditions dérogeant à la LTrans (let. b), sont réservées, ce qui fait que les dispositions de la LTrans ne s'appliquent pas à l'accès aux informations en question.

Pour déterminer si une disposition légale a la priorité au sens d'une disposition spéciale selon l'art. 4 LTrans, il convient d'interpréter les normes concernées dans chaque cas concret.

Tableau 4 : Dispositions spéciales au sens de l'art. 4 LTrans

Acte (titre court) et abréviation	RS	Disposition	Date d'entrée en vigueur
Loi sur la sécurité de l'information (LSI)	128	Art. 4 al. 1 bis	(ouvert)
Message relatif à la modification de la loi sur l'assurance maladie (2 ^e volet de mesures visant à maîtriser les coûts)	832.10	Art. 52c al. 1 et 2 P-LAMal Art. 52d al. 4 P-LAMal Disposition transitoire III, al. 5 P-LAMal	Message du 7 septembre 2022 (Etat : consultation au Parlement)
	831.20	Art. 14quinquies al. 3 P-LAI Disposition transitoire P-LAI	
Loi fédérale sur des aides financières subsidiaires destinées au sauvetage des entreprises du secteur de l'électricité d'importance systémique (LFiEl)	734.91	Art. 20 al. 4	1 ^{er} octobre 2022
Loi fédérale sur les marchés publics (LMP)	172.056.1	Art. 48, al. 1 (accès exprès imposé) Art. 11, let. e (n'est réputé disposition spéciale que pendant la procédure d'adjudication)	1 ^{er} janvier 2021
Loi sur les cautionnements solidaires liés au COVID-19 (LCaS-COVID-19)	951.26	Art. 12 al. 2	19 décembre 2020
Loi fédérale sur l'organisation de l'infrastructure ferroviaire (acte modificateur unique)			
Loi fédérale sur les chemins de fer (LCdF)	742.101	Art. 14 al. 2	1 ^{er} juillet 2020
Loi sur les installations à câbles (LICa)	743.01	Art. 24e	1 ^{er} juillet 2020
Loi sur le transport de voyageurs (LTV)	745.1	Art. 52a	1 ^{er} juillet 2020
Loi fédérale sur la navigation intérieure (LNI1)	747.201	Art. 15b	1 ^{er} juillet 2020
Loi fédérale sur le renseignement (LRens)	121	Art. 67	1 ^{er} septembre 2017
Loi sur les denrées alimentaires (LDA1)	817.0	Art. 24 Disposition spéciale selon le message du 25 mai 2011 relatif à la LDA1	1 ^{er} mai 2017
Loi fédérale sur l'encouragement de la recherche et de l'innovation (LERI)	420.1	Art. 13, al. 4 (cf. Arrêt du TAF A-6160/2018 du 4 novembre 2019 consid. 4)	1 ^{er} janvier 2014
Loi sur les banques (LB)	952.0	Art. 47 al. 1	1 ^{er} janvier 2009 (let. a et b) et 1 ^{er} juillet 2015 (let. c)
Loi sur les brevets (LBI)	232.14	Art. 90 OBI s'appuyant sur l'art. 65, al. 2, LBI	1 ^{er} juillet 2008
Ordonnance sur les brevets (OBI)	232.141	(cf. Arrêt du TF 4A_249/2021 du 10 juin 2021)	

Acte (titre court) et abréviation	RS	Disposition	Date d'entrée en vigueur
Entrée en vigueur de la LTrans			1 ^{er} juillet 2006
Loi sur le Parlement (LParl)	171.10	Art. 47, al. 1 (cf. Arrêt du TAF A-6108/2016 du 28 mars 2018 consid. 3.1)	1 ^{er} décembre
Loi sur le contrôle des biens (LCB)	946.202	Art. 4 et 5 (cf. Arrêt du TAF A-5133/2019 du 24 novembre 2021 consid. 5.3.2.4)	1 ^{er} octobre 1997
Loi fédérale sur l'impôt fédéral direct (LFID)	642.11	Art. 110 al. 1	1 ^{er} janvier 1995
Loi fédérale sur l'impôt anticipé (LIA)	642.21	Art. 37 als. 1	1 ^{er} janvier 1967
Loi fédérale sur les droits de timbre (LT)	641.10	Art. 33 al. 1	1 ^{er} juillet 1974
Loi sur la TVA (LTVA)	641.20	Art. 74 al. 1	1 ^{er} janvier 2010
Loi fédérale sur l'harmonisation des impôts directs des cantons et des communes (LHID)	642.14	Art. 39 al. 1 (cf. JAAC 2016.1 (p. 1 - 14), édition du 26 janvier 2016 : Secret fiscal et accès à des documents officiels)	1 ^{er} janvier 1993
Loi sur la statistique fédérale (LSF)	431.01	Art. 14 (cf. Arrêt du TF 1C_50/2015 du 2 décembre 2015 consid. 4.2 ss)	1 ^{er} août 1993

(Liste non exhaustive)

Tableau 5 : Dispositions ne constituant pas des dispositions spéciales au sens de l'art. 4 LTrans

Acte (titre court) et abréviation	RS	Disposition	Date d'entrée en vigueur
Loi sur la sécurité des produits (LSPro)	930.11	Art. 10, al. 4, en relation avec l'art. 12 (cf. Arrêt du TF 1C_299/2019 du 7 avril 2020 consid. 5.5)	1 ^{er} juillet 2010
Loi sur la surveillance de la révision (LSR)	221.302	Art. 19, al. 2 (cf. Arrêt du TF 1C_93/2021 du 6 mai 2022 consid. 3.6)	1 ^{er} septembre 2007
Loi sur les télécommunications (LTC)	784.10	Art. 24f (cf. Arrêt du TAF A-516/2022 du 12 septembre 2023 consid. 6.5)	1 ^{er} avril 2007
Loi fédérale sur la partie générale du droit des assurances sociales (LPGA)	830.1	Art. 33 (ne constitue pas une disposition spéciale au sens de l'art. 4 LTrans dans ce cas particulier : cf. Arrêts du TAF A-5111/2013 du 6 août 2014 consid. 4.1 ss; A-4962/2012 du 22 avril 2013 consid. 6.1.3)	1 ^{er} janvier 2003
Loi sur les produits thérapeutiques (LPTh)	812.21	Art. 61 et 62 (cf. Arrêt du TF 1C_562/2017 du 2 juillet 2018 consid. 3.2; arrêt du TAF A-3621 / 2014 du 2 septembre 2015 consid. 4.4.2.3 ss)	1 ^{er} janvier 2002
Loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité (LPP)	831.40	Art. 86 (cf. Arrêt du TF 1C_336/2021 du 3 mars 2022 consid. 3.4.3)	1 ^{er} janvier 2001

(Liste non exhaustive)

Le PFPDT

3.1 Prestations et ressources

Prestations et ressources dans le domaine de la protection des données

Effectifs

Comme mentionné dans notre dernier rapport d'activités, le PFPDT a recruté et intégré dans les temps les collaborateurs et collaboratrices supplémentaires prévus par le Conseil fédéral dans son message concernant la révision totale de la LPD, ceci avant son entrée en vigueur qui a eu lieu le 1^{er} septembre 2023 (cf. 30^e RA, ch. 3.1). Les effectifs dédiés à la protection des données sont donc demeurés stables avec 33 postes à plein temps.

Tableau 6 : Postes pouvant être affectés aux questions relatives à la LPD

2005	22
2010	23
2018	24
2019	24
2020	27
2021	27
2022	27
2023	33
2024	33

Prestations

En tant qu'autorité de protection des données compétente pour les organes fédéraux et le secteur privé, les tâches du PFPDT sont affectées, conformément au nouveau modèle de gestion de l'administration fédérale (NMG), à quatre groupes de prestations : Conseils, Surveillance, Information et Législation. Au cours de l'année de référence allant du 1^{er} avril 2023 au 31 mars 2024, les ressources en personnel dont dispose le PFPDT pour la protection des données ont été réparties entre ces groupes de la manière suivante :

Tableau 7 : Prestations Protection des données

Conseil Confédération	15,7%	
Conseil Secteur privé	20,8%	
Collab. avec les autorités étrangères	15,9%	
Collab. avec les cantons	0,9%	
Total Conseils		53,3%
Surveillance	15,5%	
Certification	0,0%	
Registre des données	0,2%	
Total Surveillance		15,7%
Information	14,4%	
Formation / Conférences	3,4%	
Total Information		17,8%
Législation	13,2%	
Total Législation		13,2%
Total Protection des données		100,0%

Conseil

Dans le domaine des prestations de conseils, le PFPDT est confronté à une demande élevée et constante du fait de son obligation légale d'accompagner les grands projets numériques. Les ressources en personnel consacrées au groupe Conseil ont atteint environ 53,3% au cours de l'année sous revue, ce qui est légèrement supérieur aux chiffres de l'année précédente (52,5%). À la fin de l'année sous revue, les conseils relevant du droit de la surveillance de 10 grands projets étaient en cours. 4 de ces projets portent sur la transformation numérique de l'administration fédérale. Le nombre des demandes et dénonciations a augmenté de presque 1000 par rapport à la période précédente, passant de 4091 à 5074. Chaque mois, les trois équipes du domaine de direction Protection des données ont répondu par une lettre standard à en moyenne 51 demandes et dénonciations de citoyens.

Les traitements numériques de données et le recours à l'intelligence artificielle (IA) s'imposent de plus en

plus, que ce soit dans l'économie privée ou dans l'administration fédérale, contribuant ainsi à l'augmentation du nombre des grands projets de traitements de données.

Tableau 8 : Conseils portant sur de grands projets en 2023

Droits fondamentaux	1
Législation nouvelle LPD	4
Transports	1
Santé	2
Police et justice	2
Total	10

Surveillance

Le dynamisme des applications fondées sur l'informatique en nuage et sur l'intelligence artificielle impose une exécution rapide des contrôles. Les adaptations des programmes et des conditions d'utilisation étant de plus en plus fréquentes et l'association des compétences juridiques et techniques étant devenue indispensable, le PFPDT doit si possible éviter les temps d'arrêt dans les procédures d'établissement des faits en réservant davantage de collaborateurs pour les contrôles très poussés. Au cours de la période sous revue, la part des ressources pouvant être affectées aux contrôles et aux procédures de surveillance était de 15,7 %, ce qui correspond à la valeur moyenne

basse des années de référence depuis 2015 ; ces ressources ont permis d'effectuer douze contrôles approfondis au cours de cette même période.

Si le personnel supplémentaire a été tout d'abord affecté de manière significative aux travaux d'introduction du nouveau droit, à l'avenir il devra être principalement chargé des tâches de surveillance. Ce faisant, le PFPDT entend augmenter progressivement la densité des contrôles concernant les organes fédéraux et quelque 12 000 grandes et moyennes entreprises commerciales, ainsi qu'environ 10 000 fondations et associations suisses.

Législation

Les changements que la transformation numérique des offices fédéraux implique au niveau des traitements de données doivent reposer sur des bases légales. Ils nécessitent donc un grand nombre de nouvelles dispositions, ou de révisions, du droit fédéral sur lesquelles le PFPDT est appelé à se prononcer dans diverses procédures de

consultation. Au cours de l'année sous revue, nous avons participé à 297 consultations des offices.

Information

Considérant l'entrée en vigueur désormais effective de la nouvelle LPD et de son ordonnance d'exécution, d'importants travaux préparatoires et des formations internes et externes ont été menés. Toutefois, les ressources affectées au groupe de prestations Information ont pu être diminuées de manière significative au cours de l'année sous revue, passant de 22,2 % à 17,8 %.

Participation aux délibérations de commissions et auditions par les commissions parlementaires

Durant la période sous revue, le PFPDT a participé comme suit aux délibérations de commissions et aux auditions par les commissions parlementaires :

- Avril 2023 : sous-commissions CDF-E et CDF-N sur les comptes 2022
- Avril 2023 : CIP-N sur l'exclusion de la LTrans par le droit de nécessité
- Avril 2023 : CIP-N sur l'initiative parlementaire Bendahan
- Avril 2023 : CAJ-N sur les répercussions du projet législatif de la Commission européenne sur le contrôle des messageries instantanées
- Mai 2023 : CIP-N sur l'exclusion de la LTrans par le droit de nécessité

- Mai et novembre 2023 : CIP-N sur l'introduction du droit à l'intégrité numérique dans la Constitution
- Mai 2023 : CER-N sur la loi sur les douanes
- Juillet, octobre et novembre 2023 : CIP-E sur la loi fédérale sur le système national de consultation des adresses des personnes physiques (loi sur le service national des adresses)
- Octobre 2023 : CIP-E sur la loi fédérale sur l'assurance-maladie. Modification (Mesures visant à freiner la hausse des coûts – 2^e volet)
- Octobre 2023 : sous-commissions CDF-E et CDF-N sur le budget 2024
- Novembre 2023 : Commission judiciaire
- Janvier 2024 : CIP-N sur la loi fédérale sur le système national de consultation des adresses des personnes physiques (loi sur le service national des adresses)
- Janvier et février 2024 : CAJ-N sur la loi fédérale sur l'identité électronique et autres moyens de preuves électroniques (loi sur l'e-ID)
- Mars 2024 : CAJ-E sur la loi fédérale sur l'identité électronique et autres moyens de preuves électroniques (loi sur l'e-ID)

Prestations et ressources dans le domaine de la loi sur la transparence

Les effectifs engagés pour les médiations et les recommandations en vertu de la loi sur la transparence demeurent constants avec 6 postes à plein temps. Le PFPDT continuera à œuvrer pour que les retards de traitement dus à la pandémie et au nombre constamment élevé de demandes en médiation soient progressivement résorbés au cours des prochains exercices. L'évolution du nombre des demandes en médiation et leur complexité déterminera si et à quelle vitesse cela peut se faire.

Compte tenu de ces éléments, le PFPDT a défini pour chaque groupe de prestations les objectifs suivants, déterminants pour le calcul des ressources :

Tableau 9 : Objectifs du PFPDT

Groupe de prestations	Objectifs
Conseil	Le PFPDT développe une présence adaptée aux attentes pour les conseils aux particuliers et pour l'accompagnement des projets de l'économie et des autorités fédérales.
Surveillance	Le PFPDT développe une densité plausible des contrôles.
Information	Le PFPDT sensibilise le public de manière proactive aux risques du numérique liés aux technologies et aux applications. Il met à sa disposition un site internet moderne et facile d'accès et des portails numériques de notification.
Législation	Le PFPDT exerce une influence précoce et active sur toutes les normes et les réglementations spéciales relatives à la protection des données qui sont élaborées sur les plans national et international. Il aide les milieux concernés à formuler des règles de bonnes pratiques.

Le PFPDT améliore son autocontrôle

L'entrée en vigueur de la nouvelle loi sur la protection des données a permis de renforcer l'autocontrôle concernant le respect et la bonne application des dispositions fédérales de protection des données au sein de l'institution du PFPDT en tant qu'autorité : le PFPDT a introduit deux nouveaux postes à temps partiel, à savoir un responsable de la protection des données et un responsable de la sécurité informatique.

L'autocontrôle a pour but de garantir, par des mesures appropriées, le respect et la bonne application des dispositions fédérales de protection des données au sein de notre autorité. Cette tâche, bien qu'ayant été déjà concrétisée avant l'entrée en vigueur de la nouvelle loi sur la protection des données, a été depuis attribuée à deux fonctions formellement indépendantes appartenant à notre autorité : le conseiller à la protection des données (data protection officer DPO) et le délégué à la sécurité informatique de l'unité organisationnelle (DSIO).

Le conseiller à la protection des données du PFPDT a pour tâche de répondre aux demandes d'information et d'examiner les traitements de données

personnelles effectués par le PFPDT en tant qu'autorité, et de recommander des mesures correctives lorsqu'une violation des prescriptions en matière de protection des données a été constatée. Il suit en outre l'examen, l'application et la mise à jour des règlements de traitement.

Le délégué à la sécurité informatique de l'unité organisationnelle du PFPDT est la personne de contact du DSIO de la Chancellerie fédérale qui est responsable de la sécurité informatique de toutes les infrastructures et applications qu'elle exploite pour le PFPDT. Au sein de notre organisation, le DSIO est le point de contact central en ce qui concerne les questions de sécurité des données. Il contrôle aussi l'élaboration et la mise en œuvre des directives de la Chancellerie fédérale en matière de sécurité des données touchant le PFPDT et participe à l'élaboration des mesures de sensibilisation.

3.2 Communication

Nouveau site internet et portails de notification

Le nouveau site internet et la nécessité d'adapter les contenus à la LPD révisée a encore beaucoup mobilisé l'équipe du PFPDT chargée de la communication pendant l'année sous revue. Depuis son lancement réussi le 11 mai 2023, le site a été enrichi régulièrement, notamment par des informations et des guides relatifs aux nouvelles dispositions légales. Les trois nouveaux portails de notification et les différents formulaires de contact proposés rencontrent un grand succès et simplifient grandement les contacts entre les usagers (particuliers, responsables du traitement) et le PFPDT (cf. aussi Accent I).

En chiffres

Avec 6 communiqués de presse et 18 messages brefs, le PFPDT s'est adressé au public en moyenne deux fois par mois, soit pour faire le point sur des procédures achevées ou en cours (procédures d'établissement des faits selon l'ancien droit et enquêtes selon le nouveau), soit pour communiquer sur des

sujets importants touchant à la protection des données ou sur des événements traités dans le débat public. Il s'est aussi exprimé sur la loi sur la transparence, en plus des 45 recommandations publiées en 2023 : l'exclusion de la loi sur la transparence par une ordonnance de nécessité dans le cas de Credit Suisse rappelle les décisions relevant du droit de nécessité prises pendant la pandémie de COVID-19 et soulève des questions juridiques de fond.

Autres thèmes

Le PFPDT s'est intéressé de près aux projets de numérisation de l'administration fédérale : notamment la tentative de sauvetage, toujours en cours, des données relatives aux vaccins de la plateforme mesvaccins.ch (cf. ch. 1.4) et l'intégration prévue de ces données

dans le dossier électronique du patient (DEP), la création d'un moyen d'identification électronique (e-ID) reconnu par l'État, ou encore la stratégie d'informatique en nuage de la Confédération avec le passage à Microsoft 365, qui nécessite l'adoption du nuage public d'un grand groupe américain. Le PFPDT suit de près les grands projets numériques de la Confédération et donne son avis comme organe de surveillance afin que le droit de la protection des données soit respecté (cf. ch. 1.1).

La cybersécurité continue de faire l'objet d'une grande attention. Les médias rapportent chaque jour des cas d'accès non autorisés à des données. Lorsqu'un cyber-incident se produit en Suisse, le PFPDT est souvent prié de fournir une appréciation. S'agissant du piratage de l'entreprise Xplain, le PFPDT a ouvert une enquête contre l'Office fédéral de la police (fedpol) et l'Office fédéral des douanes et de la sécurité des frontières (OFDF) pour cause de soupçons de violation potentiellement grave des dispositions de protection des données, enquête qu'il a étendue peu de temps après à l'entreprise concernée (cf. ch. 1.2). Au cours de l'année sous revue, le PFPDT a aussi

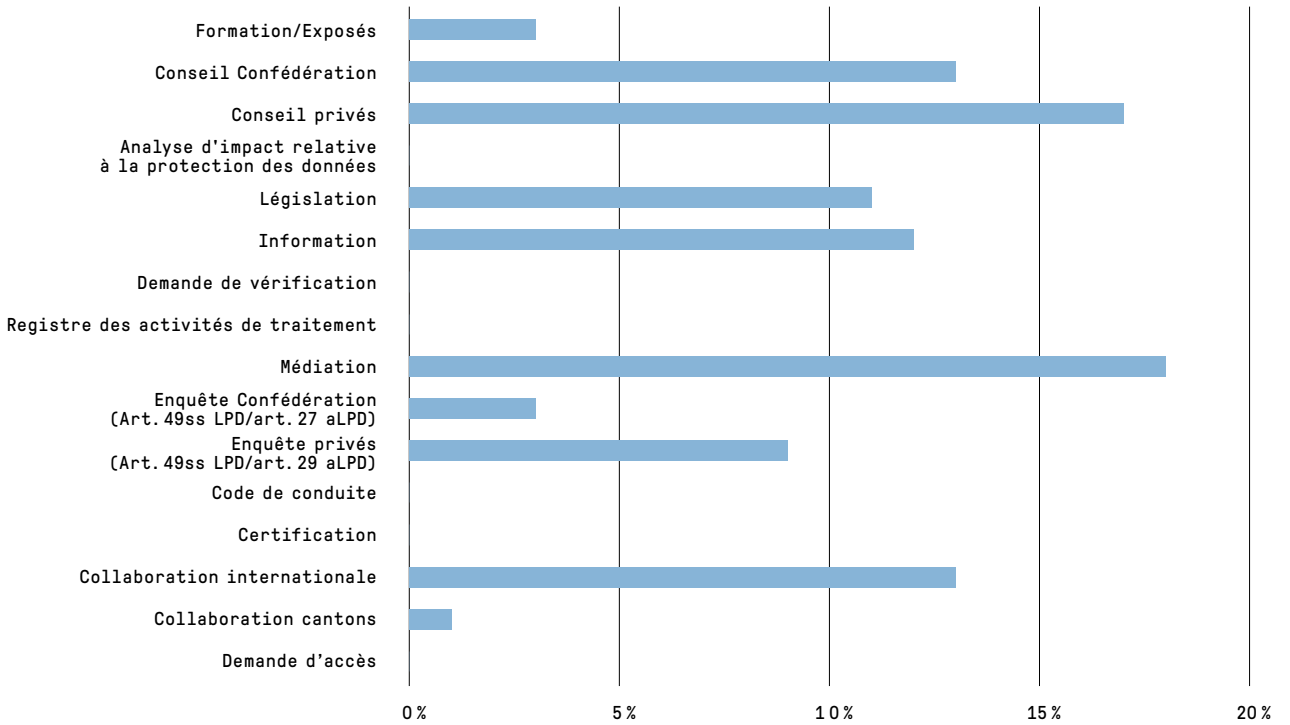
reçu de nombreuses demandes portant sur le phénomène en pleine expansion de l'intelligence artificielle (IA). Le recours de plus en plus fréquent à des applications fondées sur l'IA suscite une certaine inquiétude dans la population et la veille média montre que la crainte d'une surveillance généralisée – dans l'espace public (gares, etc.), dans les magasins voire dans les chambres à coucher lorsque les applications de santé enregistrent le temps de repos – augmente. L'essor de l'IA aggrave aussi le risque de désinformation. Les fausses informations trompent les utilisateurs de services en ligne et perturbent la formation de l'opinion. Les risques d'usurpation d'identité sont eux aussi en augmentation.



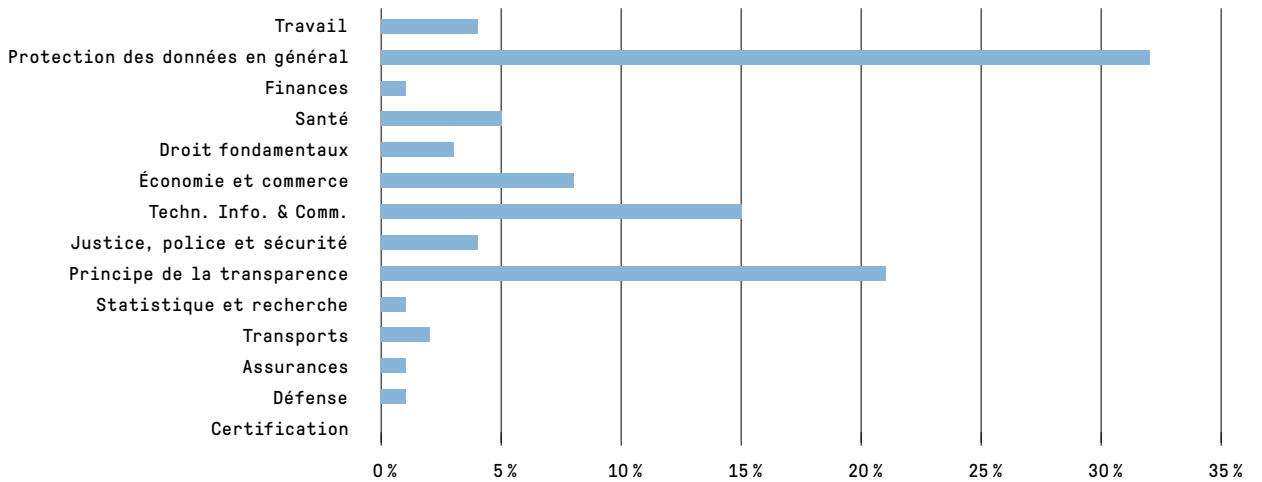
3.3 Statistiques

Statistiques des activités du PFPDT du 1^{er} avril 2023 au 31 mars 2024 (Protection des données)

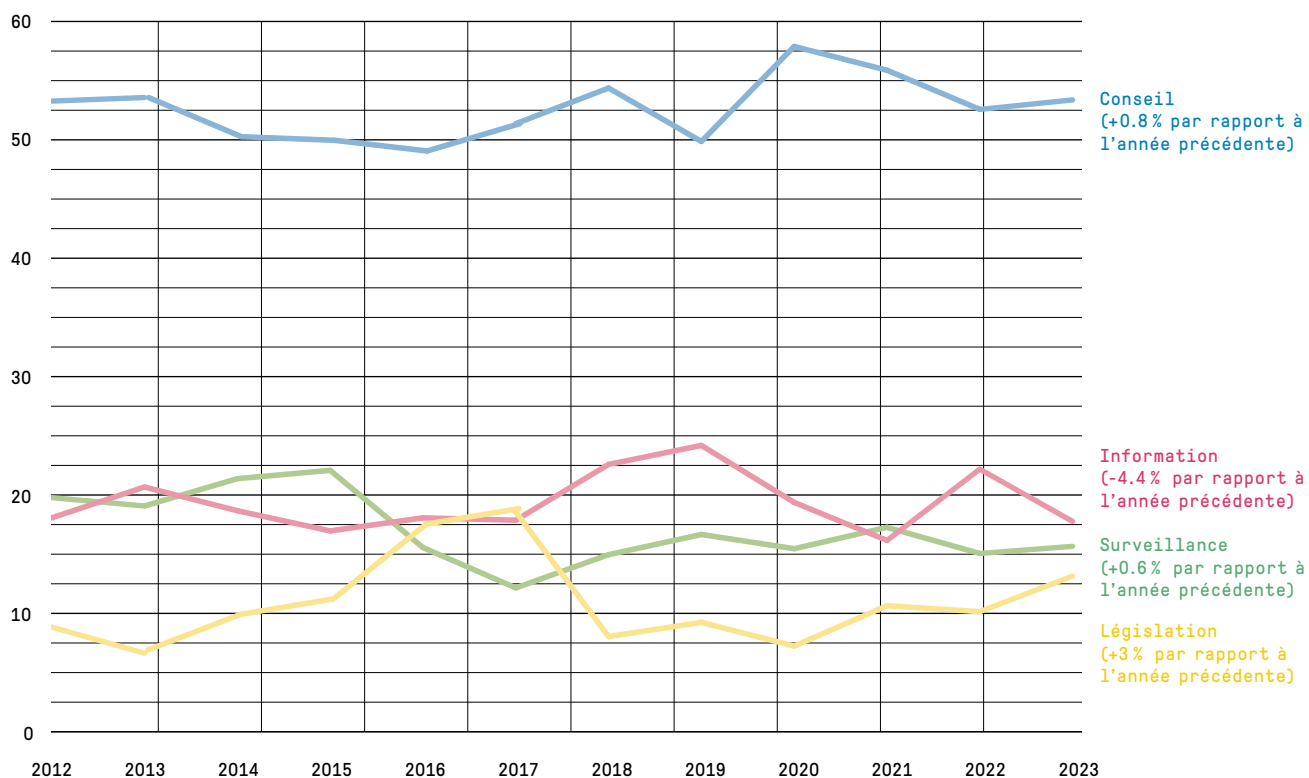
Charge de travail par tâche



Charge de travail par domaine



Comparaison pluriannuelle
(en pourcentage)



Vue d'ensemble des demandes d'accès selon la loi sur la transparence du 1^{er} janvier au 31 décembre 2023

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
ChF	90	43	21	18	0	5	3
DFAE	228	87	23	62	5	18	33
DFI	230	81	16	67	25	26	15
DFJP	152	80	14	27	9	5	17
DDPS	432	309	9	72	6	9	27
DFP	191	52	41	63	9	14	12
DEFR	175	80	27	39	5	6	18
DETEC	236	97	24	54	14	13	34
MPC	2	1	0	0	0	0	1
SP	2	0	1	0	0	0	1
Total 2023 (%)	1738 (100)	830 (48)	176 (10)	402 (23)	73 (4)	96 (6)	161 (9)
Total 2022 (%)	1180 (100)	624 (53)	99 (8)	236 (20)	53 (5)	69 (6)	99 (8)
Total 2021 (%)	1385 (100)	694 (50)	126 (9)	324 (23)	48 (4)	78 (6)	115 (8)
Total 2020 (%)	1193 (100)	610 (51)	108 (9)	293 (24)	35 (3)	80 (7)	67 (6)
Total 2019 (%)	916 (100)	542 (59)	86 (9)	171 (19)	38 (4)	43 (5)	36 (4)
Total 2018 (%)	647 (100)	355 (55)	66 (10)	119 (18)	24 (4)	50 (8)	33 (5)
Total 2017 (%)	586 (100)	325 (56)	108 (18)	106 (18)	21 (4)	26 (4)	-
Total 2016 (%)	554 (100)	299 (54)	88 (16)	105 (19)	29 (5)	33 (6)	-
Total 2015 (%)	600 (100)	320 (53)	99 (17)	128 (21)	31 (5)	22 (4)	-
Total 2014 (%)	582 (100)	302 (52)	124 (21)	124 (21)	15 (3)	17 (3)	-
Total 2013 (%)	470 (100)	218 (46)	123 (26)	103 (22)	18 (4)	8 (2)	-

Statistique des demandes d'accès selon la loi sur la transparence du 1^{er} janvier au 31 décembre 2023

		Nombre de demandes d'accès	dont soumis les années précédentes	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Chancellerie fédérale ChF	ChF	76	0	33	20	18	0	2	3
	DFPDT	14	0	10	1	0	0	3	0
	Total	90	0	43	21	18	0	5	3
Département fédéral des affaires étrangères DFAE	DFAE	228	0	87	23	62	5	18	33
	Total	228	0	87	23	62	5	18	33
Département fédéral de l'intérieur DFI	SG DFI	19	0	5	4	3	5	0	2
	BFEG	3	0	2	0	0	0	1	0
	OFC	7	2	6	0	1	0	0	0
	AFS	1	1	1	0	0	0	0	0
	MétéoSuisse	0	0	0	0	0	0	0	0
	BN	0	0	0	0	0	0	0	0
	OFSP	76	4	21	3	28	8	15	1
	OFS	10	0	7	1	0	0	1	1
	OFAS	10	0	9	0	0	0	0	1
	OSAV	33	0	13	3	10	3	1	3
	MNS	0	0	0	0	0	0	0	0
	SWISS MEDIC	67	3	13	5	25	9	8	7
	SUVA	4	0	4	0	0	0	0	0
	compenswiss	0	0	0	0	0	0	0	0
	Total	230	10	81	16	67	25	26	15
Département fédéral de justice et police DFJP	SG DFJP	15	0	9	0	2	0	2	2
	OFJ	34	0	20	5	2	0	0	7
	FEDPOL	13	0	2	6	2	1	0	2
	METAS	3	0	2	1	0	0	0	0
	SEM	70	0	36	0	20	8	3	3
	Service SCPT	3	0	0	0	1	0	0	2
	ISDC	8	0	5	2	0	0	0	1
	IPI	4	0	4	0	0	0	0	0
	CFMJ	2	0	2	0	0	0	0	0
	CAF	0	0	0	0	0	0	0	0
	ASR	0	0	0	0	0	0	0	0
	CSI	0	0	0	0	0	0	0	0
	CNPT	0	0	0	0	0	0	0	0
	Total	152	0	80	14	27	9	5	17

		Nombre de demandes d'accès	dont soumis les années précédentes	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Département fédéral de la défense, de la protection de la population et des sports DDPS	SG DDPS	83	2	17	5	41	4	5	11
	Défense	17	0	3	1	2	1	2	8
	SRC	31	0	3	2	19	0	1	6
	AS-Rens	1	0	0	1	0	0	0	0
	armasuisse	8	0	2	0	4	0	1	1
	OFSPD	277	0	276	0	0	1	0	0
	OFPP	8	0	5	0	3	0	0	0
	swisstopo	7	0	3	0	3	0	0	1
	OAC	0	0	0	0	0	0	0	0
	Total	432	2	309	9	72	6	9	27
Département fédéral des finances DFF	SG DFF	87	0	18	24	31	4	3	7
	AFF	10	0	4	1	3	1	0	1
	OPPER	3	0	2	0	0	0	0	1
	AFC	24	0	10	5	6	2	0	1
	OFDF	31	7	3	7	14	0	6	1
	OFCL	7	3	7	0	0	0	0	0
	OFIT	6	0	0	0	5	1	0	0
	CDF	6	0	3	1	2	0	0	0
	SFI	14	0	3	2	2	1	5	1
	PUBLICA	1	0	0	1	0	0	0	0
	DdC	2	0	2	0	0	0	0	0
	Total	191	10	52	41	63	9	14	12

		Nombre de demandes d'accès	dont soumis les années précédentes	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Département fédéral de l'économie, de la formation et de la recherche DEFR	SG DEFR	11	0	1	3	4	0	0	3
	SECO	47	2	7	13	20	0	2	5
	SEFRI	7	0	3	0	1	1	0	2
	OFAG	16	0	11	0	2	0	2	1
	Agroscope	0	0	0	0	0	0	0	0
	OFAE	7	2	2	1	2	1	0	1
	OFL	3	0	2	0	1	0	0	0
	SPR	10	0	2	2	6	0	0	0
	COMCO	18	1	9	6	1	2	0	0
	CIVI	0	0	0	0	0	0	0	0
	BFC	1	0	1	0	0	0	0	0
	FNS	1	0	0	0	0	0	1	0
	IFFP	0	0	0	0	0	0	0	0
	Conseil ETH	53	0	42	2	1	1	1	6
	Innosuisse	1	0	0	0	1	0	0	0
Total	175	5	80	27	39	5	6	18	

Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC	SG DETEC	24	0	10	1	0	0	1	12
	OFT	9	0	5	0	2	0	1	1
	OFAC	27	5	7	8	7	2	1	2
	OFEN	20	0	2	1	10	1	1	5
	OFROU	17	0	15	0	1	0	0	1
	OFCOM	24	0	9	0	4	4	2	5
	OFEV	98	1	44	11	26	7	4	6
	ARE	3	0	3	0	0	0	0	0
	ComCom	1	0	0	0	0	0	0	1
	IFSN	6	2	0	0	2	0	3	1
	ESTI	1	0	0	0	1	0	0	0
	PostCom	3	2	2	0	1	0	0	0
	AIEP	1	0	0	1	0	0	0	0
	IFP	0	0	0	0	0	0	0	0
	SUST	2	0	0	2	0	0	0	0
	Total	236	10	97	24	54	14	13	34

		Nombre de demandes d'accès	dont soumis les années précédentes	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Ministère public de la Confédération MPC	MPC	2	0	1	0	0	0	0	1
	Total	2	0	1	0	0	0	0	1
Services du Parlement SP	SP	2	0	0	1	0	0	0	1
	Total	2	0	0	1	0	0	0	1
Somme totale		1738	37	830	176	402	73	96	161

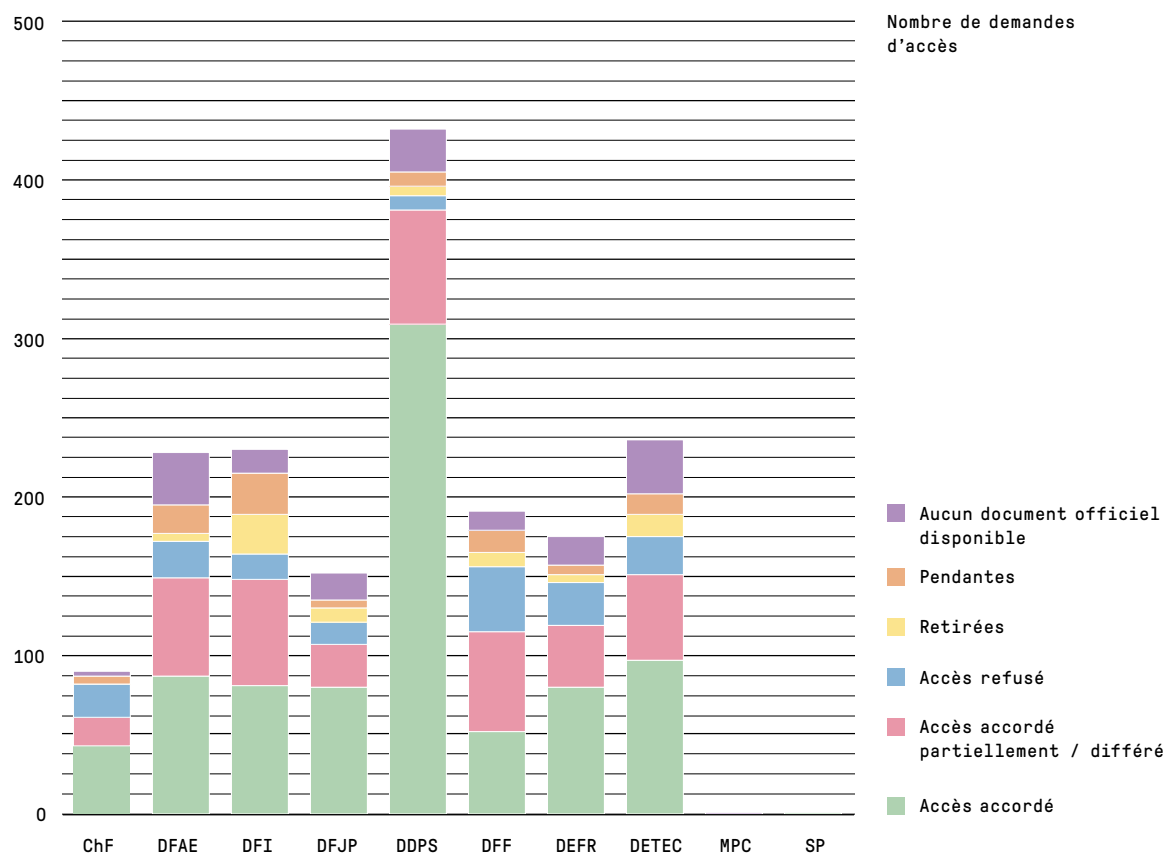
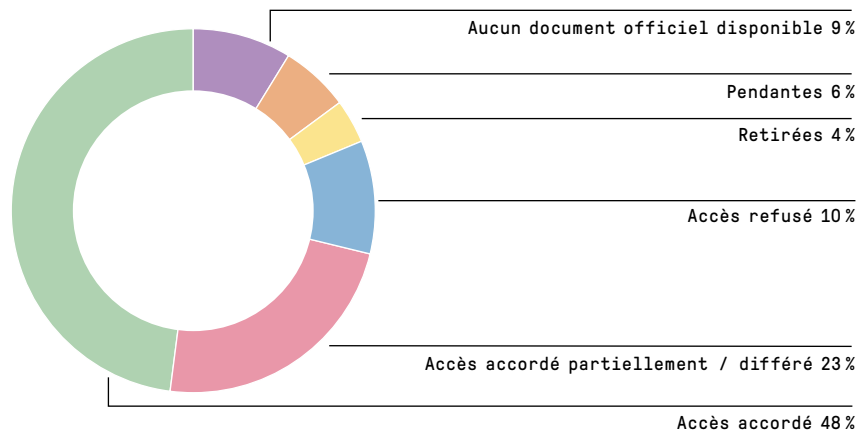
Demandes d'accès 2023 liées au COVID-19

		Demandes liées au Corona	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
Chancellerie fédérale ChF	Total	0	0	0	0	0	0	0
Département fédéral des affaires étrangères DFAE	Total	0	0	0	0	0	0	0
Département fédéral de l'intérieur DFI	OFSP	22	9	0	11	0	2	0
	OFS	1	0	0	0	0	0	1
	swissmedic	12	2	1	5	0	0	4
	Total	35	11	1	16	0	2	5
Département fédéral des finances DFF	Total	0	0	0	0	0	0	0
Département fédéral de justice et police DFJP	Total	0	0	0	0	0	0	0
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC	OFCOM	1	0	0	1	0	0	0
	ComCom	1	0	0	0	0	0	1
	Total	2	0	0	1	0	0	1
Département fédéral de la défense, de la protection de la population et des sports DDPS	Total	0	0	0	0	0	0	0
Département fédéral de l'économie, de la formation et de la recherche DEFR	SECO	1	0	0	0	0	0	1
	Conseil ETH	1	1	0	0	0	0	0
	Total	2	1	0	0	0	0	1
Ministère public de la Confédération MPC	MPC	0	0	0	0	0	0	0
	Total	0	0	0	0	0	0	0
Services du Parlement SP	SP	0	0	0	0	0	0	0
	Total	0	0	0	0	0	0	0
	Somme totale	39	12	1	17	0	2	7

Nombre de demandes en médiation

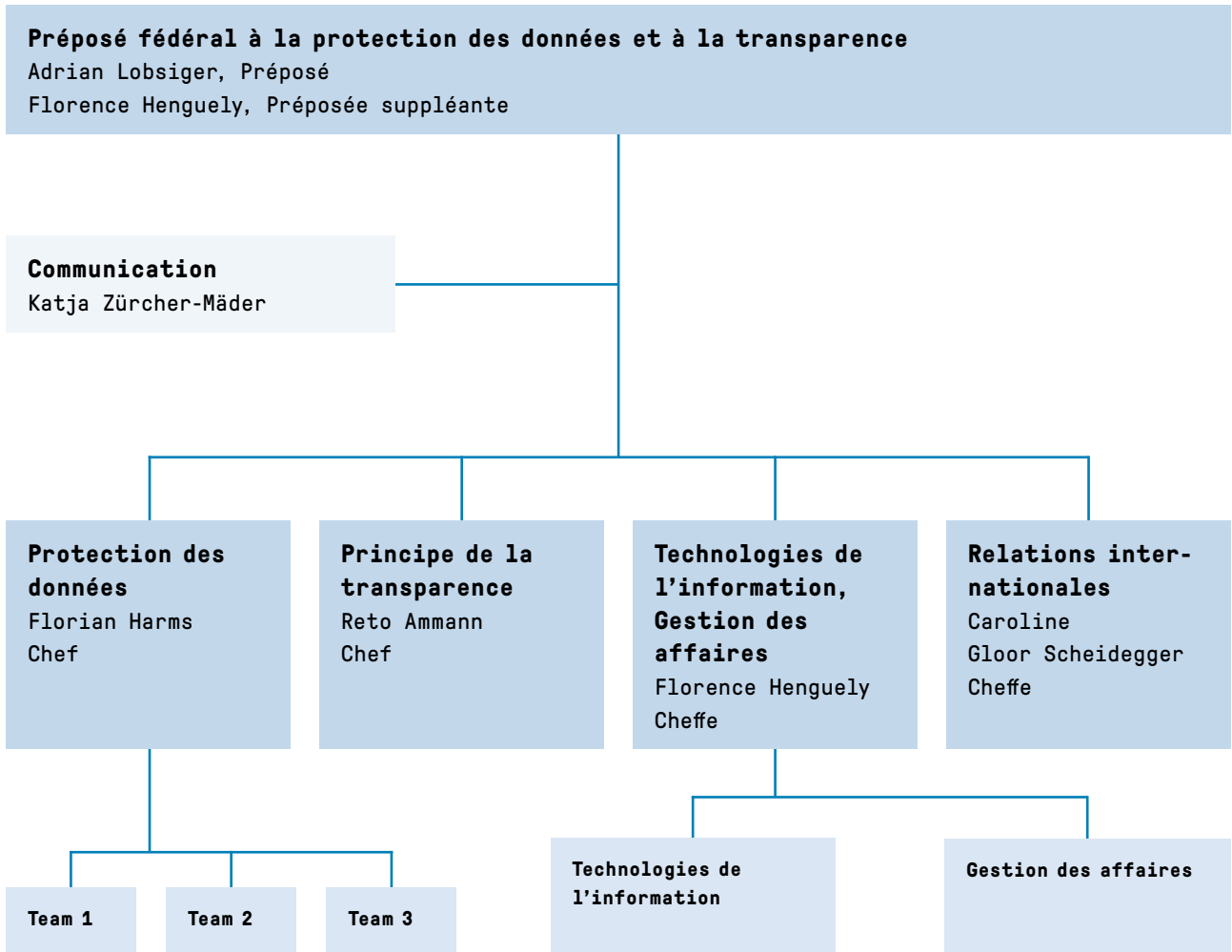
Catégories de requérants	2023	2022	2021	2020	2019	2018	2017
Médias	74	47	53	31	34	24	21
Personnes privées (ou requérants ne pouvant pas être attribués de manière précise)	31	37	49	42	40	26	35
Représentants de milieux intéressés (associations, organisations, sociétés, etc.)	8	9	16	5	7	9	14
Avocats (pour des tiers ou pour leur compte propre)	16	27	12	7	5	4	2
Entreprises	3	9	19	7	47	13	7
Universités	0	0	0	1	0	0	0
Total	132	129	149	93	133	76	79

Demandes d'accès de l'ensemble de l'administration fédérale du 1^{er} janvier au 31 décembre 2023



3.4 Organisation du PFPDT (État au 31 mars 2024)

Organigramme



Personnel du PFPDT

Nombre d'employés	47		
EPT	40.2		
par sexe	Femmes	24	51%
	Hommes	23	49%
par pourcentage d'emploi	1-89%	28	60%
	90-100%	19	40%
par langue	Allemand	35	75%
	Français	11	23%
	Italien	1	2%
par âge	20-49 ans	27	57%
	50-65 ans	20	43%
Postes dirigeants	Femmes	6	55%
	Hommes	5	45%

Liste des abréviations

AIPD Analyse d'impact relative à la protection des données

AMVP Assemblée mondiale pour la protection de la vie privée

CEPD Comité européen de la protection des données

CEPD Contrôleur européen de la protection des données

DataReg Registre des activités de traitement des organes fédéraux

DEP Dossier électronique du patient

DSIO Délégué à la sécurité informatique des unités administratives

e-ID Identité électronique

Fedpol Office fédéral de la police

IA Intelligence artificielle

LAr Loi fédérale sur l'archivage

LDPa Loi sur les données relatives aux passagers aériens

LPD Loi sur la protection des données

LRH Loi relative à la recherche sur l'être humain

LSI Loi sur la sécurité de l'information

LTPM Loi sur la transparence des personnes morales

LTrans Loi fédérale sur le principe de la transparence dans l'administration

OCPD Ordonnance sur les certifications en matière de protection des données

OFCS Office fédéral de la cybersécurité

OFDF Office fédéral de la douane et de la sécurité des frontières

OPDo Ordonnance sur la protection des données

OTrans Ordonnance sur la transparence

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

PNR Données des passagers des compagnies aériennes

Privatim Conférence des Préposé-e-s suisses à la protection des données

RA Rapport annuel du PFPDT

RGPD Règlement général sur la protection des données

SAS Service d'accréditation suisse

SIS II Système d'information Schengen de deuxième génération

TIC Technologies de l'information et de la communication

TNI Secteur Transformation numérique et gouvernance de l'information de la Chancellerie fédérale

VIS Système d'information sur les visas

Table des illustrations

Graphiques	Tableaux
Graphique 1 : Demandes d'accès – évolution depuis 2010 p. 65	Tableau 1 : Solutions amiables p. 69
Graphique 2 : Émoluments prélevés depuis l'entrée en vigueur de la LTrans p. 67	Tableau 2 : Durée de traitement des procédures de médiation p. 70
Graphique 3 : Demandes en médiation depuis l'entrée en vigueur de la LTrans p. 68	Tableau 3 : Procédures de médiation pendantes p. 71
	Tableau 4 : Dispositions spéciales au sens de l'art. 4 LTrans p. 78
	Tableau 5 : Dispositions ne constituant pas des dispositions spéciales au sens de l'art. 4 LTrans p. 79
	Tableau 6 : Postes pouvant être affectés aux questions relatives à la LPD p. 82
	Tableau 7 : Prestations protection des données p. 82
	Tableau 8 : Activités de conseil portant sur de grands projets en 2023 p. 83
	Tableau 9 : Objectifs du Préposé fédéral p. 84

Impressum

Ce rapport est disponible en quatre langues et peut être consulté sur Internet (www.leprepose.ch).

Distribution : OFCL, Vente des publications fédérales, CH-3003 Berne

www.bundespublikationen.admin.ch

Art.-Nr. 410.031.F

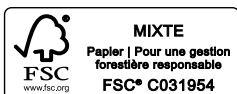
Mise en page : Ast & Fischer AG, Wabern

Photographie : Monika Flückiger

Caractères : Pressura, Documenta

Impression : Ast & Fischer AG, Wabern

Papier : PlanoArt[®], sans bois, extra blanc



Chiffres clés

Prestations protection des données

53%

Conseil

16%

Surveillance

18%

Information

13%

Législation

Demandes d'accès Principe de la transparence (LTrans)

48%

accordé

23%

accordé
partiellement/
différé

10%

refusé

4%

retirées

6%

pendantes

9%

aucun document
officiel disponible

Préoccupations relatives à la protection des données



Transparence de l'information

Les entreprises et les autorités fédérales fournissent des informations transparentes sur le traitement de leurs données : c'est compréhensible et complet.



Possibilité de choisir

Les personnes concernées donnent leur consentement et jouissent d'une réelle liberté de choix.



Analyse des risques

Les risques éventuels pour la protection des données sont déjà identifiés dans le projet et leurs effets sont minimisés par des mesures.



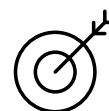
Exactitude des données

Le traitement s'effectue avec des données correctes.



Proportionnalité

Pas de collecte systématique de données, seulement dans la mesure où cela est nécessaire pour atteindre l'objectif. Le traitement des données est limité dans le temps et dans l'espace.



Finalité

Les données ne seront traitées qu'aux fins indiquées au moment de la collecte, selon les circonstances ou dans les cas prévus par la loi.



Sécurité des données

Les responsables du traitement des données veillent techniquement et organisationnellement à ce que les données personnelles soient protégées de manière adéquate.



Documentation

Tout traitement de données est documenté et classé par le responsable du traitement des données.



Responsabilité individuelle


Les organismes privés et fédéraux sont responsables du respect de leur obligation de se conformer à la législation sur la protection des données.

Préposé fédéral à la protection des données et à la transparence
Feldeggweg 1
CH-3003 Berne

E-mail : info@edoeb.admin.ch

Site web : www.leprepose.ch

 @EDÖB – PFPDT – IFPDT

 @derBeauftragte

Téléphone : +41 (0)58 462 43 95 (lu-ve, 10h-11h30)

Téléfax : +41 (0)58 465 99 96