



32^e Rapport d'activités 2024/2025

Préposé fédéral à la protection
des données et à la transparence



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2024/2025

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 2024 au 31 mars 2025 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 2024.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra



Primauté de la politique et langage

Avec une intelligence artificielle accessible à tous, la digitalisation a donné naissance à son dernier miracle technologique, qui nous émerveille par sa capacité à écrire, parler, chanter ou peindre en toute autonomie.

Mais ceux qui se contentent de « s'émerveiller » risquent de se retrouver à la traîne dans le domaine numérique. Pour éviter cela, la compétence numérique est indispensable pour tous. Ce message nous parvient par tous les canaux médiatiques. Il est également relayé par les milieux de la protection des données, qui expliquent à juste titre comment empêcher le « traçage », la transmission de données de localisation ou l'entraînement de l'intelligence artificielle avec ses propres données.

Il est certainement légitime d'attendre des responsables politiques qu'ils se familiarisent avec la réalité numérique. Toutefois, ceux qui exigent une preuve de compétences numériques pour exercer des fonctions politiques vont trop loin. Les représentants du peuple sont tout à fait capables d'évaluer les opportunités et les risques sociaux des technologies numériques. Mais ils doivent pouvoir compter sur le fait que ceux qui comprennent ces technologies et leurs environnements d'application complexes sont disposés et capables de partager leurs connaissances dans un langage compréhensible.

Au cours de la période sous revue, l'autorité fédérale de surveillance en matière de protection des données a ainsi fortement insisté pour que l'administration expose, en prose compréhensible, les risques liés à la protection des données de ses projets de numérisation dans les propositions adressées au Conseil fédéral et dans les messages à l'intention du Parlement.

Adrian Lobsiger
Préposé fédéral à la protection des données et à la transparence



Berne, le 31 mars 2025

Défis actuels	8
Protection des données	
1.1 Numérisation et droits fondamentaux	15
– Conseil : Projet CEBA de la Chancellerie fédérale	15
– Administration numérique suisse (ANS) : Interrogations juridiques sur les nouvelles tâches	16
– Fraude électorale : Pratiques déloyales en relation avec la récolte de signatures	16
– Vote électronique : Des compétences clairement définies	17
– E-ID : Implication du PFPDT dans le projet de loi sur l'identité électronique	17
– Communication électronique domaine judiciaire : Projet Justitia 4.0 de la Confédération et des cantons.....	18
– Cybercriminalité : Cyberattaque contre OneLog	18
– Cyberattaque : Clôture des enquêtes préliminaires informelles visant Concevis AG et l'Office fédéral de la statistique (OFS)	19
Accent	20
Nouvelles pratiques et activités de surveillance	
1.2 Justice, police, sécurité	29
– Cybercriminalité : Les enquêtes menées contre l'entreprise Xplain et les offices fédéraux fedpol et OFDF se terminent par l'acceptation des recommandations. . .29	
– Législation : Révision de la loi sur le renseignement ...	30
1.3 Économie et société	32
– Tracking multiplateforme : Prise de position de Ricardo et TX Group concernant les recommandations du PFPDT...32	
– Compte client : Le PFPDT accompagne la mise en œuvre des recommandations acceptées par un shop en ligne ... 33	
– Campagne en ligne : Enquête contre l'association Forum Civique Suisse	34
– Marché de l'immobilier : Questions non autorisées dans les formulaires de demande de location	36
1.4 Santé	39
– Dopage : Transmission de données médicales d'athlètes suisses	39
– Formulaires patients : Entre devoir d'information et consentement	40
– Dossier électronique du patient: Révision complète de la loi et financement transitoire	41
1.5 Travail	42
– Droit du personnel de la confédération : Plateforme Whistleblowing	42
– Droit du personnel de la Confédération : Profilage dans le cadre des évaluations et de la recherche active de personnel	43
– Surveillance des employés : Respect des principes de protection des données	44
1.6 Transports	47
– Projet Swisscom Broadcast : Le PFPDT exige des réponses à propos du réseau de drones de Swisscom	47
– Biométrie : Reconnaissance faciale à l'aéroport de Zurich.....	47
– Passenger Name Records : Loi sur les données relatives aux passagers aériens.	48
– Contrôle aux CFF : Plateforme NOVA des transports publics	48
1.7 International	50
– Extraction de données (Data Scraping)	50
– Swiss- US DPF (Data Privacy Framework)	51
– Schengen	54
– Conseil de l'Europe.....	57
– Conférence de printemps.....	59
– European Case Handling Workshop (ECHW)	59
– OCDE	59
– Privacy Symposium	61
– AMVP	61
– AFAPDP.....	62
– Rencontres bilatérales	63

Principe de la transparence

2.1 Généralités	66
2.2 Demandes d'accès – hausse considérable en 2024	68
2.3 Procédures de médiation – nette augmentation des demandes	72
– Proportion des solutions amiables	72
– Durée des procédures de médiation	73
– Nombre de cas pendants.....	75
2.4 Processus législatif	76
– Rapport de la CdG-E: Le Conseil fédéral renonce à examiner la possibilité d'octroyer un droit de disposition au PFPDT	76
– Droit du personnel de la Confédération : Limitation du principe de la transparence pour les lanceurs d'alerte ..	78
– Aviation : Limitation du principe de la transparence quant à la surveillance de l'aviation civile	79
– Aviation : Modification de l'ordonnance sur les enquêtes de sécurité en cas d'incident dans le domaine des transports (OEIT)	80
– Surveillance financière : Nouvelle loi fédérale sur la transparence des personnes morales.....	81
– Application du droit de nécessité: Rapport du Conseil fédéral.....	82
2.5 Dispositions spéciales réservées au sens de l'art. 4 LTrans	84

Le PFPDT

3.1 Prestations et ressources	90
– Prestations et ressources dans le domaine de la protection des données	90
– Prestations et ressources dans le domaine de la loi sur la transparence	92
– Visite de service de la sous-commission DFJP/ChF de la Commission de gestion du Conseil National.....	94
– Conseiller à la protection des données du PFPDT	94
3.2 Communication	96
– Communiqués de presse.....	96
– Brèves	96
– Information et sensibilisation	96
– Site internet	97
– Travail de presse.....	97
3.3 Statistiques	98
– Statistiques des activités du PFPDT du 1 ^{er} avril 2024 au 31 mars 2025	98
– Vue d'ensemble des demandes d'accès selon la loi sur la transparence du 1 ^{er} janvier au 31 décembre 2024.....	100
– Statistique des demandes d'accès selon la loi sur la transparence du 1 ^{er} janvier au 31 décembre 2024.....	101
– Nombre de demandes en médiation par catégories de requérants	104
– Demandes d'accès de l'ensemble de l'administration fédérale du 1 ^{er} janvier au 31 décembre 2024	105
3.4 Organisation du PFPDT	106
– Organigramme	106
– Personnel du PFPDT	107
Liste des abréviations	108
Table des illustrations	109
Impressum	110
Dans le pli	
– Chiffres-clés	

Défis actuels

I Protection des données

Les sociétés démocratiques occidentales disposent de technologies numériques, de capacités financières et de main-d'œuvre en quantités suffisantes pour développer leurs infrastructures de contrôle de manière à transformer en son contraire la vie privée et autodéterminée de leurs citoyennes et citoyens garantie par les constitutions libérales.

Les capteurs et les drones sont bon marché, peuvent être fabriqués presque à volonté et utilisés pour la surveillance étendue de tous les mouvements et de tous les visages dans l'espace public. Tout cela peut être combiné avec la mise en réseau de l'ensemble des systèmes d'information des autorités et d'une surveillance de l'espace virtuel perfectionnée par l'État et l'économie numérique, allant jusqu'au contrôle social assisté par l'IA ou «score social». La vie quotidienne des personnes en Occident serait alors soumise à une surveillance presque totale.

Formulée de manière neutre du point de vue technologique, la loi suisse sur la protection des données (LPD) interdit la reconnaissance faciale et le score social généralisé – même si le Préposé ne peut déduire cette interdiction que par l'interprétation de cette loi – car, contrairement à la législation européenne sur l'intelligence artificielle (AI Act), cette interdiction n'y est pas explicitement inscrite (cf. notre brève du 9 novembre 2023). Le droit de la protection des données et les autorités de surveillance – tel le PFPDT – contribuent ainsi à ce que les démocraties occidentales ne s'abandonnent pas inconsidérément au doux poison de la faisabilité technologique. La protection des données elle-même repose sur les garanties constitutionnelles de liberté et sur la conviction juridique générale que ces garanties doivent être respectées et appliquées par des institutions indépendantes de l'État de droit démocratique.

Dans bon nombre d'États occidentaux partenaires de la Suisse, un fossé se creuse entre les partisans de l'État de droit et les milieux qui prétendent n'avoir rien à cacher et, par conséquent, rejettent la protection des droits fondamentaux et des données comme étant une tutelle inutile pour eux-mêmes et comme une contrainte imposée par une bureaucratie déconnectée qui, soi-disant, reviendrait à protéger davantage les auteurs d'infractions que les citoyens. Souvent animés de ressentiments à

l'égard des «élites», ces milieux manifestent une incompréhension particulière lorsque les tribunaux et les autorités de surveillance contrôlent les actions du pouvoir exécutif.

Au sein des communautés occidentales concernées, les critiques récurrentes à l'égard de l'État de droit et le clivage des opinions, toujours plus profond, renforcent un mode de pensée dominé par une insatiable soif de sécurité. Un schéma cognitif qui exige le durcissement de toutes les infrastructures de contrôle dans la mesure de la faisabilité technologique et qui salue les effets contraignants du contrôle social numérique pour les «criminels», les «étrangers» et tous ceux qui «pensent autrement», tout en les occultant pour soi-même et ses semblables. Là où ce mode de pensée s'impose comme culture dominante en Occident, on attend également des individus qui y vivent qu'ils mènent une existence dans laquelle même leur sphère intime est déterminée par une puissance informationnelle supérieure – et ceci plus tôt que tard.

«La LPD interdit la reconnaissance faciale et le score social généralisé.»

II Principe de la transparence

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

L'intérêt croissant pour le principe de transparence entraîne une augmentation du nombre de demandes d'accès aux documents administratifs.

Il en va de même pour les procédures de médiation menées par le PFPDT. Ainsi, le nombre de demandes de médiation reçues en 2024 n'avait jamais été aussi élevé, ce qui a eu pour effet d'allonger la durée de traitement desdites procédures. Au cours de l'année sous revue, le PFPDT n'a pu respecter le délai légal de 30 jours que dans un peu plus d'un quart des cas (voir chap. 2.3). Outre le nombre croissant de demandes, la complexité accrue des questions juridiques liées aux demandes de médiation a également contribué à l'allongement des procédures. Ainsi, les questions de délimitation relatives au champ d'application de la LTrans nécessitent parfois des clarifications approfondies avant qu'une évaluation sur le fond puisse, le cas échéant, être réalisée.

Par ailleurs, l'implication de représentants légaux dans la procédure de médiation – qu'il s'agisse de ceux des demandeurs ou des tiers, ou alors de l'administration – entraîne dans la majorité des cas un allongement des délais.

Compte tenu de l'intérêt croissant pour l'accès aux documents officiels et de l'augmentation attendue du nombre de demandes de médiation, la mise en œuvre rapide des procédures de médiation demeurera un défi.

Nombre croissant d'exceptions à la LTrans prévues par des lois spéciales

Les efforts entrepris par l'administration pour exclure certains domaines de son activité ou certaines catégories de documents du champ d'application du principe de transparence se poursuivent. Le PFPDT a formulé des prises de position critiques dans le cadre des consultations des offices, relevant que l'introduction de telles restrictions affaiblit le principe de transparence ainsi que la transparence administrative qu'il vise à garantir. Il convient de déterminer si une disposition légale prévaut en tant que disposition spéciale au sens de l'art. 4 LTrans au cas par cas sur la base d'une interprétation des normes concernées.

Compte tenu du nombre croissant d'exceptions à la LTrans prévues par des lois spéciales, le PFPDT publie, comme dans son précédent rapport d'activités, un tableau présentant l'état actuel de ces exceptions (voir chap. 2.5), également consultable sur son site Internet.

«En 2024, le nombre de demandes en médiation a atteint un niveau sans précédent.»

III Coopération nationale et internationale

Coopération nationale

Les autorités de protection des données de la Confédération, des cantons et des communes continuent d'intensifier leur collaboration afin de garantir une surveillance efficace et intégrale.

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 continué à faire l'objet d'échanges entre le PFPDT et les autorités de protection des données partenaires (cf. 31^e RA, ch. III). Ces différences ont notamment été abordées dans le cadre des relations contractuelles de travail au sein des institutions privées délégataires de tâches publiques ou au bénéfice de contrats de prestations avec un canton ou des institutions publiques cantonales. Ces discussions ont par exemple été menées dans le domaine des transports publics ou médico-social tel que les homes médicalisés.

Les autorités de protection des données se sont également régulièrement entretenues au sujet de l'introduction et/ou de l'exploitation de plateformes de systèmes de bases de données communs. Cela a nécessité une analyse juridique et technique plus approfondie, en particulier concernant la répartition claire des responsabilités et des rôles.

C'est notamment le cas lorsque la Confédération exploite une plateforme qui traite des données personnelles émanant des cantons et justifié par des obligations légales cantonales. On peut par exemple citer les projets POLAP (cf. ch. 1.2), Justitia (cf. ch. 1.1), eVoting (cf. ch. 1.1). Dans le cadre du projet POLAP, le PFPDT et privatim ont par ailleurs publié une prise de position (PFPDT du 27.03.2024; privatim du 23.02.2024).

Échange avec privatim

Enfin, comme membre associé, le PFPDT a participé aux assemblées des autorités cantonales de protection des données (Conférence des Préposé(e)s suisses à la protection des données, privatim) qui permettaient de traiter des thématiques actuelles telles que les clouds et les conséquences juridiques des violations de la protection et sécurité des données.

Échange annuel avec les conseillères et conseillers à la protection des données de la Confédération

Pour la deuxième année consécutive, le PFPDT a organisé une séance d'information à l'attention des conseillères et conseillers à la protection des données de la Confédération.

En tant que premier interlocuteur, ils sont amenés à avoir des échanges réguliers avec le PFPDT. Ainsi, il est important que les nouveautés en lien avec la protection des données, que ce soit du point de vue légal, technique ou pratique, leur soient communiquées ouvertement, notamment en vue de l'accomplissement de leurs tâches légales. Cet événement leur offre également l'occasion de rencontrer leurs collègues et d'échanger sur les défis quotidiens d'une telle fonction.

Rencontres annuelles avec les associations pour la protection des données en Suisse

Comme chaque année, le PFPDT a rencontré les associations pour la protection des données afin d'échanger sur les défis actuels. Cette immersion dans la réalité des entreprises privées est primordiale puisqu'elle permet un échange sur leurs pratiques et défis. Ces échanges permettent également au PFPDT de connaître les priorités et les intérêts des différentes régions linguistiques.

Coopération internationale

Les échanges au niveau international restent d'une importance capitale, compte tenu de la présence d'entreprises technologiques mondiales sur le marché suisse et des questions d'exécution à caractère transfrontalier qui y sont liées.

Le PFPDT est toujours représenté au sein d'importants organismes internationaux. Les échanges avec les autorités de protection des données de l'UE et de l'EEE sont de première importance pour le Préposé. Au cours de l'année sous revue, il a participé avec tout autant d'intérêt aux réunions informelles des États bénéficiant d'une décision d'adéquation de l'UE (les « adequacy groups »), auxquelles ont conviés, d'une part, l'UE et, d'autre part l'autorité de protection des données de Grande-Bretagne.

Protection des données



1.1 Numérisation et droits fondamentaux

CONSEIL

Projet CEBA de la Chancellerie fédérale

Au cours de l'année sous revue, le PFPDT a poursuivi son activité réglementaire de surveillance du projet CEBA (Cloud Enabling Büroautomation). Il a mis l'accent sur l'examen de l'analyse d'impact relative à la protection des données, réalisée par l'administration, et sur les premières sessions de formation du personnel fédéral.

Lancé en 2019, le projet CEBA (projet de bureautique en nuage) est dirigé par le secteur Transformation numérique et gouvernance de l'informatique (secteur TNI) de la Chancellerie fédérale (ChF). Il vise à remplacer la gamme bureautique Office « Microsoft Office LTSC Professional Plus 2021 », actuellement utilisée dans l'environnement de travail de la Confédération, par la solution basée sur le cloud « Microsoft Office 365 » (M365). Le secteur TNI a impliqué le

PFPDT dans le projet à un stade précoce de sorte que ce dernier a déjà pu informer le public, au cours de la dernière période sous revue, de ce projet d'externalisation vers le nuage public (cf. 31^e RA, ch. 1.1 ; communiqué du 7 mars 2023).

Depuis le lancement du projet, le Préposé a notamment obtenu que le secteur TNI examine des solutions de rechange à Microsoft Office 365, utilisables à moyen terme. Actuellement, son activité de surveillance est axée sur l'adaptation et la clarification de l'analyse d'impact relative à la protection des données (AIPD) réalisée par le secteur TNI et sur les premières formations du personnel.

Le PFPDT demande au secteur TNI de vérifier la proportionnalité d'une solution fédérale basée sur le nuage et d'analyser et évaluer les risques pertinents en matière de protection des données – concernant notamment l'accès des autorités étrangères et la dépendance à l'égard de fournisseurs de services informatiques en nuage en position dominante sur le marché. Dans ses prises de position sur les mises à jour constantes de l'AIPD, le PFPDT a insisté sur la nécessité de décrire les risques majeurs de manière plus précise et de définir sans ambiguïtés les mesures nécessaires à la minimisation des risques.

Le secteur TNI travaille actuellement à apporter les précisions et les compléments requis. Des audits indépendants sont menés en parallèle. Leurs résultats seront pris en compte dans la prochaine version de l'AIPD.

Une mesure importante permettant de minimiser les risques du projet CEBA est l'étiquetage des documents contenant des données personnelles à caractère sensible et dont le traitement doit demeurer dans les centres de données de l'administration fédérale. Le personnel de la Confédération doit donc être formé en conséquence. Quelques collaborateurs du PFPDT ont assisté aux premières sessions de formation afin de s'assurer que les exigences en matière de protection des données et de sécurité étaient respectées. En tant qu'unité rattachée administrativement à la Chancellerie fédérale, le PFPDT fera également appel ultérieurement à ces services en matière de migration cloud et de formation.

ADMINISTRATION NUMÉRIQUE SUISSE (ANS)

Interrogations juridiques sur les nouvelles tâches

L'Administration numérique suisse a repris les tâches de la Conférence suisse sur l'informatique. Le PFPDT et les autorités cantonales de protection des données clarifient leur collaboration avec l'ANS dans le cadre de leurs compétences fédérales respectives.

Au cours de l'année sous revue, les tâches de la Conférence suisse sur l'informatique (CSI) ont été intégralement transférées à l'ANS (Administration numérique suisse), également soutenue conjointement par la Confédération et les cantons. En conséquence, l'ANS se charge désormais des déclarations de conditions avec les prestataires du secteur Transformation numérique et gouvernance de l'informatique (TNI). En outre, l'ANS est désormais l'actionnaire majoritaire d'eOperations Suisse SA.

Ces modifications ont amené le PFPDT et les autorités cantonales de protection des données à s'interroger

sur la nature juridique de l'ANS et sur les conséquences juridiques et les délimitations de compétences qui en résultent. Par exemple, s'il convient, en vertu de la convention cadre de droit public qui détermine son mandat de prestations, de considérer l'ANS en tant que société simple sans personnalité juridique constituée conformément au code des obligations comme un organe public ou comme un organe fédéral au sens de la LPD.

FRAUDE ÉLECTORALE

Pratiques déloyales en relation avec la récolte de signatures

Suite aux divers articles paru dans les médias ainsi que divers messages de citoyens, le PFPDT a observé, dans le cadre de sa surveillance, le cas de falsification présumée de signatures et de récolte douteuse dans le contexte des initiatives populaires et référendums. Le PFPDT a notamment analysé les questions de protection des données en lien avec les droits politiques prévus par la loi. Il s'est penché sur la question de savoir qui a accès aux données et quels sont les finalités de traitement lors de la récolte des signatures. Pour l'heure actuelle et avec les informations en possession du PFPDT, il résulte qu'il ne s'agit pas d'une problématique liée à la protection des données. En effet, il semblerait que la possible fraude fasse suite à des signatures ou adresses inventées, ainsi que des signataires qui n'existent plus. Cela exclut tout lien possible avec une personne physique identifiée ou identifiable et signifie que ces informations ne sont pas des données personnelles et que la loi sur la protection des données ne trouve pas application dans ce cas d'espèce.

VOTE ÉLECTRONIQUE

Des compétences clairement définies**Vote électronique : les cantons sont chargés de surveiller le respect de la législation sur la protection des données**

La Confédération et les cantons conduisent depuis 2004 le projet Vote électronique. Par décision du 26 juin 2019, le Conseil fédéral a chargé la Chancellerie fédérale (ChF) d'élaborer, avec les cantons, une restructuration de la phase d'essai du vote électronique. Le rapport final commun consacré à cette restructuration et à la reprise des essais prévoyait une révision des bases légales du vote électronique. La révision partielle de l'ordonnance sur les droits politiques (ODP) et la révision totale de l'ordonnance de la ChF sur le vote électronique (OVotE) sont entrées en vigueur le 1^{er} juillet 2022. En vertu de l'art. 14 OVotE, ce sont les cantons qui assument la responsabilité générale du bon déroulement du scrutin électronique.

Le rôle de la Confédération dans ce projet, plus précisément de la ChF, est d'accorder aux cantons des autorisations générales pour la réalisation à titre d'essai du vote électronique (art. 27a à 27q ODP). La Confédération et les cantons gèrent en commun un catalogue de mesures visant à assurer la sécurité du scrutin électronique en fonction des récents développements. Ce catalogue

est réexaminé, adapté et publié à intervalles réguliers. Il met en évidence les besoins existants et présente les développements prévus dans le domaine du vote électronique.

De plus, la Chancellerie fédérale est chargée du contrôle des systèmes mis en place pour le vote électronique. Ce contrôle est actuellement assuré par le système de La Poste Suisse et chaque canton décide lui-même de sa mise en œuvre. Aujourd'hui, quatre cantons disposent d'une autorisation d'utilisation du vote électronique : Saint-Gall, Bâle-Ville, Thurgovie et Grisons.

La surveillance du respect de la protection des données incombe uniquement aux autorités cantonales. En effet, s'agissant du vote électronique, la ChF ne remplit qu'un rôle d'organe de certification et la sécurité des systèmes relève des cantons.

E-ID

Implication du PFPDT dans le projet de loi sur l'identité électronique

Comme durant les exercices précédents, le PFPDT a accompagné, sur le plan de la surveillance, les travaux relatifs au projet de loi sur l'identité électronique (e-ID). Le PFPDT a notamment continué de soutenir le principe de non-traçabilité de l'e-ID afin de garantir une protection supplémentaire de la sphère privée. La non-traçabilité réfère à l'impossibilité de relier différentes transactions effectuées avec une e-ID.

Dans le cadre de la révision sur la loi sur l'identité électronique, le PFPDT avait fait part de son inquiétude que la création de l'e-ID n'engendre des prélevements excessifs de données personnelles dans le monde numérique. En effet, un accès à l'ensemble des données de l'e-ID d'un client pour vérifier par exemple son âge lors d'un simple achat en ligne de produits réservés aux adultes (alcool notamment) serait considéré comme excessif et donc abusif. Un simple accès à la seule information sur la majorité de la personne concernée suffirait.

C'est pour cette raison que le PFPDT a soutenu le principe de non-traçabilité de l'e-ID qui garantit une protection supplémentaire de la sphère privée en empêchant l'accès aux données non nécessaires. Lors de la mise en œuvre de l'identité électronique, le PFPDT a donc demandé une application contraignante de ce principe, ce qui a été accepté par les autorités et intégré dans la loi, qui a été adoptée le 20 décembre 2024 par les Chambres fédérales.

COMMUNICATION ÉLECTRONIQUE DOMAINÉ JUDICIAIRE

Projet Justitia 4.0 de la Confédération et des cantons

Le PFPDT supervise la mise en place de la plateforme justitia.swiss destinée à promouvoir la communication électronique des écrits dans le domaine judiciaire. Le projet justitia.swiss fournira une plateforme en ligne pour la communication électronique entre tous les acteurs des procédures judiciaires, à savoir les autorités judiciaires, les avocats et les autres parties à la procédure. Cette plateforme permettra la mise en place des échanges juridiques électroniques et la consultation électronique des dossiers.

Au cours de l'année sous revue, à la demande des cantons, le PFPDT a contribué à créer des conditions-cadres aussi uniformes que possible pour les projets-pilotes prévus par les cantons

et la Confédération – dont certains sont déjà en cours –, tout en assurant le fonctionnement de la plateforme dans le respect de la protection des données.

Étant donné que des problèmes juridiques, techniques et organisationnels doivent encore être résolus avant que justitia.swiss ne soit pleinement opérationnel, c'est-à-dire pas avant 2026 au plus tôt, le PFPDT a pris en charge la coordination des aspects du projet relatifs à la protection des données, d'entente avec les cantons, l'Office fédéral de la justice et l'organisation de projet justitia.swiss.

Conformément à la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire (LPCJ), qui entrera en vigueur au plus tôt le 1^{er} janvier 2026, le PFPDT devrait alors exercer seul la surveillance de la protection des données sur la plateforme justitia.swiss. Actuellement, ce sont encore les organes cantonaux en charge de la protection des données qui sont responsables du contrôle préalable des projets pilotes de justitia.swiss en cours dans les différents cantons. Toutefois, la compétence de surveillance doit être transférée au PFPDT le plus rapidement possible par la mise en vigueur rapide des dispositions requises de la LPCJ. Un projet pilote fédéral uniforme pourra ensuite être mis en œuvre et supervisé par le PFPDT.

CYBERCRIMINALITÉ

Cyberattaque contre OneLog

Cibles d'une cyberattaque le 24 octobre 2024, les services de connexion de OneLog ont été paralysés pendant une semaine environ. Désireux de garantir la sécurité des données de nombreux utilisateurs, les responsables informent en continu le PFPDT des mesures prises et de la suite des événements. Le 25 octobre 2024, la responsable de la protection des données de OneLog a informé le PFPDT que le service de connexion OneLog avait été piraté. Depuis, le PFPDT a reçu d'autres annonces spontanées de la part des responsables et actuellement, il demeure informé en continu des nouveaux éléments concernant cet événement. Selon le guide du PFPDT sur la notification des violations de la sécurité des données et l'information des personnes concernées conformément à l'art. 24 LPD, les

CYBERATTAQUE

annonces spontanées sont celles pour lesquelles le responsable du traitement n'identifie pas de risque élevé pour les personnes concernées dans le cadre de son évaluation des risques, mais souhaite informer le PFPDT de la violation de la sécurité des données pour d'autres raisons (cf. Accent, le texte sur la notification des violations de la sécurité des données). Dans ces cas justement, les annonces spontanées s'avèrent pertinentes pour toutes les parties prenantes, mais elles ont aussi un impact positif du point de vue de l'intérêt public lorsque l'analyse des risques révèle certes un risque faible sur la base des données concernées, mais qu'une couverture médiatique par exemple peut voir le jour en raison du grand nombre de personnes concernées.

OneLog est une offre de l'Alliance numérique suisse. Regroupant plusieurs entreprises de médias suisses, l'Alliance numérique suisse avait lancé son projet de système de connexion commune au cours d'une phase pilote au printemps 2021. Le PFPDT a publié un rapport à ce sujet dans son 28^e rapport d'activités (cf. 28^e RA, ch. 1.1).

Clôture des enquêtes préliminaires informelles visant Concevis AG et l'Office fédéral de la statistique (OFS)

Le PFPDT a clos les enquêtes préliminaires visant Concevis et l'Office fédéral de la statistique. Aucun manquement grave n'a été constaté et il est peu probable que les pirates informatiques aient pu lire les données visées par l'attaque. Le PFPDT a néanmoins relevé certains points devant être améliorés.

En novembre 2023, l'entreprise Concevis, société fournissant notamment des solutions logicielles, avait été victime d'une attaque par rançongiciel. Des données de l'Office fédéral de la statistique (OFS) étaient notamment concernées. Le PFPDT avait ainsi ouvert une enquête préliminaire informelle visant Concevis et une autre l'OFS (cf. 31^e RA, ch. 1.2).

L'examen mené par le PFPDT a permis de conclure que l'ouverture d'une enquête formelle au sens de l'art. 49 LPD n'était pas nécessaire, dans la mesure où aucun manquement grave n'a été constaté. En outre, les données concernées par la cyberattaque étaient cryptées et il est peu probable que les auteurs de l'attaque aient pu les lire.

Le PFPDT a toutefois constaté que certains éléments liés au traitement des données entre l'OFS et Concevis auraient dû être définis plus clairement. Il a par conséquent souligné que les contrats conclus par des unités administratives de la Confédération avec les fournisseurs de prestations devaient définir précisément le cycle de vie des données, de leur saisie à leur destruction. Il a en outre relevé la nécessité de régler clairement la possibilité pour l'office ou des prestataires externes de procéder à des contrôles et à des audits. Enfin, le PFPDT a rappelé à l'OFS et à Concevis les recommandations émises dans l'affaire Xplain, qui sont de portée générale.

Nouvelles pratiques et activités de surveillance

Pratique du PFPDT quant aux droits des personnes concernées

Toute personne peut demander au responsable du traitement si des données personnelles la concernant sont traitées. Cet instrument essentiel de la loi sur la protection des données vise à garantir la transparence et à permettre aux personnes concernées de contrôler le traitement de leurs données personnelles. Toutefois, au vu du nombre de dénonciations reçues, le PFPDT constate que cet instrument est souvent négligé par les responsables de traitement.

Le PFPDT a reçu un certain nombre de dénonciations concernant des possibles violations du droit d'accès. Dans plusieurs cas, il a constaté que les responsables de traitement ont laissé des demandes d'accès sans réponse ou se contentent

de renvoyer aux informations générales contenues dans leur politique de confidentialité, au lieu de transmettre les informations tel que précisé dans la prescription légale.

Dans le cadre de son activité de surveillance, le PFPDT est intervenu auprès de responsables de traitement, les a priés de donner suite aux demandes d'accès et de prendre les mesures nécessaires afin de garantir la conformité de leur pratique d'octroi du droit d'accès avec les prescriptions de la LPD. Dans un cas, il a ouvert une enquête formelle.

Le droit d'accès (Art. 25 LPD)

Élément clé de la loi sur la protection des données, le droit d'accès permet à tout individu d'obtenir des responsables de traitement des renseignements concernant les données personnelles traitées à son sujet.

Corollaire de ce droit, l'obligation pour les responsables de traitement de fournir des renseignements: si le responsable dispose de données personnelles concernant le requérant, il doit les lui transmettre dans un délai de 30 jours. Il doit également informer sur l'identité du responsable du traitement, la finalité du traitement, la durée de conservation des données personnelles, les informations disponibles sur l'origine des données personnelles, ou encore, le cas échéant, les

destinataires ou les catégories de destinataires auxquels des données personnelles sont communiquées. Une prolongation est possible, mais le nouveau délai doit être communiqué dans le délai de 30 jours.

De plus, il est essentiel que le responsable du traitement communique les données personnelles traitées en tant que telles afin de permettre aux personnes concernées de vérifier quelles données sont traitées, de contrôler leur exactitude et la licéité du traitement ainsi que, le cas échéant, d'en demander la rectification ou l'effacement.

Dans certains cas précis, prévus par la loi à l'art. 26 LPD, le responsable de traitement peut refuser, restreindre ou dif-

érer la communication de ces informations. Il doit alors indiquer le motif sur lequel il base cette décision, afin de permettre à la personne concernée de comprendre la ou les raisons motivant la restriction de l'accès et d'en vérifier la légitimité.

À noter également que le responsable de traitement s'expose à des conséquences pénales s'il communique des renseignements inexacts ou incomplets (violation de l'obligation de renseigner).

Obligation d'informer

Dans le cadre du projet de loi sur les données relatives aux passagers aériens (LDPa), outre divers points, le PFPDT a mis en évidence la question de l'obligation des autorités en matière d'information (cf. ch. 1.6). Selon le message relatif à LDPa, les entreprises de transport aérien doivent informer par écrit les passagers que leurs données ne seront pas traitées uniquement dans le cadre de leur vol, mais aussi en vertu de la LDPa. Il est possible de faire figurer cette information dans les conditions générales de vente des compagnies aériennes. L'obligation d'informer conformément à l'art. 5 LDPa est justifiée même s'il s'agit d'une répétition : en effet, le traitement des données relatives aux passagers aériens se déroule dans deux contextes totalement différents (déroulement technique de la réservation du vol / mise en œuvre de la LDPa), à des fins différentes (réservation du vol / lutte contre la criminalité) et sous la responsabilité d'acteurs différents (entreprises de transport aérien / fedpol). La finalité du traitement des données doit ressortir clairement de l'information (art. 6, al. 3, LPD). Les autres détails dont il faudra informer les personnes concernées découlent de la mise en œuvre de l'ordonnance sur la protection des données (OPDo).

Droit d'effacement

Au cours de l'année sous revue, le PFPDT a constaté que les demandes d'effacement des données ont été approuvées autant par les responsables privés de traitement des données que par l'administration fédérale. Dans certains cas, les conditions techniques sont plus problématiques que l'intention même d'effacement. C'est le cas par exemple lorsqu'un responsable privé partage une plateforme de données avec d'autres fournisseurs et que la personne concernée ne souhaite supprimer que les données d'un seul fournisseur. Dans la pratique, des interdépendances à caractère technique peuvent alors se produire.

Activités de surveillance et campagnes selon la nouvelle LPD

La nouvelle loi sur la protection des données a renforcé les droits des personnes concernées. Elle confie aussi au PFPDT des tâches et des compétences supplémentaires qu'il met en œuvre au moyen des instruments et activités de surveillance suivants :

Instruments

Les instruments suivants sont disponibles sur le site du PFPDT :

- **Formulaires d'annonce**

Ces formulaires permettent aux personnes concernées et aux tiers de nous signaler les violations présumées de la LPD.

- **Portails de notification pour les responsables**

Nos portails de notification permettent aux responsables de traitements de nous informer d'une violation de la sécurité des données (data breach) ou de la nomination d'un conseiller ou d'une conseillère à la protection des données.

Activités de surveillance

Selon l'aide-mémoire relatif aux enquêtes concernant les violations des prescriptions de protection des données, il convient de distinguer les activités de surveillance comme suit :

- **Enquêtes formelles**

Ces enquêtes sont menées selon le droit fédéral de la procédure administrative et servent à examiner les traitements de données personnelles qui, sur la base d'indices suffisants, pourraient enfreindre les prescriptions fédérales sur la protection des données.

- **Enquêtes préliminaires informelles**

Les enquêtes préliminaires informelles permettent au PFPDT de clarifier si les conditions d'une ouverture d'enquête formelle sont réunies ou non.

- **Interventions à bas seuil**

Les interventions à bas seuil sont des invitations écrites adressées aux responsables afin qu'ils contribuent volontairement, dans le cas de faits simples, à la mise en conformité rapide d'un traitement avec la protection des données.

Campagnes

Avant d'engager d'office des mesures de surveillance visant un responsable de traitement privé ou un organe fédéral, le PFPDT peut, par des campagnes de sensibilisation, attirer leur attention sur les risques touchant la protection des données et sur les mesures permettant de les réduire, ou encore leur préciser sa pratique en matière de surveillance.

Guides et feuillets thématiques

Si nécessaire, les précisions sur la pratique de surveillance sont consignées dans des guides et des feuillets thématiques. Au cours de l'année sous revue, ces documents ont été complétés par les publications suivantes :

- Aide-mémoire : Planifier et motiver les accès en ligne aux données personnelles (19 juin 2024)
- Guide relatif au traitement des données au moyen de cookies et de technologies similaires (22 janvier 2025)
- Guide relatif à l'annonce des violations de la sécurité des données et sur les informations des personnes concernées en vertu de l'art. 24 LPD (6 février 2025).

Activités de surveillance en chiffres

Au cours de l'exercice 2024/2025, le PFPDT a enregistré plus de 1000 notifications. Pour les données statistiques, voir le tableau 9 à la page 91.

Campagne de sensibilisation relative à l'utilisation du numéro AVS

Le PFPDT a lancé une campagne de sensibilisation relative aux obligations des Départements fédéraux et de la Chancellerie fédérale lors de l'utilisation systématique du numéro AVS. Cette campagne rappelle à ces organes en particulier leur obligation de mener périodiquement des analyses de risques.

Dans ce contexte de proactivité, le PFPDT a lancé une campagne de sensibilisation auprès des Départements fédéraux et de la Chancellerie fédérale concernant leur usage du numéro AVS. Cette campagne vise d'une part à leur rappeler les dispositions légales réglementant l'utilisation systématique du numéro AVS en dehors des assurances sociales et, d'autre part, à en vérifier la mise en œuvre au travers de vérifications par échantillonnage.

Introduites dans la Loi fédérale sur l'assurance-vieillesse et survivants (LAVS), des dispositions spécifiques imposent en effet aux utilisateurs toute une série d'obligations techniques et organisationnelles. Parmi ces mesures, deux obligations singulières ont été prévues à l'article 153^e LAVS. Il s'agit d'une part de l'obligation imposée aux Départements et à la Chancellerie fédérale, pour les banques de données détenues par eux-mêmes, de mener périodiquement des analyses de risques portant en particulier sur le risque d'un regroupement illicite de banques de données. Ces entités doivent d'autre part, en vue de ces analyses de risques, tenir un répertoire des banques de données dans lesquelles le numéro AVS est utilisé de manière systématique.

Interlocuteurs du PFPDT au sens de l'art. 28 de l'Ordonnance sur la protection des données (OPDo), les conseillères et conseillers à la protection des données de tous les Départements fédéraux et de la Chancellerie fédérale ont ainsi reçu le 26 septembre 2024 de la part du PFPDT un courrier écrit leur rappelant leurs obligations légales découlant de la LAVS. Des explications complémentaires leur ont aussi été fournies en séance interdépartementale du 30 octobre 2024.

L'ouverture de cette campagne a également été présentée aux conseillères et conseillers à la protection des données des Offices de la Confédération réunis le 26 novembre 2024 lors d'une rencontre d'information.

Obligation de désigner un représentant selon l'article 14 LPD

Le PFPDT a demandé aux entreprises étrangères qui traitent à grande échelle des données de personnes en Suisse de désigner un représentant en Suisse.

Afin de s'assurer que la loi s'applique à tous les états de fait qui déplient des effets en Suisse, même si les se sont produits à l'étranger, l'article 14 LPD précise dans quel cas d'espèce un représentant doit être désigné en Suisse. Cette désignation a notamment pour but de garantir un interlocuteur établi sur sol suisse aux personnes concernées et aux autorités ainsi que de limiter une protection amoindrie des résidents suisses par le simple fait que le responsable du traitement est établi à l'étranger.

Ainsi, toutes les entreprises privées qui traitent des données personnelles concernant des offres de biens ou de service ou le suivi de comportement de personnes en Suisse, qu'il s'agit d'un traitement à grande échelle, que le traitement est régulier et présente un risque élevé pour la personnalité des personnes concernées, doivent désigner un représentant basé en Suisse.

Le PFPDT est donc intervenu de manière ciblée auprès de nombreuses entreprises internationales répondant aux critères de la loi, afin de vérifier la nomination ainsi que la publication des coordonnées de leur représentant.

Sur son site Internet, le PFPDT fournit des informations complètes sur l'obligation de désigner un représentant conformément à l'article 14 de la LPD (cf. Protection des données/Les basiques).

Annonce des violations de la sécurité des données

Le PFPDT a publié un guide sur la manière de traiter les violations de la sécurité des données et ouvert deux enquêtes contre des responsables qui n'avaient pas informé les personnes concernées d'une telle violation.

Depuis l'entrée en vigueur de la nouvelle loi sur la protection des données, les responsables sont tenus d'annoncer au PFPDT les cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées. Au cours de l'année sous revue, le PFPDT a reçu 363 annonces de la part de responsables, conformément à l'art. 24, al. 1, LPD.

En vertu de la nouvelle LPD, tout comme de l'ancienne, certains responsables ont signalé et signalent des violations même si elles ne pressentent pas de risque élevé pour les personnes concernées. Il s'agit d'annonces volontaires, par exemple lorsque la violation pourrait susciter une résonance médiatique ou parce que des personnes concernées ou des lanceurs d'alerte pourraient s'annoncer auprès du PFPDT.

Dans le cas des annonces obligatoires, le PFPDT vérifie sommairement si les mesures prises ou prévues par le responsable du traitement pour protéger les personnes concernées et réduire les dommages sont suffisantes. Si nécessaire, le PFPDT demande des informations complémentaires concernant les faits ou requiert des mesures supplémentaires pour protéger ces personnes. Il vérifie également si elles ont été informées du cas de façon appropriée. S'agissant d'une annonce spontanée, pour laquelle le responsable n'a pas identifié de risque élevé envers la personne concernée, le PFPDT vérifie uniquement s'il existe une obligation d'informer les personnes concernées et, le cas échéant, comment cette obligation a été respectée.

Au cours de l'année sous revue, le PFPDT a constaté qu'une certaine confusion régnait, auprès de responsables, à propos de la notion de «risque élevé», qui déclenche l'obligation d'annoncer au PFPDT, et de sa distinction de la notion de «besoin de protection», qui requiert l'information de la personne concernée. Certains ne semblaient pas non plus être vraiment au clair sur les tâches leur incombaient quant à la prise de connaissance et à l'examen des notifications obligatoires et spontanées, et la mise en œuvre des obligations d'information envers les personnes concernées.

Afin d'épauler les responsables dans l'accomplissement de leurs obligations et de clarifier leur rôle, le PFPDT a publié le 22 janvier 2025 un guide traitant de la gestion des violations de la sécurité des données. Il y énonce les critères selon lesquels les responsables doivent évaluer s'il y a obligation d'annoncer au PFPDT. Il explique qu'il y a aussi obligation d'informer les personnes concernées lorsque celles-ci peuvent

ou doivent elles-mêmes prendre des mesures pour réduire ou éviter un dommage résultant d'une violation de la sécurité des données. Par exemple lorsqu'elles doivent modifier des données d'accès ou des mots de passe, bloquer leurs cartes de crédit, vérifier leurs relevés de compte ou certains messages et demandes (hameçonnage).

Le PFPDT peut requérir que les personnes concernées soient informées s'il estime qu'elles ont besoin d'être protégées ou s'il existe un intérêt public à ce que les responsables du traitement fournissent des informations en raison du grand nombre de personnes concernées ou d'une couverture médiatique. Cette compétence lui est donnée indépendamment du fait que le responsable du traitement lui ait préalablement communiqué la violation spontanément ou en tant qu'annonce obligatoire, ou qu'il ne la lui ait pas communiquée du tout.

Le PFPDT a ouvert une enquête en vertu des art. 49 ss LPD contre deux responsables qui n'avaient pas informé les personnes concernées de la violation en question – ou ne les avaient pas suffisamment informées – alors que cela semblait nécessaire à leur protection. Les deux responsables ont considéré qu'il n'y avait pas d'obligation d'information et ont refusé, même après la requête du PFPDT, d'informer les personnes concernées. Les procédures sont toujours en cours.

Les violations de la sécurité des données en chiffres

Au cours de l'exercice 2024/2025, le PFPDT a enregistré un total de 363 violations de la sécurité des données. Plus d'informations au ch. 1.3.

Augmentation du nombre des examens d'AIPD

Depuis l'entrée en vigueur de la nouvelle loi sur la protection des données, plusieurs organes de la Confédération ont soumis pour avis au PFPDT leurs analyses d'impact sur la protection des données (AIPD). Une AIPD doit être effectuée lorsqu'un traitement de données est susceptible d'engendrer un risque potentiellement élevé pour la personnalité ou les droits fondamentaux des personnes concernées.

L'AIPD est un outil permettant aux responsables de traitements de données d'identifier, d'évaluer et de réduire de manière appropriée les risques menaçant la sécurité des données. Si l'AIPD révèle que le traitement prévu présente encore un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, cela malgré les mesures envisagées par le responsable, ce dernier doit requérir un avis du PFPDT.

Une exception s'applique aux responsables privés s'ils ont consulté leur conseiller ou conseillère à la protection des données. Le PFPDT a déjà publié pour eux en 2023 un aide-mémoire concernant l'AIPD. La plupart de leurs réactions en retour sur l'utilisation de cet outil sont positives, et plusieurs responsables ont développé des modèles et des outils d'évaluation automatisés. Le PFPDT se félicite de ces initiatives privées à même de faciliter les ajustements nécessaires de l'AIPD.

L'AIPD dans les projets de la Confédération

Ainsi qu'escompté, plusieurs organes de la Confédération nous ont envoyé leurs AIPD pour avis. En effet, conformément aux directives du Conseil fédéral à ce sujet, les AIPD doivent être jointes aux consultations des offices relatives aux projets de loi (par ex. dans le cadre de la consultation de la loi sur les données relatives aux passagers aériens LDPA, cf. ch. 1.6).

Les compléments introduits par le PFPDT visaient en particulier à résumer clairement à l'adresse du Conseil fédéral et du Parlement les risques liés aux traitements de données envisagés et les mesures prises pour les limiter, afin que ces organes politiques puissent prendre leur décision en connaissance des risques résiduels encourus.

Mise en œuvre de l'obligation de journalisation

L'obligation de journalisation en vertu de l'art. 4 OPDo est applicable depuis le 1^{er} septembre 2023, date d'entrée en vigueur de la nouvelle loi sur la protection des données (LPD) et de l'ordonnance y relative (OPDo). Elle oblige les responsables de traitement et leurs sous-traitants à enregistrer les processus tels que le stockage, la modification, la lecture, la communication, l'effacement et la destruction des données lors de traitements automatisés de données personnelles. Les données de journalisation servent à déceler, suivre et clarifier les violations de la protection des données.

L'administration fédérale, qui utilise un grand nombre d'applications, est soumise dans son ensemble à l'obligation de journalisation. Depuis plus de vingt ans, cette obligation s'applique au traitement des données personnelles sensibles et des profils de personnalité; de plus, elle fait partie intégrante de la protection de base des TIC dans l'administration fédérale (ch. T2.1 c et ch. 5) que doit mettre en œuvre chaque unité administrative de la Confédération. La journalisation de données personnelles ordinaires est aussi une pratique courante lorsque la Confédération doit gérer d'importants systèmes d'information tels que GEVER, le système de gestion des dossiers électroniques.

Dispositions transitoires en vue de l'introduction de la journalisation des lectures

L'art. 46 OPDo contient une disposition transitoire visant à concilier l'introduction de la fonctionnalité de journalisation des lectures requise à l'art. 4, al. 2, OPDo avec les cycles de développement des systèmes informatiques (TIC). Cette disposition prévoit que l'extension de l'obligation de journalisation pour les systèmes non soumis à la directive Schengen (UE) 2016/680 ne s'applique que trois ans après l'entrée en vigueur de l'OPDo (donc à partir du 1^{er} septembre 2026) ou à la fin du cycle de vie du système. De ce fait, cette obligation

peut être suspendue jusqu'à ce que des ajustements inhérents au système soient de toute façon nécessaires. Cette réglementation a pour but d'éviter que tous les systèmes d'information du gouvernement fédéral soient adaptés en une seule fois, au 1^{er} septembre 2026.

Défis et mesures

L'obligation de journalisation s'applique aussi bien aux responsables du traitement de données qu'à leurs sous-traitants. Ils sont tenus de journaliser les traitements automatisés de données personnelles telles que l'enregistrement, la modification, la lecture, la communication, l'effacement et la destruction des données. Cette journalisation assure la transparence requise et permet de réagir rapidement en cas de violation de la protection des données. Les données des procès-verbaux de journalisation servent à détecter, suivre et analyser les violations de la protection des données.

Cependant, l'obligation de journalisation peut entraîner une charge de travail supplémentaire considérable pour les opérateurs d'applications, notamment l'adaptation et la mise à l'échelle progressives de l'infrastructure informatique existante aux nouvelles exigences.

Sur la base de valeurs empiriques, l'Office fédéral de l'informatique et de la communication (OFIT) a établi une estimation des coûts dont les résultats, notamment dans le cadre de la consultation des offices sur l'OPDo, ont mis en lumière des demandes, fondées sur l'analyse des risques, visant à limiter l'obligation de journalisation. Le PFPDT organisera en 2025 une table ronde avec les services concernés de l'administration fédérale de sorte à tenir dûment compte de ces demandes dans le cadre des conditions légales.



← 2



1.2 Justice, police, sécurité

CYBERCRIMINALITÉ

Les enquêtes menées contre l'entreprise Xplain et les offices fédéraux fedpol et OFDF se terminent par l'acceptation des recommandations

Au cours des trois enquêtes ouvertes contre fedpol, l'OFDF et l'entreprise Xplain, le PFPDT a constaté des violations de la loi sur la protection des données. Les résultats publiés de ces enquêtes ont montré d'une part que fedpol et l'OFDF avaient transmis des données personnelles à l'entreprise privée Xplain sans prendre les mesures nécessaires de protection des données et, d'autre part, que Xplain les

avait conservées en violation de la protection des données et, en partie, de ses obligations contractuelles.

Dans ses rapports, le PFPDT conclut que ni l'Office fédéral de la police (fedpol), ni l'Office fédéral de la douane et de la sécurité des frontières (OFDF) n'avaient clairement convenu avec l'entreprise privée Xplain si, et dans quelles conditions, des données personnelles de ces offices fédéraux pouvaient être conservées sur le serveur de Xplain

dans le cadre de services d'assistance. Ces deux offices auraient dû néanmoins préciser expressément dans quelle mesure ces données personnelles pouvaient être transmises à Xplain et conservées par celle-ci. Le processus en place était conçu de telle sorte que des données personnelles étaient transmises à Xplain dans le cadre de cas d'assistance sans que des exigences précises aient été définies pour la transmission et le respect de la sécurité des données auprès de Xplain. Il en résultait une accumulation de données non structurées de ces deux offices fédéraux sur le serveur de Xplain. Le PFPDT a également constaté que la

Recommandations pour la sous-traitance

Pour l'exploitation et le développement de ses applications numériques, l'administration fédérale collabore avec des entreprises privées qui se voient ainsi confier le traitement de données personnelles. L'analyse de l'attaque au rançongiciel contre Xplain, effectuée dans le cadre de l'activité de surveillance, illustre de manière exemplaire les risques élevés et les dommages potentiels qui accompagnent de tels transferts de données. Les recommandations acceptées par les différentes parties obligent désormais l'administration fédérale et ses prestataires privés dans leur ensemble à recenser les risques élevés et à prendre en temps utile des mesures propres à les abaisser à un niveau acceptable.

Selon les conclusions des trois enquêtes, ils doivent respecter les principales dispositions suivantes de la législation fédérale sur la protection des données :

- Les organes fédéraux sont « responsables » de la protection des données. Lorsqu'ils sous-traitent des tâches à des entreprises privées (par ex. des tâches de support), ils doivent à ce titre déterminer s'il est nécessaire que des données personnelles quittent l'infrastructure informatique protégée de l'administration fédérale et s'il faut absolument permettre à des mandataires privés d'accéder à cette infrastructure. Il faut aussi

se poser la question d'une anonymisation de ces données personnelles avant leur transfert et examiner s'il y a lieu de prendre d'autres mesures techniques et organisationnelles afin d'éviter des violations de la protection des données.

- Après avoir analysé les risques en matière de protection des données et fixé les mesures appropriées permettant de les réduire au maximum, les organes fédéraux et les entreprises privées doivent documenter clairement et intégralement les processus de mise en œuvre (par ex. flux de données, anonymisation, modalités d'accès). Les organes fédéraux doivent en outre fixer contractuellement avec leurs mandataires les mesures techniques et organisationnelles requises et si nécessaire, prévoir des peines conventionnelles.
- Les sous-traitants privés sont tenus de respecter le cadre des directives et des obligations contractuelles en ce qui concerne l'étendue, l'intensité et la durée du traitement de données personnelles. Les mesures propres à permettre le respect de ces directives sont des concepts qui prévoient l'effacement des données en temps utile, la sensibilisation et la formation des collaborateurs ainsi que la réalisation régulière d'audits internes ou externes.

LÉGISLATION

quantité de données personnelles transmises dans le cadre de ce processus était disproportionnée.

Fin mai 2024, fedpol et l'OFDF ainsi que Xplain ont accepté dans leur intégralité les recommandations du PFPDT relatives à l'attaque par rançoniciel visant Xplain.

Les procédures d'établissement des faits contre l'OFDF et fedpol concernant la licéité des accès de collaborateurs de l'OFDF au système de recherches informatisées de police RIPOL, exploité

par fedpol, ont été dissociées des procédures concernant Xplain et sont toujours en cours.

Contrôles au sein de l'administration fédérale

Dans son communiqué de presse du 4 juin 2024 clôturant la procédure en l'affaire Xplain, le PFPDT a demandé à l'administration fédérale et à ses sous-traitants privés de réexaminer leur collaboration en matière de traitement des données personnelles à la lumière des conclusions de ses trois enquêtes. Dans le même communiqué, le PFPDT a annoncé des contrôles dans l'ensemble de l'administration.

En septembre 2024, le PFPDT a procédé aux premiers contrôles aléatoires au sein de l'administration fédérale.

Révision de la loi sur le renseignement

Une révision de la loi fédérale sur le renseignement (LRens) s'impose en raison de la redéfinition et de l'élargissement des traitements de données provenant des activités de renseignement.

À la suite de l'enquête administrative concernant l'acquisition d'informations par le domaine Cyber du Service de renseignement de la Confédération (SRC), le Département de la Défense, de la protection de la population et des

Plateforme nationale de recherche policière POLAP

Au cours de l'année 2024/2025, le PFPDT a multiplié les critiques à l'encontre du projet d'interconnexion nationale des systèmes de police cantonaux sur une plateforme appelée POLAP qui serait gérée avec la participation de la Confédération (cf. 31^e RA, ch. 1.2). L'arrêt 1C_63/2023 du Tribunal fédéral du 17 octobre 2024 légitime ces critiques.

Le Tribunal fédéral devait se prononcer sur un recours formé contre une réglementation du canton de Lucerne qui devait permettre la connexion des systèmes cantonaux à POLAP dès la mise en service de cette plateforme. Le Tribunal fédéral a annulé la réglementation en question au motif qu'elle ne constituait pas une base légale suffisamment précise pour l'accès prévu aux données. En outre, elle contrevenait au principe de proportionnalité tout en portant atteinte aux droits des personnes concernées par la procédure d'assistance administrative.

Les autorités de protection des données de la Confédération et des cantons ont recommandé de revoir le projet de convention de la Conférence des directrices et directeurs des départements cantonaux de justice et police, concernant l'échange de données policières impliquant la Confédération, recommandation qui n'a pas encore été effectuée. De son côté, fedpol, n'a pas encore élaboré la base légale expresse annoncée pour l'exploitation de POLAP, qui fait partie intégrante de la stratégie nationale de lutte contre le crime organisé. Le PFPDT part du principe que la Confédération et les cantons poursuivront leurs travaux cette année et qu'ils veilleront à l'informer lui, de même que ses homologues cantonaux, des prochaines étapes, et à les consulter en temps utile surtout les questions relevant de la sécurité des données.

sports (DDPS) a scindé en deux parties les travaux en cours concernant la révision de la LRens. Le PFPDT a déjà pris position sur la première partie visant entre autres à modifier le droit d'accès (cf. 29^e R.A, ch. 1.2).

La révision prévoit notamment une approche entièrement nouvelle des traitements de données provenant des activités de renseignement. Plus précisément, le projet de loi nomme les catégories de données personnelles traitées en lieu et place des différents systèmes d'information. Une procédure de consultation complémentaire concernant la deuxième partie de la révision devrait avoir lieu d'ici juillet 2025. Le PFPDT accompagne les travaux.



1.3 Économie et société

TRACKING MULTIPLATEFORME

Prise de position de Ricardo et TX Group concernant les recommandations du PFPDT

Au cours de l'année sous revue, le PFPDT a publié son rapport final après avoir donné la possibilité à Ricardo et à TX Group de prendre position sur ses recommandations. Le Préposé examine actuellement la suite à donner.

Au printemps 2024, le PFPDT clôturait la procédure menée sous l'ancien droit concernant la plateforme d'enchères Ricardo et le tracking multiplateforme

effectué à des fins de publicité ciblée, qu'il avait ouverte à l'encontre de Ricardo et de TX Group (TX).

Dans son rapport final, le PFPDT recommandait en particulier à Ricardo d'adapter sa plateforme de façon à ce que les utilisateurs soient informés de manière claire et transparente du suivi effectué par TX et de ses finalités et d'obtenir le consentement de ses utilisateurs avant de communiquer les données à TX à des fins de publicité ciblée. Il recommandait à TX de supprimer les données déjà transmises dans ce contexte, dans la mesure où la société ne disposerait pas du consentement requis (cf. 3^e RA, ch. 1.3).

Les deux sociétés se sont prononcées sur le rapport final et les recommandations du PFPDT. Dans leurs prises de position respectives, Ricardo et TX contestent la qualification des données en tant que données personnelles et par conséquent l'application de la loi sur la protection des données. Les sociétés ont fait savoir qu'elles n'allait pas suivre les recommandations, qu'elles considèrent juridiquement infondées ou sans objet, car elles se réfèreraient à un état de fait dépassé et à une loi entretemps abrogée.

Guide relatif aux traitements de données au moyen de cookies et de technologies similaires

L'utilisation de cookies et de technologies similaires par les exploitants de sites web et d'applications ainsi que les traitements de données en découlant concernent toutes les personnes qui utilisent Internet quotidiennement. En application de l'ancienne LPD, le PFPDT s'était penché sur ces traitements de données dans le cadre des clarifications concernant la plateforme d'enchères Ricardo et Digitec Galaxus. Depuis l'entrée en vigueur de la nouvelle loi sur la protection des données, qui a mené entre autres à l'abandon de la notion de profil de personnalité au profit des notions de « profilage » et de « profilage à haut risque », la question se pose – pour les exploitants de sites web et d'applications – de savoir ce qu'il faut désormais prendre en compte lors de l'utilisation de cookies et de technologies similaires.

Afin de clarifier la situation sur ce point et de préciser sa pratique de surveillance sous le nouveau droit, le PFPDT a publié un guide le 22 janvier 2025. Ce guide s'adresse en premier lieu aux responsables privés, mais contient aussi des renvois ponctuels aux dispositions spéciales applicables aux organes fédéraux.

Ce guide explique :

- comment la disposition spéciale de l'art. 45c de la loi fédérale sur les télécommunications doit être appliquée cumulativement aux normes générales de la LPD,
- quelle est la responsabilité des exploitants de sites web lorsqu'ils utilisent des services tiers et des cookies tiers,
- comment ils peuvent remplir leurs devoirs d'informations dans ce contexte et
- comment ils peuvent accorder les droits « de conception » des personnes concernées et les mettre en œuvre techniquement de sorte qu'un consentement justifié soit obtenu de manière valable ou que le droit légal d'opposition soit accordé de manière juridiquement satisfaisante.

COMPTÉ CLIENT

Le PFPDT s'est réservé la possibilité de faire procéder aux adaptations nécessaires de la plateforme Ricardo par des mesures appropriées s'il devait constater que les manquements relevés dans son rapport final perduraient. Le 22 janvier 2025, il a publié un guide sur l'utilisation des cookies, qui contient des indications concrètes sur les exigences à respecter pour être en conformité avec la nouvelle LPD.

À la demande de Ricardo et de TX, le PFPDT a publié une version caviardée de son rapport final en octobre 2024 accompagné d'un communiqué de presse. Suite à une demande d'accès accordée en vertu de la loi sur la transparence (LTrans), le rapport non caviardé a été publié sur le site web du PFPDT en mars 2025.

Le PFPDT accompagne la mise en œuvre des recommandations acceptées par un shop en ligne

Par ses recommandations formelles, le PFPDT a clos le 15 avril 2024 son examen des faits concernant l'entreprise suisse de vente en ligne Digitec Galaxus. Il accompagne actuellement la mise en œuvre, prévue pour le second trimestre 2025, de la recommandation acceptée par cette entreprise.

La recommandation acceptée par la plateforme en ligne Digitec Galaxus concernait l'impossibilité, pour le client, de s'opposer aux traitements de données examinés, notamment ceux qui étaient effectués à des fins de marketing. De plus, le client ne pouvait pas passer commande sans créer un compte client et le traitement des données en découlant n'était pas absolument nécessaire à l'exécution du contrat de vente; de ce fait, le lien entre le compte client et la commande était contraire au principe de proportionnalité (cf. 31^e RA, ch. 1.3). Le PFPDT a

donc recommandé à Digitec Galaxus de modifier son traitement des données de sorte qu'il n'empêtre pas plus que nécessaire sur le droit à l'autodétermination informationnelle de ses clients.

En décembre 2024, Digitec Galaxus a proposé une solution au PFPDT pour la mise en œuvre des recommandations acceptées et que le Préposé avait formulées sous l'égide de l'ancienne LPD. Digitec Galaxus nous a informé que la mise en œuvre concrète des recommandations aurait lieu au cours du second trimestre de l'année 2025. Le 22 janvier 2025, le PFPDT a publié un guide détaillé sur l'utilisation des cookies; ce guide contient des indications concrètes que Digitec Galaxus doit respecter pour se conformer à la protection des données en vertu de la nouvelle LPD.

CAMPAGNE EN LIGNE

Enquête contre l'association Forum Civique Suisse

Le PFPDT a examiné les traitements de données effectués par l'association Forum civique suisse (Bürgerforum Schweiz) dans le cadre de sa campagne en ligne « Pfarrer-Check ». Ces traitements incluent la collecte des coordonnées de prêtres, pasteurs et autres agents pastoraux dans le but de leur envoyer un questionnaire. S'ajoute à cela la gestion sur Internet d'une banque de données offrant notamment un accès public aux noms des personnes ayant reçu le questionnaire, et le cas échéant, la manière dont elles y ont répondu. Certaines d'entre elles ayant été enregistrées dans cette banque de données contre leur gré, le PFPDT a ordonné une mesure administrative à propos de laquelle le Tribunal administratif fédéral doit désormais se prononcer.

Au cours de l'année 2023, le PFPDT a été rendu attentif aux traitements de données effectués par le Forum civique suisse dans le cadre de sa campagne en ligne « Pfarrer-Check ». Cette campagne a pour objet de collecter les données de contact de personnes actives dans le secteur ecclésial (prêtres, pasteurs, membres de conseils d'église et

de synodes, employés d'universités, animatrices et animateurs jeunesse) – dont les adresses sont publiques – pour ensuite leur envoyer un questionnaire. Les réponses à ce questionnaire devraient permettre d'établir si ces personnes partagent les convictions religieuses du Forum civique suisse. Le Forum, qui exploite une banque de données en accès public sur la base de ces informations, a refusé de tenir compte des demandes d'effacement des personnes y figurant contre leur gré (cf. 31^e RA, ch. 1.3).

Désireux d'étudier de plus près les traitements en question quant à leur conformité à la législation sur la protection des données, le PFPDT a ouvert une enquête formelle fin 2023. Dans ce contexte, il a conclu que le Forum civique suisse enfreignait le principe de proportionnalité en publiant, dans sa base de données accessible au public, des données de personnes qui n'avaient été

que « saisies » ou simplement « contactées ». Du point de vue du PFPDT, ces données ne sont pas appropriées pour obtenir des informations fiables sur les convictions religieuses des personnes concernées, ni nécessaires pour démontrer la représentativité de l'enquête. Leur publication nécessite donc un motif justificatif en vertu de la loi sur la protection des données.

De l'avis du PFPDT, il n'existe aucun intérêt prépondérant privé ou public qui justifierait de faire figurer dans la base de données le statut « saisies » ou « contactées » pour des personnes répertoriées publiquement ailleurs. Par conséquent, même si elles sont répertoriées publiquement ailleurs, on ne peut enregistrer dans cette banque de données que les personnes qui y ont donné au préalable leur consentement juridiquement valable. Si une personne a déjà déposé une demande d'effacement, ses données doivent être effacées. Au printemps 2024, le PFPDT a ordonné une mesure administrative dans ce sens (cf. 31^e RA, ch. 1.3). Au cours de l'année sous revue, l'association Forum civique suisse a recouru contre cette mesure auprès du Tribunal administratif fédéral, dont la décision est encore attendue.



MARCHÉ DE L'IMMOBILIER

Questions non autorisées dans les formulaires de demande de location

Les formulaires fournis par les propriétaires en vue de la location d'un logement doivent respecter les principes de protection des données. Le PFPDT clarifie la situation juridique depuis l'entrée en vigueur de la nouvelle LPD et rappelle à l'ordre les gérances immobilières dont les formulaires portent sur des renseignements qui empiètent trop sur les droits de la personnalité des locataires potentiels.

Dès les années 90, le PFPDT a émis des recommandations portant sur le traitement des données personnelles de candidats à la location (cf. 4^e RA, 1996/1997, p. 49). La collecte de données auprès des locataires potentiels

est en principe autorisée dans la mesure où ces informations permettent de sélectionner des locataires adéquats, sur la base de critères objectifs. En particulier, le traitement des données doit être transparent et limité à des fins spécifiques. La finalité est définie par le projet de conclusion du contrat. Selon le principe de proportionnalité, seules les données qui remplissent objectivement cet objectif peuvent être collectées et traitées. Le traitement des données ne doit pas porter inutilement atteinte à la sphère privée des personnes concernées. Une décision de la Commission de protection des données de 1996 a largement confirmé l'avis du PFPDT et constitue, depuis lors, la pierre angulaire de sa longue pratique.

Au cours de l'année sous revue, le PFPDT a eu l'occasion de se pencher à nouveau sur cette question et a vérifié, sur la base d'exemples concrets, si sa pratique était toujours actuelle à la lumière de la nouvelle loi sur la protection des données. Il a reçu de nombreux signalements de personnes dénonçant des formulaires d'inscription ; les médias ont également attiré à plusieurs reprises son attention sur des cas douteux. Au

cours de cette année, le PFPDT a ainsi mené une campagne dont les mesures se sont déroulées sur trois niveaux :

Dans le cadre de son mandat de sensibilisation, le PFPDT a notamment adapté l'« Aide-mémoire concernant les formulaires d'inscription relatifs à la location d'un appartement » afin de clarifier les exigences en matière de protection des données. Il a simplifié les formulations et les a complétées par des exemples illustrant comment les propriétaires peuvent obtenir et traiter les données des locataires potentiels dans le respect des principes de la LPD.

Dans le cadre de son mandat de conseil, le PFPDT a discuté avec la SVIT (Association suisse de l'économie immobilière), et avec l'APF (Association des propriétaires fonciers). Il a confirmé sa

position à propos du caractère illicite de la demande de renseignements sur l'état civil, la nationalité, le lieu d'origine, la religion, la situation actuelle en matière de logement et les copies de la carte d'identité. Les arguments des spécialistes du secteur ont toutefois convaincus le PFPDT qu'une copie de l'extrait du registre des poursuites peut être exigée de la part de tous les candidats dès la procédure d'inscription, et pas seulement du locataire retenu, comme le défendait jusqu'à présent le PFPDT. Il est toutefois important que ces copies soient immédiatement détruites si les locataires potentiels ne sont pas sélectionnés. L'aide-mémoire a été adapté dans ce sens. Le PFPDT a également transmis cette version révisée à l'Association des locataires.

Par ailleurs, le PFPDT a profité de ces entretiens pour attirer l'attention des spécialistes sur d'autres problèmes touchant la protection des données au cours du processus de location, par exemple la communication d'informations sur le locataire en place afin de convenir d'une visite du logement ou encore la prise de photos du logement tel qu'il est habité, sans le consentement du locataire. À la suite à cet échange,

la SVIT a complété ses recommandations concernant les données personnelles figurant sur les formulaires d'inscription en vue de la location de logements.

Dans le cadre de son activité de surveillance, le PFPDT a examiné les formulaires d'inscription qui lui ont été signalés, fournis par différentes régies immobilières en Suisse alémanique et en Suisse romande. Lorsque certaines informations demandées violaient le principe de proportionnalité, il a écrit aux responsables dans le cadre d'une intervention à bas-seuil. Il y était notamment demandé la nationalité, l'état civil ou l'existence d'une curatelle.

D'autres questions non autorisées portaient sur le logement antérieur, par exemple la durée du bail, le nombre de pièces ou le montant du loyer. Certaines régies immobilières exigeaient en outre systématiquement les fiches de salaire des trois derniers mois ou les originaux des extraits du registre des poursuites, ou encore leur propre formulaire contenaient une déclaration de consentement générale qui permettait au futur bailleur de se procurer toutes les autres informations nécessaires sur le candidat. Dans un cas particulier, la régie immobilière avait même engagé un détective privé pour enquêter auprès de tiers sur un locataire potentiel.

Même si les interventions du PFPDT ont majoritairement produit l'effet désiré, toutes les régies immobilières contactées ne se sont pas montrées disposées à modifier volontairement leurs pratiques. Ainsi, le traitement des données personnelles accompagnant la conclusion d'un contrat de location devrait continuer à occuper le PFPDT au cours de l'année à venir en raison de la numérisation croissante du secteur immobilier.



1.4 Santé

DOPAGE

Transmission de données médicales d'athlètes suisses

La transmission systématique de dossiers médicaux à l'Agence mondiale antidopage (AMA) à des fins de contrôles ponctuels serait disproportionnée et ne reposerait pas sur une base légale suffisante. L'AMA avait demandé à Swiss Sport Integrity (SSI) de mettre en œuvre cette mesure. Toutefois, suite à l'intervention du PFPDT, SSI pourra poursuivre sa pratique actuelle.

Dans le cadre de la lutte contre le dopage, Swiss Sport Integrity (SSI) collabore avec l'AMA qui a notamment pour rôle de veiller au respect du Programme mondial antidopage. L'AMA a conduit un audit de SSI et a ordonné un certain nombre de mesures. L'une de ces mesures concernait les données des athlètes au bénéfice d'une autorisation d'usage à des fins thérapeutiques (AUT), soit l'autorisation spéciale pour un athlète de pouvoir consommer une substance dopante dans le cadre d'une thérapie. Elle visait à ce que SSI transmette systématiquement à l'AMA les dossiers médicaux de tous les athlètes au bénéfice d'une AUT, afin de pouvoir procéder

à des contrôles ponctuels. Jusqu'à présent, SSI ne transmettait qu'un bref résumé de la situation médicale de l'athlète. Le dossier médical n'était envoyé que si l'AMA souhaitait effectivement procéder au contrôle d'un athlète en particulier. Ce changement de pratique aurait donc entraîné un traitement de données bien plus conséquent, raison pour laquelle SSI a pris contact avec le PFPDT.

Dans un courrier que SSI a ensuite transmis à l'AMA, le PFPDT a rappelé que tout traitement de données personnelles doit respecter le principe de proportionnalité. Après examen du cas, il est arrivé à la conclusion que la modification demandée par l'AMA n'était pas proportionnée. En effet, l'envoi systématique des dossiers médicaux de tous les athlètes au bénéfice d'une

AUT n'est pas nécessaire à l'activité de surveillance de l'AMA, qui n'effectue que des contrôles ponctuels. La pratique actuelle donne satisfaction et permet à l'AMA d'effectuer des contrôles lorsqu'elle le souhaite, de sorte que le changement demandé ne répond pas à un besoin essentiel. De plus, l'intérêt des athlètes à ne transmettre leurs données sensibles qu'en cas de contrôle effectif est important. Dans ce contexte, le PFPDT a aussi rappelé que tout envoi de données à un tiers, qui plus est à l'étranger (l'AMA est basée au Canada), représente un risque supplémentaire : cette prise de risque doit donc être légitimée par un intérêt prépondérant, ce qui n'est pas le cas en espèce.

De plus, le PFPDT a également relevé que SSI ne disposait vraisemblablement pas d'une base légale suffisamment spécifique pour autoriser une transmission de données systématique, tel qu'envisagée.

L'AMA a tenu compte de la position du PFPDT. Elle a accepté que SSI poursuive sa pratique actuelle et a clos la procédure la concernant.

FORMULAIRES PATIENTS

Entre devoir d'information et consentement

Le formulaire de consentement pour les patients remis lors de leur visite chez un médecin ou un autre thérapeute soulève de nombreux questionnements. Au vu de la confusion que ce formulaire génère parfois en incorporant plusieurs aspects juridiques, le PFPDT entend sensibiliser les fournisseurs de prestations, respectivement leurs faîtières, sur les exigences de la LPD à ce sujet.

Durant l'année sous revue, le PFPDT a régulièrement été sollicité sur des questions en lien avec les formulaires de consentement des patients. Il publiera prochainement sur son site internet une information à l'intention des fournisseurs de prestations, respectivement de leurs faîtières, afin qu'ils adaptent leurs formulaires aux exigences de la Loi fédérale sur la protection des données (LPD) si nécessaire.

Dans les grandes lignes, sous l'angle de la protection des données, il convient de bien distinguer entre les exigences liées au devoir d'information et celles du consentement.

Le devoir d'information

S'agissant des médecins et autres thérapeutes, le devoir d'information n'est pas nouveau puisqu'il préexistait sous l'ancienne LPD lorsque le traitement portait sur des données sensibles, telles les données de santé. À noter qu'avec l'entrée en vigueur de la nouvelle LPD, le devoir d'information a été élargi à toutes les catégories de données personnelles.

L'information doit comprendre toutes les indications nécessaires pour garantir la transparence du traitement et permettre à la personne concernée de faire valoir ses droits. L'information doit être adaptée aux situations et doit au moins porter sur les données visées à l'art. 19 al. 1 LPD. Le degré de détail dépend du type de données collectées, de la nature et de l'ampleur du traitement, du risque d'atteinte et de la gravité de l'atteinte aux droits de la personnalité.

Le devoir d'information n'est soumis à aucune exigence de forme. L'information doit être transparente, concise, compréhensible et facilement accessible. Même si l'information peut être donnée oralement, pour des raisons de preuve liées au respect du devoir, il peut être pertinent de documenter l'information ou de procéder par écrit. Cependant le patient est libre de lire (ou non) le document et n'est pas tenu d'en accuser réception ni de confirmer son accord. En pratique, des précisions dans un formulaire ou la transmission d'une feuille d'information spécifique (éventuellement à signer pour prise de connaissance) sont suffisantes.

Le consentement

Ici aussi, la nouvelle LPD n'apporte pas de modification fondamentale. Le consentement n'est en principe pas une condition préalable au traitement, mais entre en considération en tant que motif justificatif en particulier lors de communication de données personnelles sensibles à des tiers. Pour les autres cas de figure, le traitement peut éventuellement se justifier par un intérêt privé prépondérant lorsque le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat.

Pour être valable, outre le fait qu'il doit être donné avant ou en même temps que le début du traitement pour lequel il est requis, le consentement doit être libre et éclairé : la personne concernée doit recevoir au minimum les informations de l'art. 19 LPD. En fonction du contexte et de la nature des données traitées, il est parfois nécessaire d'ajouter des précisions pour que la personne concernée soit en mesure d'évaluer la portée de l'autorisation ; spécifique : le consentement doit être donné pour un traitement ou plusieurs traitements déterminés et couvrir l'ensemble des finalités du traitement. Il ne peut pas être donné de manière générale pour n'importe quel traitement futur.

Le consentement reste libre dans sa forme. Il n'est donc pas nécessaire qu'il soit donné par écrit. Le responsable du traitement doit cependant apporter la preuve du consentement. Il a donc un intérêt documenter le consentement même si celui-ci ne dépend d'aucune forme.

DOSSIER ÉLECTRONIQUE DU PATIENT

Révision complète de la loi et financement transitoire

Le dossier électronique du patient (DEP) ne cesse de se développer. Le projet de révision complète de la loi mis en consultation a montré qu'une centralisation plus marquée est souhaitée. Sur cette base, le Conseil fédéral a décidé qu'il incombera désormais à la Confédération de mettre à disposition l'infrastructure technique et d'en assurer son développement. Dans l'intervalle, le Parlement a accepté, un financement transitoire pour soutenir l'exploitation et le développement du DEP. Le PFPDT suit le dossier.

En été 2023, le Conseil fédéral a mis en consultation le projet de révision complète de la loi sur le dossier électronique du patient (DEP) sur lequel le PFPDT avait pris position (cf. 31^eRA, ch. 1.4). Dans ce cadre, plusieurs mesures étaient envisagées afin de continuer à améliorer et à développer le dossier électronique du patient, par exemple en obligeant tous les fournisseurs de prestations à s'y enregistrer ou en introduisant un modèle d'opt-out (droit d'opposition au lieu du consentement explicite). En outre, la révision contient une réglementation plus claire des rôles de la Confédération et des cantons dans le cadre du DEP.

Au vu des critiques émises quant à la structure décentralisée du DEP, le Conseil fédéral prévoit désormais une centralisation plus marquée du dossier électronique. Sur cette base, il a décidé lors de sa séance du 27 septembre 2024 qu'il incombera désormais à la Confédération de mettre à disposition l'infrastructure technique et d'en assurer son développement. Jusqu'à présent, les différentes infrastructures techniques de DEP sont mises à disposition par les communautés et communautés de référence, lesquels recourent à différents fournisseurs de plateformes informatiques.

Le message relatif à la révision complète inclut cette modification et sera vraisemblablement soumis au Parlement à l'automne 2025.

Financement transitoire, consentement et accès aux services de recherche des données

Étant donné que la révision complète de la loi nécessaire au développement du dossier électronique du patient prendra plusieurs années, le Conseil fédéral a présenté au Parlement, dans le cadre d'une révision séparée de la loi sur le DEP, un financement transitoire pour les fournisseurs de DEP (communautés de référence) afin d'encourager la diffusion et l'utilisation immédiate du DEP. Pour soutenir son exploitation et son développement, le Parlement a approuvé au printemps 2024 une aide financière à hauteur de 30 francs par DEP ouvert à verser pendant cinq ans à compter de l'entrée en vigueur de

la modification de la loi susmentionnée. Ce financement transitoire est entré en vigueur le 1^{er} octobre 2024.

Cette révision partielle permettra également d'inscrire le DEP comme un instrument de l'assurance obligatoire des soins (AOS) tout en simplifiant le processus d'ouverture des dossiers. Les patients peuvent désormais confirmer leur consentement pour l'ouverture d'un DEP avec un moyen d'identification électronique d'un éditeur certifié; une signature manuscrite ou numérique n'est plus nécessaire. Par ailleurs, les cantons auront accès au service de recherche des institutions de santé et des professionnels de la santé afin de vérifier le respect de l'obligation pour les hôpitaux, les maisons de naissance et les établissements médico-sociaux, ainsi que les médecins nouvellement admis depuis le 1^{er} janvier 2022, de s'affilier à une communauté certifiée ou à une communauté de référence.

Le PFPDT continuera à suivre activement le développement du DEP et à veiller au respect des exigences de la protection des données, notamment lors des consultations des offices relatives à sa mise en œuvre ou dans le cadre de questions spécifiques.

1.5 Travail

DROIT DU PERSONNEL DE LA CONFÉDÉRATION

Plateforme Whistleblowing

Le PFPDT est intervenu par différentes prises de position pour que les traitements de données afférents aux dénonciations et aux signalements whistleblowing annoncés par les employés de la Confédération soient réglementés de manière plus précise au niveau de la loi. Dans le cadre du projet de révision de la loi sur le personnel de la Confédération (LPers), le PFPDT a pris position en faveur d'une amélioration des dispositions réglementant les traitements de données effectués lors des annonces faites à titre de lanceurs d'alerte (signalements whistleblowing). Les employés de la Confédération sont en effet tenus de dénoncer tous les crimes et délits poursuivis d'office dont ils ont eu connaissance ou qui leur ont été signalés dans l'exercice de leur fonction. Ils doivent les communiquer à leurs supérieurs, au Contrôle fédéral des finances (CDF) ou aux autorités de poursuite pénale. Ils peuvent également signaler d'autres irrégularités qu'ils ont constatées ou dont ils ont eu connaissance dans l'exercice de leur fonction.

Or dans sa version actuelle, l'article 22a LPers prévoyant les annonces à la plateforme whistleblowing du CDF est lacunaire. Si la tâche légale du CDF est réglée dans la LPers et que le registre

whistleblowing est bien déclaré au PFPDT, les traitements de données en tant que tels ne sont pas définis au niveau de la loi, cette dernière prévoyant uniquement que « le CDF établit les faits et prend les mesures nécessaires ». Or les traitements de données personnelles sensibles que le CDF effectue doivent être réglés de manière détaillée dans la loi. Ce d'autant plus que les dénonciations peuvent être nominatives et que certaines dénonciations impliqueront des personnes précises et des données sensibles, tels les cas d'indiscrétions ou de délits relevant du droit pénal (corruption, détournement de fonds, irrégularités dans les marchés publics ...).

Tenant compte des prises de position du PFPDT émises durant les procédures de consultation des offices, des modifications ont été apportées au niveau des projets de révision de

trois législations fédérales différentes. Ces modifications concernent tant les précisions à apporter sur les annonces whistleblowing elles-mêmes et leurs processus que sur les traitements de données qui en découlent.

Ainsi le projet de modification de l'article 22a LPers a été complété avec des précisions sur les conditions de dénonciations et de signalements et des clarifications sur les organes auprès de qui celles-ci peuvent être effectuées. En particulier la possibilité pour les employés du Département fédéral des affaires étrangères (DFAE) de signaler directement auprès de la plateforme du DFAE a été clairement réglée au niveau de la loi.

D'autre part, des dispositions spécifiques aux traitements de données effectués par le CDF dans ses activités touchant aux annonces whistleblowing ont été introduites dans un nouvel article 10a de la Loi fédérale sur le Contrôle fédéral des finances (LCF). Ce projet de disposition règle notamment l'exploitation de la centrale d'enregistrements des signalements et des dénonciations, les traitements de données sensibles qui y sont effectués ou encore les communications de données auprès d'autres autorités.

Enfin, les traitements de données issues des annonces effectuées par le biais de la plateforme du DFAE ont été réglementés dans la Loi fédérale sur le traitement des données personnelles par le Département fédéral des affaires

DROIT DU PERSONNEL DE LA CONFÉDÉRATION

étrangères (RS 235.2). Ainsi une nouvelle section 10 « Personnes concernées par des signalements relatifs à des crimes, à des délits ou à des irrégularités » a été introduite dans le projet afin de réglementer les traitements de données que le DFAE effectuera en relation avec des annonces relevant de l'art. 22a LPers qui seront déposées sur sa plateforme whistleblowing.

Ces précisions développées sur la base des prises de position du PFPDT et introduites dans le cadre de ces révisions de lois fédérales assureront une sécurité juridique s'agissant des traitements de données effectués dans le cadre des dénonciations et des signalements whistleblowing et apporteront au cadre légal la densité normative adéquate.

Profilage dans le cadre des évaluations et de la recherche active de personnel

Dans le cadre de la révision de la loi sur le personnel de la Confédération, le PFPDT s'est engagé, à différentes reprises, pour que la base légale du profilage dans le cadre des évaluations et de la recherche active de personnel soit suffisamment précise et transparente. En outre, il a demandé que ces méthodes de traitement de données soient précédées d'une analyse d'impact sur la protection des données, ce qui permet d'évaluer les risques associés et de définir les mesures de protection adéquates.

Le PFPDT s'est prononcé sur différents aspects de la protection des données dans le cadre de la révision de la loi sur le personnel de la Confédération (LPers). Avec l'entrée en vigueur de la nouvelle LPD, la notion de « profil de la personnalité » a été supprimée et deux notions ont été introduites, le « profilage » et le « profilage à risque élevé ». La LPers doit donc être adaptée à cette nouvelle terminologie. À ce propos, deux activités sont particulièrement importantes : l'assessment (évaluations et tests

de personnalité concernant candidats et employés) et la recherche active de personnel. Alors que l'assessment était déjà prévu dans la LPers actuelle, le processus de recherche active de personnel, c'est-à-dire le traitement d'informations sur des personnes qui ne sont ni candidats ni employés, n'était pas encore inscrit dans la loi.

Afin que la Confédération, en tant qu'employeur, puisse continuer à utiliser les assessments dans le domaine du recrutement, des exigences des promotions et du potentiel de développement – par exemple pour évaluer l'aptitude d'un employé à réaliser un projet ou obtenir une promotion, ou encore pour recommander une carrière professionnelle à ses employés –, la disposition de la LPers a dû être adaptée en fonction de ce nouveau concept de profilage.

SURVEILLANCE DES EMPLOYÉS

En outre, la recherche active de personnel nécessite une base légale afin que les employeurs puissent utiliser les réseaux sociaux (par ex. LinkedIn) dans le but de rechercher des candidats qualifiés et d'évaluer l'aptitude d'une personne à occuper un poste spécifique.

Selon les circonstances, ce type de traitements de données peut non seulement constituer un profilage, mais également un profilage à risque élevé, car même des informations anodines sont rapidement à même de donner une image complète de la personne en question, permettant d'évaluer des aspects essentiels de sa personnalité. Il est donc nécessaire de créer une base légale suffisamment précise et transparente pour que les principes de légalité et de transparence soient respectés. Il convient notamment de déterminer les catégories de données

particulièrement sensibles, nécessaires aux différentes opérations, et les définir dans la loi. L'Office fédéral du personnel (OFPER) a complété et précisé cette disposition en fonction de la prise de position du PFPDT.

Le PFPDT a par ailleurs estimé que les méthodes de traitement prévues par la révision de la loi doivent faire l'objet d'analyses d'impact sur la protection des données, le profilage pouvant, en raison de la nature et de l'étendue du traitement, entraîner un risque élevé pour la personnalité des personnes concernées. Il faut donc identifier les risques associés et décrire les mesures de protection permettant d'y faire face. L'OFPER a procédé aux analyses de risque demandées, a constaté la présence de différents risques et défini les mesures permettant de les réduire. Parmi ces mesures, citons la réglementation légale des autorisations d'accès, diverses mesures de sécurité des données, la formation et la sensibilisation des employés, l'introduction de directives et la journalisation des traitements. Les analyses de risques ont été exposées dans le message du Conseil fédéral destiné aux Chambres fédérales.

Respect des principes de protection des données

L'utilisation de systèmes de surveillance sur le lieu de travail a conduit le PFPDT à intervenir à plusieurs reprises. Pour être conforme aux principes de la protection des données, un système de surveillance doit notamment être limité au strict nécessaire et les collaborateurs doivent être informés de manière adéquate. Au cours de l'année sous revue, le PFPDT a été fréquemment consulté sur la conformité de systèmes de surveillance vidéo avec les exigences de la protection des données. Dans certains cas, il est intervenu sur la base d'examens préliminaires et d'interventions à bas seuil et, dans ce contexte, a rappelé les principes de la protection des données. Il a par ailleurs ouvert une enquête portant sur un système de surveillance.



65797 km

D / B
PARK
N R

Un employeur ne peut traiter les données concernant son employé que dans la mesure où elles concernent l'aptitude de ce dernier à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail (principe de proportionnalité). L'employeur doit toutefois veiller à la santé de ses employés et protéger leur personnalité. Ainsi, il lui est interdit d'utiliser des systèmes de vidéosurveillance pour contrôler de manière ciblée leur comportement. S'il est nécessaire de recourir à un système de surveillance pour une autre raison, ce système doit être conçu de manière à ne porter aucune atteinte à leur santé et à leur liberté de mouvement. La surveillance doit donc être limitée au strict nécessaire.

Dans le cas d'une installation de vidéosurveillance, cela signifie par exemple que les enregistrements ne peuvent pas être utilisés pour surveiller le comportement des employés

et que l'employeur doit avoir pour ce faire un intérêt légitime qui l'emporte sur l'intérêt des employés à protéger leur personnalité. Le positionnement et les réglages des caméras vidéo doivent alors permettre que la zone d'enregistrement soit limitée au minimum et que les employés aient la possibilité de se retirer du champ de la caméra. Il est par ailleurs en général interdit de filmer dans la zone de pause.

Autre aspect important: la transparence. Avant la mise en place d'un système de surveillance, il faut que les employés soient informés de manière complète et compréhensible sur le type, le but et la portée du système. À cet égard, les lacunes dans la pratique sont légion: dans bien des cas, les employés ne sont pas suffisamment ou pas du tout informés de la mise en place de mesures de surveillance.

Le respect de ces principes est d'une importance capitale. En effet, le consentement donné dans le cadre de la relation de travail ne peut être invoqué que de manière limitée dans le contexte de mesures de surveillance étant donné que souvent, le rapport de subordination entrave la liberté de choix des employés.

Surveillance des employés

La surveillance des employés est un sujet auquel le PFPDT est régulièrement confronté : la saisie électronique du temps de travail, le traçage par GPS ou l'accès aux mails professionnels des employés constituent quelques exemples qui soulèvent fréquemment des questions de protection des données. Le PFPDT a clos la procédure d'établissement des faits concernant la saisie électronique des temps de travail dans une entreprise de nettoyage de bâtiments (cf. 27^e RA, ch. 1.6).

1.6 Transports

PROJET SWISSCOM BROADCAST

BIOMÉTRIE

Le PFPDT exige des réponses à propos du réseau de drones de Swisscom

Le réseau suisse de drones de Swisscom Broadcast permettra de déployer une nouvelle infrastructure pour les vols de drones automatisés dans les années à venir. Celle-ci devrait permettre d'utiliser ces drones en tant que service, par exemple pour des inspections d'infrastructures, des interventions policières ou en vue de la protection de zones étendues. Le PFPDT a procédé à des investigations auprès du prestataire de services Swisscom Broadcast afin de s'assurer qu'au cours de l'utilisation de cette infrastructure, les données personnelles seront traitées dans le respect de la législation. Ces vérifications ont montré que l'opérateur du réseau de drones prend les mesures nécessaires pour garantir la protection des données. Cette protection inclut, entre autres, la réalisation d'un examen préalable des risques avant la mise en service du réseau de drones, ainsi qu'une analyse d'impact relative à la protection des données s'il existe des risques élevés pour la personnalité ou les droits fondamentaux des personnes concernées. Le PFPDT restera attentif à la mise en place de cette infrastructure et s'entretiendra régulièrement avec l'opérateur à ce sujet.

Reconnaissance faciale à l'aéroport de Zurich

La reconnaissance faciale à l'aéroport de Zurich ne peut être introduite que si elle repose sur une base légale. Ce projet étant susceptible de présenter des risques substantiels pour les personnes concernées quant aux droits de la personnalité et aux droits fondamentaux, le PFPDT l'a examiné en détail. La société Flughafen Zürich AG a informé le PFPDT de son projet d'acquérir une technologie permettant l'identification des passagers par la reconnaissance faciale automatisée. En parallèle, il a été demandé au PFPDT d'établir une première évaluation du projet sous l'angle de la protection des données. Dès lors que les données biométriques qu'il est envisagé d'utiliser pour le contrôle des cartes d'embarquement des passagers et, de ce fait, pour leur identification doivent être qualifiées de données personnelles sensibles au sens de la LPD, ce genre de traitement de données comporte fondamentalement des risques élevés pour la personnalité et les droits fondamentaux des personnes concernées.

La société Flughafen Zürich AG exerçant son activité sur la base d'une concession d'exploitation conformément à la loi sur l'aviation, elle est considérée comme un organe fédéral au sens de la LPD. Les traitements de données personnelles sensibles par les organes fédéraux doivent reposer sur une base légale formelle. La révision en cours

de la loi sur l'aviation prévoit, dans la lignée des réglementations internationales, la possibilité d'utiliser des données biométriques pour contrôler les cartes d'embarquement. Cependant, d'ici l'entrée en vigueur de cette révision, la base légale requise fait défaut. L'utilisation de la reconnaissance faciale n'est donc possible que dans le cadre d'essais pilotes selon les dispositions de la LPD.

D'après les informations transmises par la société Flughafen Zürich AG, il est prévu d'utiliser la reconnaissance faciale uniquement dans le cadre du contrôle des cartes d'embarquement et sur une base volontaire. En outre, une signalisation bien visible indiquera, dans l'aéroport de Zurich, les zones dans lesquelles les passagers pourront à l'avenir faire enregistrer leurs données biométriques. Le PFPDT a analysé de très près le cadre juridique et technique du traitement en question et, dans le cadre de ses activités de surveillance, il continuera d'accompagner Flughafen Zürich AG dans le cas d'une mise en œuvre de ce projet.

PASSENGER NAME RECORDS

Loi sur les données relatives aux passagers aériens

Actuellement, la Suisse ne peut pas utiliser systématiquement les données relatives aux passagers aériens faute de base légale. La future loi sur les données relatives aux passagers aériens (LDPa) vise à combler cette lacune. Le Conseil fédéral a transmis le message relatif à cette loi au Parlement le 15 mai 2024. Le Conseil national et le Conseil des États ont approuvé la loi le 21 mars 2025. Le délai référendaire court jusqu'au 10 juillet 2025.

Au moment de réserver un billet d'avion, les passagers doivent communiquer à la compagnie aérienne ou à l'agence de voyage des informations personnelles telles que nom, prénom, coordonnées (y c. adresse et numéro de téléphone), moyen de paiement, etc. La constitution de ce dossier passager (Passenger Name Records [PNR]) fait l'objet de prescriptions internationales édictées par l'ONU, l'Organisation de l'aviation civile internationale (OACI) et l'UE. Le PNR sert à lutter contre le terrorisme et la grande criminalité. Les États-Unis font de sa communication une condition au maintien de la Suisse dans leur programme d'exemption de visa (Visa Waiver Program [VWP]) pour les voyages professionnels ou touristiques (cf. à ce propos l'article concernant BTLE et CEPD au ch. 1.7).

Le PFPDT a examiné le projet de LDPa et l'analyse d'impact relative à la protection des données personnelles effectuée par l'office fédéral compétent. Il a demandé des précisions dont il a été tenu compte. Le PFPDT reste attentif à l'évolution du projet.

CONTRÔLE AUX CFF

Plateforme NOVA des transports publics

Le PFPDT a vérifié les améliorations requises en matière de protection des données sur la plateforme de distribution centrale NOVA.

Après avoir constaté en 2022 une faille sur la plateforme de distribution centrale NOVA, que les CFF exploitent sur mandat de l'organisation de branche des transports publics Alliance SwissPass (cf. 29^e RA, ch. 1.7 et 31^e RA, ch. 1.6), le PFPDT a demandé aux CFF de réaliser

un audit afin de vérifier si les règles de suppression requises avaient été mises en place.

L'Alliance SwissPass a par ailleurs mis en vigueur au 1^{er} janvier 2024 des normes contraignantes en matière de sécurité de l'information (Prescription 591) que les entreprises de transport affiliées à NOVA doivent respecter. Les entreprises déjà affiliées étaient tenues de prouver au moyen d'une auto-évaluation, au plus tard pour la fin juin 2024, qu'elles respectaient ces normes. Le PFPDT a donc demandé aux CFF de lui établir également un rapport à ce sujet.

Les CFF ont indiqué au PFPDT avoir effectué début 2024 un audit au cours duquel il a été constaté que les règles de suppression définies avaient été intégralement mises en œuvre dans toutes les applications NOVA. Ils ont ajouté que les structures nécessaires à l'évaluation et au développement continu de la Prescription 591 avaient été créées. Au cours de l'année 2025, un tableau plus objectif de la situation actuelle devrait être dressé. Le PFPDT reste attentif à l'évolution du projet.



1.7 International

Du fait de la présence sur le marché suisse d'entreprises technologiques de premier plan à l'échelle mondiale, le PFPDT est confronté à diverses questions d'application de portée transnationale. Toutefois, pour y répondre, il dispose aujourd'hui de meilleurs instruments grâce à la modernisation des législations sur la protection des données aux niveaux suisse, européen et mondial.

La coopération transnationale avec les autorités étrangères de protection des données est indispensable si nous voulons que la LPD et les accords de droit international s'appliquent à ces entreprises actives dans le monde entier. Grâce à l'échange accéléré d'informations dans le cadre de l'entraide administrative internationale, d'une part la population concernée par les traitements de données est mieux protégée juridiquement, d'autre part les responsables de ces traitements bénéficient d'une meilleure sécurité juridique.

Dans le cadre informel des «groupes d'adéquation», le PFPDT s'est donc entretenu sur le sujet avec les autorités de protection des données des États auxquels l'UE a officiellement certifié qu'ils disposent d'un niveau de protection des données équivalent en matière de législation et d'application

de la protection des données. En ce qui concerne les plateformes sociales et d'autres offres de grandes entreprises internationales, nous avons dégagé des solutions permettant d'accélérer l'entraide administrative et de simplifier la transmission de documents.

D'une part, la Convention du Conseil de l'Europe sur la notification à l'étranger de documents en matière administrative (RS 0.172.030.5 – CEN), applicable aussi à la surveillance de la protection des données, permet une notification simplifiée des documents entre les États contractants. D'autre part, selon la LPD, le PFPDT est habilité à remettre aux autorités étrangères une déclaration spécifiant que la Suisse autorise la notification directe sur son territoire si elles lui accordent la réciprocité.

DATA SCRAPING

Déclaration commune finale sur l'extraction de données

Après avoir publié une déclaration commune sur l'extraction de données en 2023, le PFPDT et ses homologues de 16 autres autorités ont collaboré avec certaines des plus grandes entreprises de médias sociaux au monde. Cette collaboration s'est soldée par la publication d'une déclaration finale qui présente de nouveaux points à retenir pour l'industrie.

L'extraction massive de données personnelles provenant des plateformes de médias sociaux, notamment pour soutenir les systèmes d'intelligence artificielle, suscite des préoccupations croissantes. À cette fin, les autorités de protection des données du monde entier ont complété la déclaration commune de 2023 par une déclaration finale. Celle-ci fournit des directives supplémentaires pour aider les entreprises à s'assurer que les renseignements personnels de leurs utilisateurs sont protégés contre l'extraction illégale de données, notamment que les organisations :

- Se conforment aux lois sur la protection des renseignements personnels et des données lorsqu'elles utilisent des renseignements personnels (y compris ceux provenant de leurs propres plateformes) pour élaborer de grands modèles de langage à l'aide de l'intelligence artificielle ;

SWISS-US DPF

- Déploient une série de mesures de protection combinées, les révisent et les mettent à jour régulièrement pour tenir compte de l'évolution des techniques et des technologies d'extraction;
- S'assurent que l'extraction de données à des fins commerciales ou socialement bénéfiques est légitime et conforme à des modalités contractuelles strictes.

La première déclaration, signée en 2023 (cf. RA 31, ch. 1.7), a ensuite été soumise aux sociétés mères de YouTube, TikTok, Instagram, Threads, Facebook, LinkedIn, Weibo et X (la plateforme anciennement connue sous le nom de Twitter).

Cette démarche a donné lieu à un dialogue entre les autorités de protection des données et plusieurs de ces entreprises de médias sociaux, ainsi qu'avec l'alliance pour l'atténuation des effets de l'extraction non autorisée de données (Mitigating Unauthorized Scraping Alliance), une organisation qui vise à lutter contre l'extraction non autorisée de données. Les autorités de protection des données ont pu ainsi mieux comprendre les défis que doivent relever les organisations pour se protéger contre l'extraction illégale de données,

notamment le degré de sophistication croissant des extracteurs de données, les progrès constants de la technologie d'extraction de données et la difficulté de différencier les extracteurs de données des utilisateurs autorisés.

En général, les entreprises de médias sociaux ont confirmé aux autorités de protection des données la mise en œuvre bon nombre des mesures énumérées dans la déclaration initiale. Parmi les mesures supplémentaires présentées dans la déclaration commune finale, mentionnons l'utilisation d'éléments de conception de la plateforme qui rendent plus difficile l'extraction de données automatisée, des mesures de protection qui tirent parti de l'intelligence artificielle et des solutions à moindre coût que les petites et moyennes entreprises pourraient utiliser pour respecter leurs obligations en matière de protection des données.

Cadre pour la transmission de données vers les États-Unis

L'Union européenne et le Royaume-Uni s'étant accordés en 2023 avec les États-Unis sur un nouveau cadre de protection applicable au transfert de données vers les États-Unis (cf. 31^e RA, ch. 1.7), un cadre similaire – le Data Privacy Framework (Swiss-US DPF) – est entré en vigueur le 15 septembre 2024 entre la Suisse et les États-Unis. De ce fait, les États-Unis ont été rajoutés à la liste – approuvée par le Conseil fédéral – des États garantissant un niveau adéquat de protection des données. À noter que l'adéquation des États-Unis est limitée aux entreprises certifiées en vertu de ce nouveau cadre.

Outre le DPF, le cadre juridique sur lequel repose la décision d'adéquation du Conseil fédéral comprend également l'executive order 14086 (EO 14086 / décret exécutif), introduisant un mécanisme de recours à deux niveaux, des garanties supplémentaires pour les personnes concernées, ainsi que différentes dispositions d'exécution par lesquelles le ministère établit le de la Justice précise les garanties énoncées dans ce décret.

D'une part, ce mécanisme de recours à deux niveaux entend améliorer les possibilités de protection juridique ressortissant de l'arrêt Schrems II. De



l'autre, il permettra d'éliminer les faiblesses de l'ancien bouclier de protection des données Suisse-États-Unis (Swiss-US Privacy Shield). Dans un premier temps, le responsable américain de la protection des libertés civiles (Civil Liberties Protection Officer – CLPO), rattaché au Bureau du directeur du renseignement national (Office of the Director of National Intelligence – ODNI), examine les plaintes individuelles. Dès que l'enquête du CLPO est terminée, la personne concernée peut demander que, dans un deuxième temps, la décision soit réexaminée par le nouveau Tribunal de contrôle de la protection des données (Data Protection Review Court – DPRC).

Recours devant le PFPDT

Pendant toute la procédure, la communication entre les autorités américaines et la personne concernée en Suisse se déroule exclusivement par l'intermédiaire du PFPDT. Durant la phase initiale, cette personne dépose son recours auprès du PFPDT. Avant

de transmettre le recours au CLPO-ODNI, ce dernier vérifie que le dossier est complet. Il lui faut de plus examiner que le recours déposé remplisse les conditions d'un recours qualifié (qualifying complaint) ; pour être considéré comme tel, ce recours doit être déposé par écrit. Le recourant doit prouver son identité et fournir les informations de base permettant de vérifier le recours. Il n'est pas nécessaire que le plaignant apporte la preuve d'une ingérence présumée des autorités américaines, une présomption raisonnable suffit. En outre, le recourant doit indiquer les moyens spécifiques par lesquels ses données ont été transmises aux États-Unis. Lorsque toutes les conditions sont remplies, le PFPDT transmet le recours au CLPO-ODNI.

Lorsque le CLPO a terminé son examen du cas, le plaignant est informé par le PFPDT que l'examen a bien eu lieu et, soit qu'aucune violation n'a été constatée, soit que le CLPO-ODNI a ordonné une mesure corrective appropriée. Cette réponse standard, toujours identique, ne confirme ni n'infirme que le plaignant a été l'objet des activités des services de renseignement américains. Une réponse standard identique est également transmise à la personne concernée par le PFPDT lorsque le recours est porté devant le DPRC. Une

procédure similaire avec des réponses standard est également utilisée en Suisse pour traiter les demandes d'accès en vertu de la loi fédérale sur le renseignement.

Entreprises américaines non certifiées

En cas de transmission de données de la Suisse vers des entreprises américaines non certifiées, des garanties supplémentaires au sens de l'art. 16, al. 2, LPD demeurent nécessaires afin d'assurer une protection adéquate de ces données (par ex. des clauses contractuelles types ou des règles internes contraignantes en matière de protection des données). Il convient toutefois de souligner que les garanties et les voies de recours introduites par l'EO 14086 s'appliquent à toutes les transmissions de données de la Suisse vers les États-Unis et pas seulement à celles qui sont effectuées sur la base de la décision d'adéquation du Conseil fédéral au sens de l'art. 16, al. 1, LPD.

SCHENGEN**Évaluation de la Suisse**

Du 20 au 24 janvier 2025, la Suisse, en qualité de membre associé à Schengen, a accueilli un groupe d'experts européens chargé d'évaluer la mise en œuvre de l'acquis de Schengen dans le domaine de la protection des données.

Une équipe composée d'experts des autorités de contrôle de la protection des données des États membres de Schengen («modèle pair-à-pair»), d'un observateur du Contrôleur européen de la protection des données (CEPD) et d'une représentante de la Commission européenne s'est rendue en Suisse afin d'évaluer la mise en œuvre de l'acquis de Schengen dans le domaine de la protection des données.

Conformément au programme d'évaluation pluriannuel 2023–2029, tous les États membres de Schengen sont évalués sur leur performance globale concernant la mise en œuvre de l'acquis de Schengen dans les domaines de la gestion des frontières extérieures, des frontières intérieures sans contrôle aux frontières, de la politique des visas, du retour, des systèmes informatiques à grande échelle destinés à soutenir l'application de l'acquis de Schengen, ainsi que de la coopération policière, de la coopération judiciaire en matière pénale et de la protection des données. Le programme d'évaluation Schengen de troisième génération a pour objet de fournir un tableau complet de l'application de l'acquis de Schengen et de renforcer ainsi la confiance mutuelle

dans l'espace Schengen. Désormais, cette évaluation n'a plus lieu tous les cinq ans, mais tous les sept ans (cf. 31^e RA, ch. 1.7).

La partie de l'évaluation relative à la protection des données a pour objectif de vérifier que les exigences de l'acquis de Schengen en matière de protection des données sont effectivement mises en œuvre. Le PFPDT a participé activement aux travaux liés à cette évaluation Schengen de la Suisse. Il a reçu les experts européens dans ses locaux le 20 janvier 2025, leur a présenté sa fonction et ses activités et a répondu aux questions encore ouvertes.

Le droit européen prévoit la transmission des versions préliminaires du rapport d'évaluation et des recommandations par la Commission européenne à la Suisse quatre semaines après la clôture de l'évaluation. La Suisse dispose ensuite de deux semaines pour prendre position. Le rapport d'évaluation analyse les aspects qualitatifs, quantitatifs, opérationnels, administratifs et organisationnels et énumère les manquements constatés lors de l'évaluation, les points à améliorer ainsi que les bonnes pratiques.

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

Le groupe de coordination du contrôle du système d'information VIS a été transféré dans le comité de surveillance coordonnée, qui est désormais également responsable des systèmes d'information EES et ETIAS.

Le groupe de coordination du contrôle du système d'information sur les visas (VIS SCG) a été transféré dans le comité de surveillance coordonnée (Coordinated Supervision Committee [CSC]). Le groupe est toujours composé des mêmes autorités de protection des données, dont la Suisse. La présidence et le secrétariat sont passés du Contrôleur européen de la protection des données au Comité européen de la protection des données (CEPD). Le CSC recouvrira à terme le système d'entrée-sortie (Entry Exit System [EES]) et le système européen d'information et d'autorisation concernant les voyages (European Travel Information and Authorisation System [ETIAS]).

Le CEPD évalue actuellement le nombre de demandes d'accès, de rectification ou de suppression concernant les données traitées dans le système d'information Schengen (SIS), que les États membres de Schengen ont fourni pour la première fois. Il détermine le

SCHENGEN	SCHENGEN
<p>nombre de cas dans lesquels l'accès a été accordé, ou dans lesquels les données ont été rectifiées ou supprimées. Le rapport devrait être achevé en 2025.</p> <p>La mise en œuvre opérationnelle d'EES, prévue le 10 novembre 2024, a pris du retard en raison d'un système central insuffisamment stable et robuste au niveau européen. Elle devrait se faire progressivement dans les différents États membres et associés de l'espace Schengen jusqu'au mois d'octobre 2025.</p> <p>De plus, un représentant du PFPDT a participé à l'évaluation de la Hongrie.</p>	<p>Groupe de coordination des autorités suisses de protection des données</p> <p>Le groupe de coordination Schengen des autorités de protection des données de la Confédération et des cantons s'est réuni à deux reprises sous la présidence du PFPDT. L'autorité de protection des données de la Principauté de Liechtenstein en est membre avec un statut d'observateur</p> <p>Le PFPDT a communiqué à ses homologues cantonaux les résultats des travaux des groupes européens de coordination du contrôle des systèmes d'information SIS et VIS ainsi que l'avancement des travaux de mise en œuvre du système d'entrée et de sortie (EES) et du système européen d'information et d'autorisation concernant les voyages (ETIAS). Le groupe de coordination a par ailleurs effectué des visites à l'Office fédéral de la police (fedpol) et à son bureau SIRENE. Il a aussi élaboré des textes types concernant les systèmes SIS et VIS pour les sites web cantonaux et mis à jour le guide des contrôles SIS.</p>
	<p>Activités au niveau national</p> <p>Le contrôle effectué chez fedpol en tant que point d'accès central du système central d'information sur les visas (C-VIS) et le contrôle des fichiers journaux C-VIS au Corps des gardes-frontière sont terminés. Le PFPDT a en outre effectué un contrôle des fichiers journaux SIS à l'Office central des armes de fedpol. Le contrôle mené chez fedpol portait sur les traitements de données à la centrale d'engagement comme point d'accès central du C-VIS. Le PFPDT n'ayant constaté aucun traitement illicite de données personnelles, il a terminé le contrôle sans rendre de décision.</p>

SCHENGEN

Lors du contrôle des fichiers journaux et des traitements de données au Corps des gardes-frontière, le PFPDT a constaté un accès illicite au SIS. Il a exigé de l'Office fédéral de la sécurité des douanes et de la sécurité des frontières (OFDF) qu'il procède à des ajustements dans la gestion des autorisations et à des contrôles internes. Le PFPDT suivra la mise en œuvre de ces mesures.

Le PFPDT a procédé à un contrôle par échantillonnage des fichiers journaux à l'Office central des armes de fedpol afin de vérifier la légitimité des accès effectués par le personnel autorisé. À cette fin, il a demandé au conseiller à la protection des données de fedpol de lui extraire tous les accès effectués entre le 4 et le 8 septembre 2024 pour pouvoir les analyser. Dans son rapport final du 19 décembre 2024, le PFPDT déclare n'avoir constaté aucun accès illicite.

BTLE et EDPB

En qualité de sous-groupe de travail du Comité européen de la protection des données (European Data Protection Board / EDPB), le BTLE (Borders, Travel and Law Enforcement / Frontières, voyages et application de la loi) traite de thèmes relatifs à l'acquis de Schengen. La Suisse participe à ses travaux en tant que pays associé à Schengen.

Au cours de l'année sous revue, le sous-groupe de travail BTLE a achevé les travaux concernant les grandes lignes de l'art. 37 de la directive (UE)

2016/680 Law Enforcement Directive/LED (cf. 31^e RA, ch. 1.7). L'art. 37 LED décrit les conditions légales (garanties) à respecter lorsque des données sont transférées vers un pays tiers (extérieur à l'UE et à l'EEE). En juin 2024, l'EDPB a approuvé et adopté les grandes lignes de l'art. 37 LED.

De plus, le PFPDT a participé aux travaux de mise en œuvre de la directive (UE) 2016/681 relative à l'utilisation des dossiers passagers (PNR) sur la base de larrêt PNR (C-817/19) de la Cour de justice de l'Union européenne (CJUE). Cet arrêt portait sur l'utilisation des dossiers passagers (données PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les

CONSEIL DE L'EUROPE

enquêtes et les poursuites en la matière. Il énonce d'importantes restrictions concernant le traitement des données à caractère personnel afin que l'application de la directive PNR soit conforme à la Convention européenne des droits de l'homme (CEDH). Parmi les restrictions importantes, nous pouvons citer l'application exclusive aux infractions terroristes et aux formes graves de criminalité, ainsi que la stricte limitation à cinq ans de la durée de conservation de toutes les données PNR (cf. égal. à ce sujet ch. 1.6).

Actuellement, les discussions portent aussi sur le guide de l'EDPB concernant l'interaction entre le règlement européen sur l'intelligence artificielle (AI Act) et la législation européenne en matière de protection des données (RGPD, LED).

Entrée en vigueur de la Convention 108+ à bout touchant

[La convention modernisée du Conseil de l'Europe sur la protection des données \(Convention 108+\) devrait entrer en vigueur en 2026. Lors de ses assemblées plénières, le comité consultatif de la convention a adopté le troisième et dernier module des clauses contractuelles types pour le transfert de données à caractère personnel et des lignes directrices sur le traitement des données à caractère personnel dans le cadre de votations et d'élections.](#)

L'entrée en vigueur de la Convention 108+ a encore pris du retard mais devrait intervenir dans le courant de l'année 2026. Comme indiqué dans le dernier rapport d'activités, elle n'entrera en vigueur que lorsque 38 États contractants l'auront ratifiée (cf. 31^e RA, ch. 1.7). La convention étant ouverte aux États non membres du Conseil de l'Europe, elle déploie ses effets au-delà de l'Europe. Fin mars 2025, 33 États l'avaient ratifiée et 13 l'avaient signée sans l'avoir encore ratifiée. La procédure de ratification étant bien avancée dans différents États, une entrée en vigueur pour la fin 2026 paraît vraisemblable. La Convention 108+ prévoit de remplacer le comité consultatif par un comité conventionnel et de mettre en place un mécanisme de suivi.

Le PFPDT a participé aux deux réunions plénières et aux deux réunions du bureau du comité consultatif. Lors de son assemblée plénière de juin 2024, le comité a adopté le troisième et dernier module des clauses contractuelles

types pour le transfert transfrontalier de données à caractère personnel. Ce module 3 s'applique au transfert de données de sous-traitant à sous-traitant (le premier module traite du transfert de données entre deux responsables de traitement, le deuxième du transfert de données du responsable de traitement à un sous-traitant). Les trois modules ont été réunis dans un seul document. Le PFPDT reconnaît ces clauses contractuelles types du Conseil de l'Europe et les a publiées sur son site. Le comité a par ailleurs adopté des directrices pour la protection des personnes physiques lors du traitement de données à caractère personnel aux fins de l'enregistrement et de l'authentification des électeurs.

L'ordre du jour de la réunion plénière de novembre 2024 prévoyait notamment le renouvellement du bureau du comité consultatif. La représentante de l'autorité de protection des données de l'Argentine a été élue présidente, et la représentante du PFPDT a été confirmée dans ses fonctions de première vice-présidente.



S

M

CONFÉRENCE DE PRINTEMPS

Conférence des autorités européennes de protection des données

Les autorités européennes chargées de la protection des données se réunissent chaque année pour la Conférence de printemps et discutent à cette occasion de thèmes relatifs à leur pratique de surveillance. En 2024, cette rencontre s'est tenue à Riga du 14 au 16 mai, sous l'égide de l'autorité lettone de protection des données.

La 32^e Conférence européenne des autorités de protection des données a rassemblé 130 délégués et 3 organisations provenant de 45 pays. Les discussions ont porté sur les pratiques en matière de surveillance et sur la collaboration transfrontalière, thèmes désormais majeurs du fait de l'évolution technologique.

Le Préposé a participé à une table ronde sur les procédures de coopération entre les États de l'EEE et les États non-membres de l'EEE, ainsi que sur les défis que posent les traitements, au-delà de toute frontière, de données personnelles par les géants mondiaux de la tech.

ECHW

Ateliers sur des cas pratiques

Le European Case Handling Workshop (ECHW / Atelier européen de traitement des données) est un sous-groupe de travail de la Conférence de printemps. Cette rencontre annuelle entre experts est axée sur l'examen de cas pratiques de surveillance. Organisée par l'autorité estonienne de protection des données, elle s'est tenue les 5 et 6 décembre 2024 à Tallinn.

Les ateliers organisés ont abordé notamment l'utilisation de caméras vidéo dans l'espace public et au sein de complexes résidentiels, la réalisation d'analyses d'impact relatives à la protection des données ainsi que la définition des données personnelles sur les réseaux sociaux. La représentante du PFPDT a présenté, dans une perspective comparative, une étude de cas traitant de l'utilisation des caméras de reconnaissance faciale dans la sphère publique.

OCDE

Groupe de travail sur la gouvernance des données et la vie privée

L'OCDE favorise la recherche et l'analyse dans le domaine de la gestion de données et encourage un débat international sur le droit de la protection des données qui tienne compte des derniers développements dans ce domaine. Elle entend garantir la sécurité et l'efficacité du trafic transfrontaliers de données afin de renforcer la confiance dans ces échanges. Ses travaux visent à promouvoir un environnement numérique mondial qui permette des flux de données sûrs et sans heurts par-delà les frontières nationales.

L'une des priorités de l'OCDE est de garantir un niveau élevé de protection et de contrôle des données, en particulier lors de transferts transfrontaliers. L'OCDE vise à développer des normes et des directives susceptibles qui répondent aux besoins en matière de sécurité des données tout en soutenant la force d'innovation et la libre circulation de l'information. En fin de compte, elle souhaite contribuer par ses efforts à établir un cadre transparent et digne de confiance qui exploite pleinement le potentiel des technologies numériques tout en protégeant les droits et les libertés des utilisateurs.

Groupe de travail sur la gouvernance des données et la vie privée

Le PFPDT est représenté dans le groupe de travail de l'OCDE sur la gouvernance des données et la vie privée (Data Governance and Privacy Working Party [DGP]), lequel est rattaché au Comité des politiques de l'économie numérique (CPEN) de l'OCDE. Composé de délégués des 38 États 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 fondées sur des faits avérés, ses travaux ayant pour but de maximiser les avantages sociaux et économiques d'une utilisation large et efficace des données tout en maîtrisant les risques et les difficultés qui en résultent pour la protection de la vie privée.

L'une des priorités du DGP concerne l'analyse de l'accès des autorités aux données du secteur privé, lequel doit concilier l'exercice des tâches publiques et la protection des données. Le DGP analyse aussi les interactions complexes entre différents cadres réglementaires du numérique afin d'en dégager des structures de gouvernance cohérentes et solides. Il a par ailleurs examiné le rôle des intermédiaires de données, instances neutres chargées d'assurer la sécurité et l'efficacité des échanges de données. Il accorde une attention particulière à l'intégration de l'IA dans les systèmes numériques et aux technologies d'amélioration de la

protection de la vie privée. Il s'est également penché sur la dynamique des paiements transfrontaliers afin d'en améliorer l'efficacité et la sécurité dans une économie mondialisée. L'objectif est de dresser un aperçu des interactions entre la gouvernance des données, les lois sur la protection des données et les réglementations financières relatives à ces transactions, afin de permettre aux autorités de protection des données de mieux comprendre le mode de fonctionnement et les défis de conformité de ce secteur.

SYMPOSIUM

Privacy Symposium de Venise

L'extraction massive de données, la protection de la sphère privée dans le cadre de l'action humanitaire et la coopération internationale et régionale étaient au cœur des débats lors du Privacy Symposium.

Avec plus de 300 autorités et experts partageant leurs perspectives, le Privacy Symposium offre un lieu d'échange pour les professionnels de la protection des données, les experts, les autorités et les chercheurs.

Le PFPDT est intervenu lors de différents panels portant notamment sur :

- l'extraction des données (« data scraping ») avec d'autres autorités de protection des données cosignataires de la déclaration commune sur l'extraction de données (cf. texte sur l'extraction des données ci-dessus).
- la protection des données dans l'action humanitaire, en présence d'organisations internationales et d'autorités de protection des données (cf. encadré sur le GT AID). À cette occasion, les panelistes ont exploré la relation entre la protection des données et l'action humanitaire, de l'aide à la réponse aux catastrophes au suivi des tendances de déplacement, où les données jouent un rôle crucial dans l'élaboration d'interventions humanitaires efficaces.

AMVP

Protéger la vie privée à l'ère numérique

Le pouvoir de l'information était au cœur des préoccupations de l'Assemblée mondiale pour la protection de la vie privée. Lors de sa réunion annuelle, elle a adopté quatre résolutions sur des questions essentielles.

Sous le thème central « Le pouvoir du i », l'Assemblée mondiale pour la protection de la vie privée (AMVP) s'est concentrée sur huit thématiques importantes : individu, innovation, information, intégrité, indépendance, international, interculturel et indigène.

Au cours de la session ouverte, la question du respect et de l'équilibre entre le pouvoir de l'information et la nécessité pour les citoyens de contrôler leurs données personnelles était au cœur du débat. Les sujets abordés étaient liés à la détermination des préjudices de la vie privée à la protection des données et à la santé mentale, à l'impact de la technologie sur les autorités de régulation ou aux avantages et aux défis des outils de transfert de données. Parallèlement, les participants ont discuté du rôle de la confidentialité des données dans les crises humanitaires, de la réduction

des inégalités en matière de droit à la vie privée – en explorant les différentes dimensions de la confidentialité de la diversité –, du partage des données entre les gouvernements et les tierces parties, etc. Un dialogue constructif visant à renforcer l'efficacité des modèles juridiques actuels et, d'autre part, à promouvoir les moyens de les améliorer en fonction des changements technologiques.

Lors de la session fermée, l'AMVP a adopté quatre résolutions :

- Approuver et encourager l'utilisation de mécanismes de certification de la protection des données ;

- Les principes concernant le traitement des informations personnelles dans le domaine des neurosciences et des neurotechnologies ;
- La libre circulation des données en toute confiance et la réglementation efficace des flux mondiaux de données ;
- Les nouvelles règles et procédures de l'AMVP.

L'Assemblée mondiale pour la vie privée – dont le PFPDT est membre – a été créée en 1979. Elle rassemble les autorités de protection des données de plus de 100 pays et 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. Sa 46^e édition s'est tenue du 29 octobre au 1^{er} novembre 2024 à St-Hélier (Jersey).

Nouvelle présidente et statuts modernisés

Les autorités membres de l'Association francophone des autorités de protection des données personnelles (AFAPDP) ont élu une nouvelle présidente et adopté les nouveaux statuts de l'association. Également au programme : l'accompagnement des autorités malgaches à la mise en place d'une commission dédiée.

Lors de leur assemblée générale, les membres ont élu – à l'unanimité – une nouvelle présidente en la personne de la commissaire de l'Île Maurice, Drudeisha Madhub. Première femme à la tête du réseau, elle est aussi la première représentante de la zone Afrique-Océan indien depuis la création de l'AFAPDP.

AMVP – GT AID

Renforcer la protection de la vie privée dans un contexte d'urgence

GT AID, le groupe de travail de l'AMVP dédié à l'action humanitaire et présidé par le PFPDT, a renforcé son action de sensibilisation pour la protection de la vie privée dans un contexte d'urgence. Il a notamment organisé un panel dédié lors du Symposium de Venise et participé à la 3^e édition du manuel du CICR sur la protection des données personnelles dans l'action humanitaire. Dans le cadre de son activité de promotion de la protection de la vie

privée à l'échelle mondiale, il a participé à plusieurs panels dont celui de l'atelier des organisations internationales sur la protection des données coorganisé par le CEPD et la Banque mondiale. Le groupe a également élaboré une liste des pays africains disposant d'une loi sur la protection des données personnelles et d'une autorité de protection, avec les points de contact au sein des autorités.

RENCONTRES BILATÉRALES

Dans le cadre d'un groupe de travail, le PFPDT a participé à l'élaboration d'une version modernisée des statuts de l'association qui dataient de 2013. Ces derniers ont ensuite été adoptés.

Les membres ont également discuté de l'accompagnement des autorités malgaches sur le volet « protection des données personnelles » du projet de l'Organisation internationale de la Francophonie visant la modernisation de l'écosystème de l'état civil de Madagascar. Il s'agit notamment de contribuer à la mise en place de la Commission malagasy de l'informatique et des libertés (CMIL).

L'AFAPDP rassemble les autorités indépendantes de 26 pays – dont la Suisse – partageant une langue, une tradition juridique et des valeurs communes. Cette 16^e assemblée générale s'est tenue à St-Hélier, Jersey le 28 novembre 2024.

Échanges entre homologues

Durant l'année passée en revue, le PFPDT a reçu deux délégations étrangères à Berne afin de discuter des défis communs et de la coopération bilatérale.

En juin 2024, le Préposé a reçu son homologue autrichien, Matthias Schmidl, nouvellement élu, pour un échange. Ce dernier a porté sur les défis communs

et la coopération bilatérale dans le domaine de la numérisation et de la protection des données ainsi que sur la liberté d'information et le principe de transparence.

En août 2024, le Préposé a reçu son homologue somalien, Mohamed Ali, premier préposé du pays. La loi somalienne sur la protection des données a en effet été adoptée en mars 2023. Lors de leur échange, les deux préposés ont abordé les premières expériences de la nouvelle autorité chargée de la protection des données et les défis généraux en la matière dans un monde numérique.

Principe de la transparence

2.1 Généralités

La loi du 17 décembre 2004 sur la transparence (LTrans ; RS 152.3) 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 améliorant la compréhension de l'action administrative et, partant, son acceptation, elle vise à promouvoir 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 2024 montrent que le besoin des médias et de la société en informations spécifiques et quant à la transparence de l'administration (ou de l'activité administrative) est toujours aussi fort et a même généré un nouveau pic de demandes. Au cours de l'année sous revue, le nombre de ces demandes a augmenté de près de 30 % par rapport à l'année précédente. Selon les informations fournies par les autorités, cette

augmentation s'est également répercutée sur leur charge de travail. L'application du principe de la transparence constitue globalement un défi de taille et reste exigeante. Les chiffres ci-après (cf. ch. 2.2) révèlent que la tendance constatée ces dernières années, à savoir un pourcentage constamment élevé de cas dans lesquels l'accès est entièrement accordé, s'est confirmée au cours de 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 LTrans leur offre la possibilité de déposer une demande en médiation auprès du Préposé. En 2024, le nombre de procédures de médiation engagées a atteint un niveau inédit depuis l'entrée

en vigueur de la LTrans : Le PFPDT a enregistré 202 demandes, soit une augmentation de 53 % par rapport à l'année précédente. Le but de la procédure de médiation est de parvenir rapidement à un accord entre les parties concernées. La tenue de procédures de médiation orales sur place a également fait ses preuves en 2024 : 76 % des séances ont abouti à une solution amiable.

Le nombre des demandes en médiation, élevé depuis plusieurs années, et la complexité croissante des questions juridiques à résoudre ont entraîné un retard dans le traitement des cas. En conséquence, le Préposé a dépassé le délai légal de 30 jours dans 72 % des procédures. Cette évolution négative devrait s'accentuer, avec pour conséquence de retarder davantage encore le traitement des cas, que le législateur a pourtant voulu rapide (cf. ch. 2.3 pour plus de détails).

Au début de l'année 2025, un demandeur, en l'occurrence un homme politique local, a manqué une nouvelle fois de se présenter à la médiation, sans

fournir d'excuse. Le Préposé déplore ce genre de négligence qui a entraîné une perte de temps et du travail inutile à ses juristes et à l'autorité compétente. En cas d'absence non justifiée du demandeur, la loi prévoit le classement de la procédure de médiation.

Dans une autre affaire, une autorité n'a pas respecté l'accord écrit contracté avec le demandeur lors de la procédure de médiation. Lorsqu'une autorité ne respecte pas ses obligations contractuelles, le demandeur peut agir par la voie de l'action devant le Tribunal administratif fédéral pour accéder aux documents officiels selon les modalités convenues.

En 2024 toujours, l'administration a tenté de faire exclure du principe de la transparence des domaines de son activité ou certaines catégories de documents. Un aperçu des dispositions spéciales réservées en vertu de l'art. 4 LTrans figure au ch. 2.5.

Le Préposé tient à souligner l'exception faite par le Conseil fédéral au champ d'application de la loi sur la transparence pour le Service suisse d'enquête de sécurité (SESE), en vertu de l'art. 2, al. 3, LTrans (cf. ch. 2.4). Du point de vue du PFPDT, le problème central réside dans le fait que l'administration s'exclut elle-même du principe de la transparence et anticipe de facto une décision du législateur en attente (dans le cadre de la révision partielle de la loi sur l'aviation). Le Préposé conteste en outre la nécessité de cette restriction inconditionnelle de la LTrans, considérant que toute exception de ce type affaiblit le principe de la transparence et par ainsi, la promotion de la transparence dans l'administration.

Il constate toutefois que le changement de paradigme opéré par la loi sur la transparence, passant du principe du secret à celui de la transparence, a été mis en œuvre par la plupart des autorités fédérales et continue d'être activement appliqué.

2.2 Demandes d'accès – hausse considérable en 2024

Selon les chiffres communiqués par les autorités fédérales, 2186 demandes d'accès ont été déposées au cours de l'année sous revue (contre 1701 en 2023), ce qui correspond à une augmentation de 29 % par rapport à 2023. À cela s'ajoutent 46 demandes déposées antérieurement mais traitées en 2024. Les autorités ont accordé un accès intégral aux documents dans 1159 cas (52 %), contre 830 (48 %) en 2023, et un accès limité ou différé dans 474 cas (21 %), contre 402 (23 %) en 2023. Dans 179 cas (8 %), l'accès a été totalement refusé, contre 176 (10 %) en 2023. Selon les indications des autorités, 133 demandes d'accès (6 %) ont été retirées, contre 73 (4 %) l'année précédente, 102 demandes étaient pendantes à la fin 2024, et dans 185 cas, aucun document officiel n'était disponible.

Le Préposé constate qu'au cours de l'année sous revue, l'accès intégral aux documents a été accordé dans plus de la moitié des cas. À l'exception de l'année dernière, cette tendance observée depuis plusieurs années semble donc se confirmer en 2024. Les refus d'accès complets se sont stabilisés au fil des ans à un faible niveau (environ 10 %).

Départements et offices fédéraux

En 2024, certaines unités administratives ont fait l'objet d'une attention particulière de la part des médias et de la société. Du fait de leur domaine d'activité, le DDPS (527), le DETEC (324) et le DFAE (306), notamment, ont été confrontés à un grand nombre de demandes d'accès. 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 fastidieuse entre offices ou entre départements.

Au niveau des offices, les chiffres communiqués montrent que l'OFSPPO a enregistré le plus grand nombre de demandes d'accès (317) en 2024. Viennent ensuite le domaine des EPF (143), l'OFEV (139) et la ChF (94). Sept autorités ont déclaré n'avoir reçu aucune demande d'accès au cours de l'année sous revue. Le PFPDT lui-même en a reçu 29, auxquelles il a accordé un accès

complet dans 18 cas. Dans un cas, l'accès a été entièrement refusé et dans quatre cas, le Préposé a accordé un accès partiel. Six demandes étaient encore pendantes fin 2024.

Le montant total des émoluments perçus en 2024 pour l'accès aux documents officiels s'élève à 9950 francs, soit nettement moins (30 %) que l'année précédente (14 226,20 francs). Alors que la ChF, le DFAE, le DFJP, le DDPS, les services du Parlement et le MPC n'ont pas perçu d'émoluments, les quatre autres départements ont facturé aux demandeurs une partie du temps consacré au traitement (DFI: 4250 francs ; DDPS: 3600 francs ; DFF: 2000 francs ; DETEC: 100 francs). Signalons que des émoluments n'ont été perçus que pour 7 des 2232 demandes traitées, contre 19 l'année précédente, ce qui représente une nette diminution tant du nombre de cas concernés que du montant total des émoluments. La perception d'émoluments reste exceptionnelle (0,3 % des cas). La pratique de l'administration selon laquelle les documents officiels peuvent en principe être consultés gratuitement est inscrite dans la LTrans depuis le 1^{er} novembre 2023. La perception d'émoluments est possible à titre

exceptionnel lorsqu'une demande d'accès nécessite un traitement particulièrement complexe.

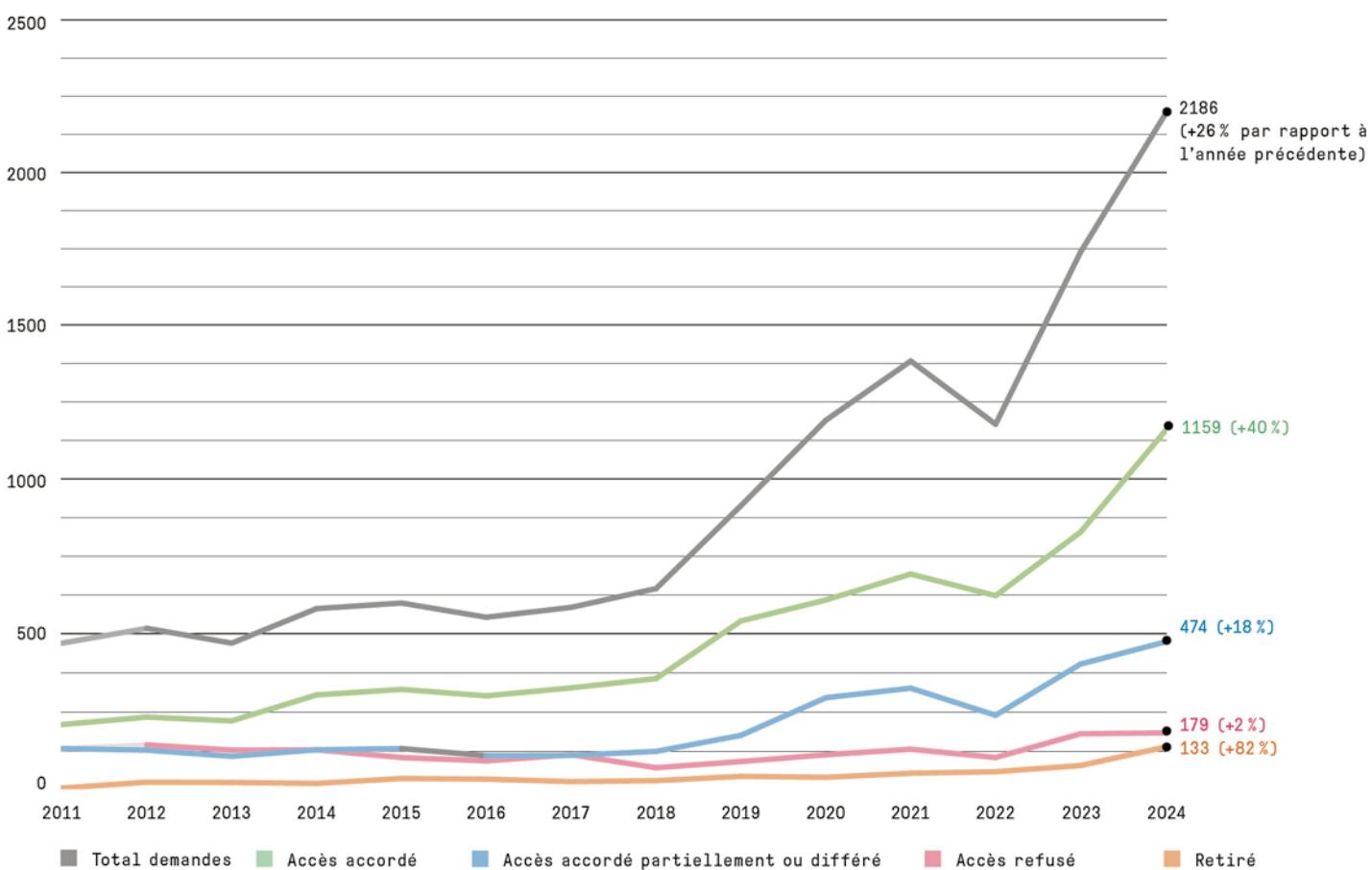
En ce qui concerne le temps consacré au traitement des demandes, le Préposé rappelle que les autorités ne sont pas tenues de le consigner et qu'il n'existe pas de directive de saisie uniforme pour l'ensemble de l'administration fédérale. Les informations qui lui sont transmises sur une base volontaire ne reflètent que partiellement

les heures de travail réellement effectuées. Selon ces données, le temps consacré au traitement a de nouveau nettement augmenté sur un an, passant de 6 469 à 7 256 heures.

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

traitement ne correspond que partiellement au temps réellement investi. En plus des 4 82 heures indiquées ponctuellement par ses unités spécialisées compétentes, l'OFSP a signalé pour le traitement des demandes d'accès (y c. les procédures de médiation et de recours) et l'assistance juridique fournie par sa conseillère à la transparence une charge de travail importante estimée à au moins 3,6 équivalents temps plein. Il devrait en être de même pour d'autres autorités.

Graphique 1 : Demandes d'accès – évolution depuis 2011





4b
Arbeitsfläche

3
Institutsarbeiten

Le temps consacré à la préparation des procédures de médiation a lui aussi considérablement augmenté: 1271 heures contre 730 l'année précédente (en 2022: 1006h; en 2021: 865h; en 2020: 569h).

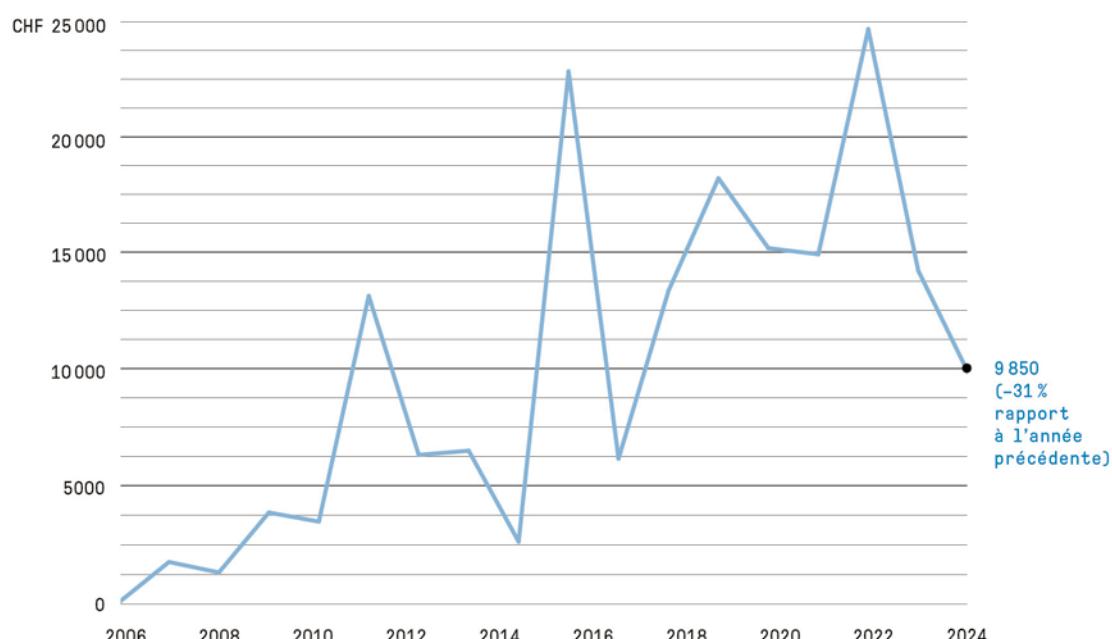
Services du Parlement

Les Services du Parlement ont déclaré avoir reçu cinq demandes d'accès au cours de l'année sous revue. Dans un cas, l'accès a été entièrement accordé, dans un autre il l'a été partiellement, dans deux cas il a été entièrement refusé, et dans un cas il n'existe aucun document officiel.

Ministère public de la Confédération

Le MPC a déclaré avoir reçu en 2024 huit demandes. L'accès a été accordé entièrement dans 3 cas et refusé entièrement dans 2 autres. Trois cas étaient pendants fin 2024.

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



2.3 Procédures de médiation – nette augmentation des demandes

En 2024, 202 demandes en médiation ont été déposées auprès du PFPDT, un nombre jamais atteint jusque-là depuis l'entrée en vigueur de la LTrans. Cela représente une augmentation de 53 % par rapport aux 132 demandes reçues en 2023. La plupart des demandes émanaient de particuliers (66) et de journalistes (61). Ces chiffres permettent de tirer les conclusions suivantes : Sur les 838 cas dans lesquels l'administration fédérale a refusé entièrement ou partiellement l'accès, l'a différé ou a estimé que la demande ne correspondait à aucun document officiel, 202 (soit 24 %) ont donné lieu au dépôt d'une demande en médiation.

En 2024, le PFPDT a traité 157 demandes, du jamais vu. Parmi celles-ci 130 avaient été déposées dans l'année et 27 l'année précédente. Dans 92 cas, un accord a pu être trouvé entre les parties. En outre, le PFPDT a émis 31 recommandations, qui ont permis de régler 32 cas dans lesquels aucun accord ne se profilait.

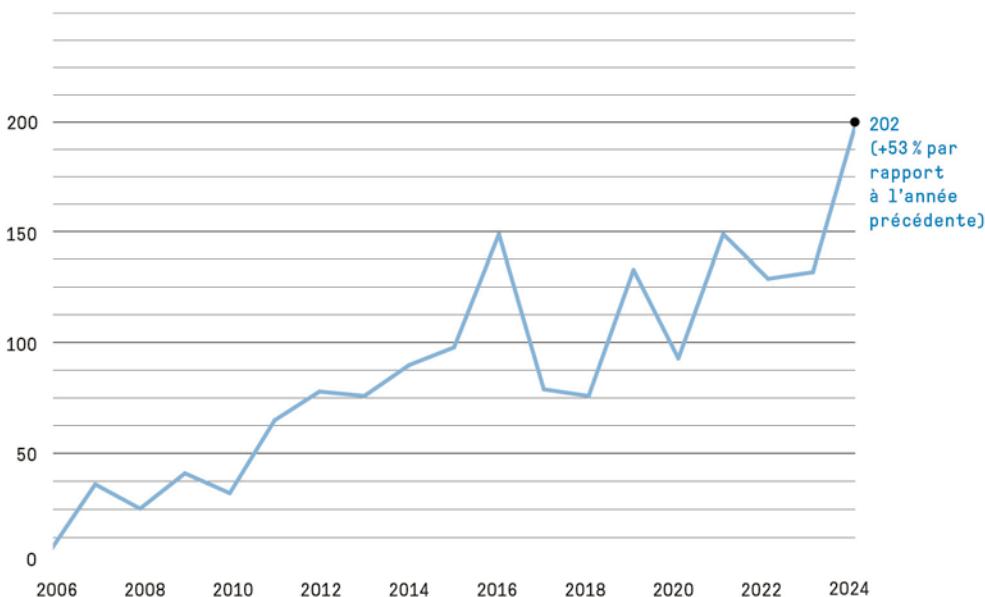
Parmi les cas réglés, on compte également 15 demandes remises hors délai, 10 cas dans lesquels les conditions d'application de la LTrans n'étaient pas réunies, ainsi que 8 qui ont été retirées. Enfin, 10 procédures de médiation ont été suspendues en accord avec les parties ou à la requête des demandeurs.

Proportion des solutions amiables

Les solutions à l'amiabiles 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.

L'efficacité des séances de médiation orales apparaît surtout dans le rapport entre les solutions amiables et les recommandations. Au cours de l'année sous revue, 92 solutions amiables ont été trouvées, et le Préposé a émis 31 recommandations afin de régler 32 cas. Par rapport aux recommandations, les solutions amiables représentent donc

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



74 % des procédures. Pendant l'année sous revue, sur les 82 procédures menées, 62 (76 %) ont abouti à un accord.

Ces chiffres établissent clairement que la pratique de médiation orale du PFPDT est adaptée à la recherche de solutions amiables. Il faut donc la maintenir, d'autant qu'elle profite à toutes les parties.

Remarque : toutes les recommandations émises au cours de l'année sous revue sont consultables sur le site du Préposé (www.edoeb.admin.ch).

Tableau 1 : Solutions amiables

2024	74 %
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 32 représente trois durées de traitement, étant entendu que la durée pendant laquelle une procédure est suspendue à la demande des parties ou en accord avec elles n'est pas prise en compte. Il peut y avoir suspension, notamment, lorsqu'une autorité souhaite revoir sa position à l'issue d'une séance de médiation, ou lorsqu'elle doit procéder à l'audition de tiers concernés. Si la séance est reportée à la demande d'une partie (p. ex. pour cause de congés ou de maladie), la prolongation de la procédure qui en découle n'est pas non plus prise en compte dans la durée du traitement

Le tableau montre que 28 % des procédures réglées en 2024 l'ont été dans le délai réglementaire de 30 jours, 45 % dans un délai compris entre 31 et 99 jours, et 27 % en 100 jours ou plus.

Sur les 44 cas traités en 30 jours, 16 seulement (36 %) ont donné lieu à un examen matériel de l'objet de la médiation. Dans les 28 autres cas (64 %), il n'y a pas eu d'appréciation matérielle quant au fond, soit parce qu'il était évident que la LTrans ne s'appliquait pas, soit parce que les conditions formelles d'ouverture d'une procédure de médiation n'étaient pas remplies.

Les retards de traitement hérités des années précédentes et le grand nombre de nouveaux dossiers en 2024 ont entraîné un nouvel allongement de la durée des procédures. À cela s'ajoute le fait que le nombre des demandes entrantes est fluctuant. À titre d'exemple, le Préposé en a reçu beaucoup en juin (30) et en octobre (26), contre seulement 8 en août et 9 en décembre.

Avant la pandémie, le délai légal de 30 jours était régulièrement respecté lorsque la séance de médiation se terminait par un accord. Cela n'a pas été le cas pendant l'année sous revue, mais 20 % des procédures aboutissant à un

accord ont duré moins de 30 jours (contre 35 % l'année précédente). Dans 95 % des cas, la séance de médiation a dû être programmée de telle sorte que le délai soit déjà expiré au moment de la séance, en raison des ressources en personnel disponibles et du retard accumulé dans le traitement des dossiers. Lorsque le Préposé était contraint, faute de solution amiable, de formuler une recommandation écrite, il n'a pu respecter le délai légal de 30 jours suivant la réception de la demande dans aucun cas.

D'autres raisons expliquent par ailleurs le dépassement des délais : demandes d'accès particulièrement volumineuses, nombre important de tiers impliqués dans la procédure ou complexité juridique des questions. Le traitement de ces cas nécessitant souvent un surcroît important de travail, le Préposé peut, conformément à l'art. 12a de l'ordonnance sur le principe de la transparence

dans l'administration (OTrans; RS 152.31), prolonger le délai réglementaire de manière appropriée.

Tandis que le dépassement du court délai de 30 jours est considéré comme inhérent au système dans les cas complexes ou les procédures multipartites (impliquant plusieurs tiers) en raison de la possibilité de prolongation offerte par la loi, les nouveaux dépassements qui tiennent uniquement à la forte augmentation des demandes consistent, juridiquement, en des retards injustifiés.

Tableau 2: Durée 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	Période 2024
30 jours maximum	11%	59%	50%	57%	43%	42%	25%	27%	28%
de 31 à 99 jours	45%	37%	50%	38%	30%	51%	42%	35%	45%
100 jours ou plus	44%	4%	0%	5%	27%	7%	33%	38%	27%

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

Nombre de cas pendants

Les chiffres ci-dessous indiquent le nombre de cas pendants à la fin de chaque année. Début janvier 2025, 66 procédures de médiation étaient pendantes, dont 10 suspendues (2 datant respectivement de 2019 et 2021, 2 de 2022 et 6 de l'année sous revue). Le Préposé en a terminé 19 avant la mise sous presse du présent rapport.

Tableau 3: Procédures de médiation pendantes

Fin 2024	66 (dont 19 terminées à la mise sous presse et 10 suspendues)
Fin 2023	31 (dont 17 terminées à la mise sous presse et 9 suspendues)
Fin 2022	42 (dont 11 terminées à la mise sous presse et 13 suspendues)
Fin 2021	27 (dont 8 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

RAPPORT DE LA CDG-E

Le Conseil fédéral renonce à examiner la possibilité d'octroyer un droit d'intervention ou de décision du PFPDT

Dans son rapport sur les courriels introuvables au Secrétariat général du Département fédéral de l'intérieur (SG-DFI), la Commission de gestion du Conseil des États (CdG-E) a constaté que les prescriptions en matière de classement et d'archivage n'étaient pas uniformes dans l'administration fédérale et nécessitaient une clarification. Concluant de son enquête qu'il fallait renforcer le droit du Préposé de consulter les documents officiels, elle a formulé cinq recommandations. Le Conseil fédéral a rendu compte de son évaluation de ces recommandations dans un rapport. Dans son rapport du 10 octobre 2023 intitulé « 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 les bases légales de la conservation, du classement et de

l'archivage des documents (loi sur l'archivage [LAr]) et de l'accès aux documents officiels (loi sur la transparence [LTrans]). Le PFPDT s'est exprimé en détail à ce sujet dans ses derniers rapports d'activités (cf. 31^e RA, ch. 2.4 et 30^e RA, ch. 2.4). Le rapport de la CdG-E renferme cinq recommandations au Conseil fédéral, dont trois présentent un lien direct avec la LTrans :

- dans la recommandation 1, la CdG-E invite le Conseil fédéral à examiner si 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, la CdG-E invite le Conseil fédéral à examiner si la LTrans s'applique ou devrait s'appliquer aussi aux procédures pénales 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, la CdG-E invite le Conseil fédéral à examiner l'opportunité d'une modification de la LTrans conférant au PFPDT un droit d'intervention ou de décision lorsque son droit de consulter les documents n'est pas respecté.

Dans son premier avis, du 11 janvier 2024, le Conseil fédéral s'est déclaré d'accord avec les recommandations 1 à 4. À propos de la recommandation 5, il a refusé d'octroyer au Préposé un droit d'intervention ou de décision mais s'est dit prêt à examiner les possibilités d'intervention qu'a le PFPDT lorsque la consultation de documents ne lui est pas accordée.

Le Conseil fédéral a alors chargé le Département fédéral de justice et police (DFJP) d'examiner les différentes recommandations pour la fin 2024 et de lui soumettre, dans un rapport, des propositions quant à la suite à leur donner. Le Préposé a eu l'occasion de se prononcer sur le projet de rapport concernant les différentes recommandations et les explications du Conseil fédéral dans le cadre d'une consultation préalable et d'une consultation des offices organisée par le DFJP.

À propos de la recommandation 1, le Conseil fédéral estime que dans le cas des documents qui ont trait non seulement à une personne dans l'exer-

cice de ses fonctions, mais aussi à sa sphère privée, il faut examiner au cas par cas s'il existe un droit d'accès en vertu de la LTrans ou un droit de consultation en vertu de la LAr. Il n'identifie aucune nécessité de modifier la loi et estime que la recommandation 1 de la CdG-E ne porte que sur un aspect spécifique de la coordination entre la LTrans et la LAr. Lors des consultations, le Préposé a quant à lui défendu le point de vue selon lequel une révision (partielle) est indispensable pour régler la coordination entre la LTrans et la LAr avec la sécurité juridique nécessaire, étant donné les différences qui opposent les deux lois sur le plan matériel et sur celui de la procédure, différences que le Conseil fédéral reconnaît du reste clairement dans son rapport.

- S'agissant de la recommandation 4 et du champ d'application de la LTrans, le Préposé constate que ses remarques concernant la jurisprudence du Tribunal fédéral, qui a déjà statué sur la façon dont l'art. 3, al. 1, let. a, LTrans doit être appliqué, n'ont pas été prises en compte. Selon une compréhen-

sion restrictive du motif d'exclusion des documents concernant les procédures visées à l'art. 3, al. 1, let. a, LTrans, le Tribunal fédéral a conclu que seuls les actes de procédure au sens strict étaient exclus du champ d'application de la LTrans, et ce « que la procédure soit pendante ou close ». Le Préposé considère par conséquent que le Tribunal fédéral a réglé définitivement la question de l'accès aux actes de procédure.

- À propos de la recommandation 5, le Conseil fédéral s'en est tenu à son avis du 11 janvier 2024, refusant d'examiner la possibilité d'octroyer un droit de décision au PFPDT au motif que la médiation au sens de la LTrans est une procédure informelle, dans laquelle le PFPDT n'a aucune compétence décisionnelle, qui ne crée pas de précédent et ne donne lieu à aucun procès-verbal. Lors de la consultation des offices, le Préposé a fait remarquer que cette décision ne répondait qu'en partie au souhait de la CdG-E d'examiner l'opportunité d'octroyer au Préposé non seulement un droit d'intervention mais aussi un droit de décision. Sa proposition de procéder à un tel examen ultérieurement n'a pas été retenue.

Le rapport du Conseil fédéral à la CdG-E du 13 décembre 2024 a été approuvé et publié sous la forme proposée par le DFJP.

Limitation du principe de la transparence pour les lanceurs d'alerte

La révision de la loi sur le personnel de la Confédération (LPers) en cours d'examen au Parlement prévoit d'importantes limitations du principe de la transparence, notamment en ce qui concerne le traitement des signalements effectués par des lanceurs d'alerte. Le Préposé a fait part de son opposition à ces restrictions à plusieurs reprises. Le 28 août 2024, le Conseil fédéral a transmis au Parlement le message concernant la modification de la LPers, qui prévoit non seulement de modifier le régime de la prévoyance professionnelle mais aussi de renforcer la protection des données en relation avec le profilage et de faire avancer la numérisation dans le domaine des ressources

humaines (cf. ch. 1.5). Des modifications isolées visent en outre à accroître l'efficacité du droit du personnel.

Parmi les mesures visant une efficacité accrue, le Conseil fédéral propose à l'art. 22a, al. 7, du projet (P-LPers) d'exclure du champ d'application de la LTrans les pièces documentant un signalement au sens de l'art. 22a P-LPers (signalement, dénonciation et protection des lanceurs d'alerte), jointes à un signalement ou établies sur la base d'un signalement. L'Office fédéral du personnel (OFPER), responsable du projet, justifie cette restriction par la nécessité de préserver à long terme la confiance en l'instrument que constitue le lancement d'alertes et de protéger les personnes auxquelles les signalements reprochent un comportement illicite.

Le Préposé a démontré en vain, lors de deux consultations des offices et d'une consultation intermédiaire, que les intérêts privés légitimes resteraient protégés même si la LTrans s'appliquait. Il a expliqué que l'instrument du lancement d'alertes bénéficiait d'ores et déjà d'une grande confiance, l'art. 22a LPers qui le règle étant en vigueur depuis le 1^{er} janvier 2011. Les employés de la Confédération ont bien intégré l'obligation de dénoncer les infractions poursuivies d'office et le droit de signaler d'autres irrégularités qui figurent dans cette disposition. Le nombre de cas

signalés est d'ailleurs en augmentation constante, comme le montrent les évaluations statistiques du Contrôle fédéral des finances. Le Préposé ne voit pas en quoi le maintien de la réglementation actuelle (sans réserve au sens de l'art. 4 LTrans) pourrait entraîner une perte de confiance. Il considère par ailleurs que la LTrans offre suffisamment de moyens de garantir la protection des informations sensibles et des données personnelles tant des lanceurs d'alerte que des personnes concernées par les faits dénoncés (cf. art. 7 et 9 LTrans). Il ne voit donc pas la nécessité de soustraire au regard du public tous les signalements, annexes comprises, établis sur la base d'une telle dénonciation, y compris les documents et rapports finaux établis dans la foulée. Cela n'est pas non plus conforme au principe de la proportionnalité visé à l'art. 5 Cst. Le Préposé estime que compte tenu de l'intérêt public légitime à voir traiter sérieusement les manquements

AVIATION

signalés d'employés de l'administration, rien ne justifie la dérogation prévue au principe de la transparence.

Enfin, le PFPDT fait remarquer, que les plateformes de signalement n'ont pas à être reléguées dans un domaine secret de l'État, ne serait-ce que parce qu'elles sont chargées, en vertu de la loi, d'examiner les unités administratives et les employés concernés par un signalement, ce qui leur donne une position particulière aux yeux du public.

Le message transmis par le Conseil fédéral et en cours d'examen au Parlement contient toujours la limitation du champ d'application de la LTrans et rend fidèlement compte de la position divergente du Préposé.

Limitation du principe de la transparence quant à la surveillance de l'aviation civile

La surveillance de l'aviation civile doit être largement exclue du principe de la transparence. Le Préposé a manifesté son opposition à ce projet lors de la consultation des offices puis dans le cadre de la procédure de consultation. Le projet mis en consultation de la loi sur l'aviation (P-LA) élaboré par l'Office fédéral de l'aviation civile (OFAC) prévoit de larges dérogations au principe de la transparence, notamment en ce qui concerne la surveillance légale de l'OFAC. L'art. 107d, al. 2, P-LA dispose que la LTrans ne s'appliquera pas « à l'accès aux données personnelles et aux données concernant des personnes morales, contenues dans les documents officiels énumérés ci-après ni lorsque l'octroi de l'accès auxdits documents compromet la sécurité ou la sûreté » : rapports portant sur des audits, des inspections, des expertises et des contrôles de l'OFAC (let. a) ; comptes rendus et documents associés concernant des événements, adressés à l'OFAC en vertu du règlement (UE) no 376/2014¹¹ (let. b), et documents officiels relatifs aux enquêtes de sécurité du Service suisse d'enquête de sécurité (let. c).

Le Préposé, qui est assujetti à la LTrans en sa qualité d'autorité de surveillance, s'est opposé aux dispositions

prévues, estimant que la LTrans offre suffisamment de possibilités de garantir la protection d'informations sensibles, y compris dans le domaine des activités de surveillance et en relation avec les enquêtes de sécurité (cf. art. 7 et 9 LTrans). Il a d'ailleurs rappelé que c'est à dessein que le législateur n'a pas placé la confidentialité entre l'autorité de surveillance et les assujettis parmi les exceptions à la LTrans.

Pour justifier la dérogation proposée, l'OFAC explique que les assujettis ne respecteront leur « obligation légale de compte rendu » que s'ils ont la certitude que les informations en question ne seront pas rendues publiques. Cette prémissé, inexacte selon le Préposé, ne tient pas compte du fait que, dans un État de droit, les obligations légales de renseigner et de signaler sont censées être respectées. De plus, on ne peut pas restreindre le champ d'application de la LTrans sous prétexte que certains

AVIATION

assujettis pourraient commettre des infractions. Le Préposé juge par ailleurs indéfendable et présomptueux l'argument de l'OFAC selon lequel les rapports contiennent souvent des détails techniques dont le profane peine généralement à comprendre la signification. En conclusion, le Préposé n'identifie aucun motif valable pour soustraire intégralement au principe de la transparence dans l'administration et donc pour garder secrets, de façon inconditionnelle, des aspects essentiels de l'activité de surveillance.

Le Préposé fait d'ailleurs remarquer que le public est particulièrement attentif aux autorités assumant des tâches de surveillance, d'audit, de contrôle ou d'inspection puisque la loi les charge d'examiner d'autres unités administratives et / ou des particuliers. Il dénonce résolument toute tentative d'une autorité de surveillance de se soustraire au champ d'application de la LTrans avec des arguments du type « risque de manquement à l'obligation de signaler » ou « trop complexe pour la population », surtout dans des domaines aussi sensibles que celui de l'aviation.

Le Préposé s'était déjà résolument opposé à une telle restriction lorsqu'elle avait été proposée dans le cadre de la révision partielle 1+ de la LA en 2014-2015 (cf. 22^e RA, ch. 2.2.2). Cette proposition

n'avait finalement pas été retenue, mais l'OFAC omet d'expliquer en quoi l'évolution de la situation depuis lors la rendrait nécessaire aujourd'hui.

L'OFAC ayant refusé, à l'issue de la consultation des offices, d'exposer la position du Préposé dans le rapport explicatif relatif au projet de révision, le Préposé s'est vu forcé, par mesure de transparence, de prendre une nouvelle fois position lors de la consultation.

Modification de l'ordonnance sur les enquêtes de sécurité en cas d'incident dans le domaine des transports (OEIT)

Le Conseil fédéral a exclu le Service suisse d'enquête de sécurité (SESE) du champ d'application de la LTrans par la modification qui est entrée en vigueur le 1^{er} janvier 2025. Lors de la consultation des offices, le Préposé s'est élevé en vain contre cette limitation du principe de la transparence.

En vertu de l'art. 2, al. 3, let. a, LTrans, le Conseil fédéral peut exclure des unités de l'administration fédérale au champ d'application de la loi à raison de la personne si l'accomplissement des tâches qui leur ont été confiées l'exige. En se référant à cette possibilité, il établit, dans le nouvel art. 54a OEIT, que le SESE est exclu du champ d'application de la LTrans dans la mesure où traite des données de personnes physiques et morales.

Le Département de l'environnement, des transports, de l'énergie et de la communication (DETEC), responsable de la modification de l'ordonnance, a justifié cette exclusion en arguant que le SESE n'obtient les informations nécessaires au maintien de la sécurité des transports que si les informateurs ont l'assurance que leurs renseignements

SURVEILLANCE FINANCIÈRE

ne seront pas rendus publics. L'administration fédérale invoque régulièrement cet argument afin de justifier la nécessité (apparente) d'une exclusion du champ d'application de la LTrans. Or comme le Préposé l'a expliqué à maintes reprises, cet argument ne convainc pas (cf. texte ci-dessus sur la révision de la LA, 31^e RA, ch. 2.4 et 22^e RA, ch. 2.2.2). En outre, le DETEC n'a pas expliqué en quoi les exceptions prévues par la LTrans ne suffisent pas à garantir l'exécution des tâches du SESE.

Avec la modification de l'OEIT décidée par le Conseil fédéral, l'administration s'exclut elle-même du principe de la transparence auquel elle est censée se conformer. C'est d'autant plus surprenant que l'OFAC, ou plus exactement le DETEC, propose déjà dans le cadre de la révision partielle de

la LA (cf. ci-dessus), donc au niveau de la loi, l'instauration d'une disposition spéciale afin d'exclure le SESE du champ d'application de la LTrans. Le Conseil fédéral anticipe donc le processus de décision parlementaire.

Alors que l'exclusion du SESE visée à l'art. 54a OEIT est entrée en vigueur le 1^{er} janvier 2025, le DETEC explique à propos de cette disposition qu'elle doit être provisoire au motif qu'une restriction du champ d'application du principe de la transparence devrait en principe être réservée au pouvoir législatif.

Nouvelle loi fédérale sur la transparence des personnes morales

La loi sur la transparence des personnes morales vise à créer un registre central permettant d'identifier les ayants droit économiques effectifs des personnes morales. Malgré l'intervention du PFPDT, le projet de loi prévoit une exclusion du champ d'application de la LTrans. Le 22 mai 2024, le Conseil fédéral a transmis au Parlement le message concernant la loi fédérale sur la transparence des personnes morales et l'identification des ayants droit économiques (LTPM). Ce projet prévoit la création d'un registre regroupant des informations à jour sur les ayants droit économiques des entités juridiques enregistrées, dans le but de renforcer

DROIT DE NÉCESSITÉ

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

Le Préposé déplore que le Conseil fédéral ait inséré dans le projet de loi, à l'issue de la procédure de consultation (cf. 31^e RA, ch. 2.4), une exclusion expresse du champ d'application de la LTrans : ainsi, selon l'art. 53, al. 4 du projet de loi, la LTrans ne s'appliquera pas aux données du registre de transparence concernant des personnes physiques ou morales.

Le Secrétariat d'État aux questions financières internationales (SFI), l'autorité compétente, justifie la restriction par le fait que l'objectif principal du registre est d'améliorer la lutte contre le blanchiment d'argent et le financement du terrorisme. Selon le SFI, un accès plus large au registre n'apporterait aucune valeur ajoutée et porterait une atteinte disproportionnée aux droits de la protection de la personnalité.

Le Préposé a démontré en vain, lors de la consultation des offices, que les intérêts privés légitimes resteraient protégés même si la LTrans s'appliquait. Celle-ci protège en effet expressément les secrets d'affaires (art. 7, al. 1, let. g, LTrans), la sphère privée et les données personnelles des personnes physiques et des personnes morales (art. 7 al. 2 LTrans, art. 9 al. 2 LTrans en lien avec art. 36 LPD et art. 57s LOGA). Le PFPDT a fait remarquer que les banques de données ou les registres utilisés par les autorités pour l'accomplissement de tâches publiques sont en principe couverts par le droit d'accès selon la LTrans. Il estime par conséquent que prévoir, sans justification, une réglementation différente pour le registre de transparence est contraire au principe de la transparence.

Le projet transmis par le Conseil fédéral et en cours d'examen au Parlement contient toujours la limitation du champ d'application de la LTrans. Précisons que le message du Conseil fédéral rend fidèlement compte de la position du Préposé.

Application du droit de nécessité : rapport du Conseil fédéral

Dans son rapport du 19 juin 2024, le Conseil fédéral déclare que le principe de la transparence revêt une importance capitale, surtout en temps de crise, et que son application ne peut être exclue que dans des cas exceptionnels. Le rapport rend compte de la position du PFPDT.

Au cours des vingt dernières années, le Conseil fédéral a fait usage à plusieurs reprises de son droit d'édicter, en s'appuyant sur la Constitution, des ordonnances de nécessité face à un risque de crise (cf. art. 184, al. 3, et 185, al. 3, Cst.). Il y a notamment recouru en relation avec le mécanisme de sauvetage destiné au secteur de l'électricité et avec le rachat de Credit Suisse par UBS, afin

d'exclure du principe de la transparence dans l'administration les activités transférées à celle-ci. Le Parlement a chargé le Conseil fédéral de présenter dans un rapport les bases légales qui fondent le droit de nécessité ainsi que ses limites, et de faire le point sur les adaptations nécessaires.

Dans son rapport du 19 juin 2024, le Conseil fédéral déclare que l'application du droit de consulter des documents officiels inscrit dans la LTrans ne peut être exclue par le droit de nécessité que dans des cas exceptionnels. Il estime qu'il s'agit là d'un instrument de contrôle de l'administration par les citoyens que le législateur a instauré, et qui est d'autant plus important en temps de crise. Toute restriction de ce droit doit par conséquent être dûment justifiée.

Lors de la consultation des offices, le Préposé a donné son avis sur le projet de rapport rédigé par l'Office fédéral de la justice. Il souhaitait avant tout la suppression de deux passages relatifs

à une appréciation juridique sur des questions de droit non encore réglées. Dans son avis, il a en outre réitéré ses critiques quant à la justification avancée dans le rapport selon laquelle l'exclusion du principe de la transparence serait le seul moyen de garantir le respect des obligations de signaler prévues par la loi (cf. Texte sur la révision de la LA et 31^e RA, ch. 2.4 et 22^e RA, ch. 2.2.2). Le Préposé se félicite de ce que les suppressions demandées aient été effectuées et de ce que le message rende compte de sa position.

Dans son communiqué du 6 avril 2023, le Préposé avait déjà fait remarquer que le fait que le recours au droit de nécessité fût nécessaire pour soutenir le secteur de l'électricité ou le secteur financier ne permettait pas de justifier la nécessité d'exclure par la voie du même droit de nécessité l'application de la LTrans. Il a confirmé cette appréciation dans ses recommandations du 27 novembre 2023 concernant l'accès aux documents relatifs au rachat de Credit Suisse par UBS. Il signale par ailleurs que dans son rapport du 17 décembre 2024 sur la gestion par les autorités de la fusion d'urgence de Credit Suisse, la Commission d'enquête parlementaire émet des doutes sur la proportionnalité d'une dérogation au principe de la transparence dans l'administration et invite le Conseil fédéral à toujours appliquer la LTrans, même lorsqu'il édicte des actes en vertu du droit de nécessité (recommandation n° 17 du rapport).

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 le personnel fédéral (LPers)	177.220.1	Art. 22a al. 7 E-LPers	Message du 28 août 2024 État : consultation au parlement
Message relatif à la loi fédérale sur la transparence des personnes morales et l'identification des ayants droit économiques (LTPM)		Art. 53 al. 4 LTrans	Message du 22 mai 2024 État : consultation au parlement
Modification de la loi sur l'assurance maladie (2 ^e volet de mesures visant à maîtriser les coûts)	832.10 831.20	Art. 52c LAMAL (norme de délégation) Art. 52d al. 5 LAMAL Disposition transitoire LAMAL al. 4 Art. 14 ^{quinquies} al. 2 u. 3 LAI (norme de délégation) Art. 14 ^{sexies} al. 5 LAI Disposition transitoire LAI al. 1	Adoptée par le Parlement le 21 mars 2025.
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

Acte (titre court) et abréviation	RS	Disposition	Date d'entrée en vigueur
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 (cf. Arrêt du TF 4A_249/2021 du 10 juin 2021)	1 ^{er} juillet 2008
Ordonnance sur les brevets (OBI)	232.141		
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

Tableau 5 : Dispositions ne constituant PAS des dispositions spéciales aus sense 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



Le PFPDT

3.1 Prestations et ressources

Prestations et ressources dans le domaine de la protection des données

Effectifs

Les effectifs du PFPDT dédiés à la protection des données sont demeurés stables depuis 2023, année de l'entrée en vigueur de la nouvelle LPD, avec 33 postes à plein temps.

Tableau 6: Effectifs affectés aux questions relatives à la LPD

2023	33
2024	33
2025	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 01.04.2024 au 31.03.2025, 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	20.8 %
Conseil Secteur privé	18,0 %
Collab. avec les autorités étrangères	15,1 %
Collab. avec les cantons	1,2 %
Total Conseils	55,1 %
Surveillance	20,2 %
Certification	0,1 %
Total Surveillance	20,3 %
Information	12,5 %
Formation / Conférences	2,6 %
Total Information	15,1 %
Législation	9,5 %
Total Législation	9,5 %
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 des grands projets numériques. Il exerce sa fonction de conseil aussi bien au sein de l'administration fédérale, par exemple dans les projets CEBA (cf. ch. 1.1), POLAP (cf. ch. 1.2), la reconnaissance faciale à l'aéroport de Zürich (cf. ch. 1.6) ou encore Justitia 4.0 (cf. ch. 1.1) qu'auprès d'entreprises publiques (CFF, Swisscom, cf. ch. 1.6) et des entreprises privées. Dans le cadre de ces projets, le PFPDT est souvent amené à examiner des analyses d'impact relatives à la protection des données. Les ressources en personnel consacrées au groupe Conseil ont atteint 55,1% au cours de l'année sous revue, ce qui est légèrement supérieur à la valeur de l'année précédente (53,3%).

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

Tableau 8: Objectifs du PFPDT en matière de protection des données

Groupes 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.

Surveillance et campagnes

Le nombre de dénonciations que les trois équipes du domaine de direction Protection des données ont traitées pour l'année sous revue se chiffre à 1053. Ainsi, la part des ressources affectées aux activités de surveillance et aux procédures s'élevait à 20,3 %, ce qui représente une nette augmentation par rapport à la moyenne de 15 % des années de référence depuis 2015. Comme prévu lors de la planification de ses objectifs stratégiques, le PFPDT a renforcé son activité de surveillance, ce qui se reflète dans les statistiques. Le tableau ci-dessous distingue les différentes activités de surveillance du PFPDT, des interventions à bas seuils en passant par les enquêtes préliminaires aux enquêtes formelles.

Deux campagnes ont été mises sur pied afin de sensibiliser le plus grand nombre de personnes, organes fédéraux ou entreprises privées à des thématiques choisies. Ainsi, une campagne au sujet de l'utilisation du NAVS en dehors des assurances sociales a été déployée auprès des organes fédéraux (cf. Accent) et une campagne concernant les formulaires d'inscription relatifs à la location d'un appartement a été publiée et communiquées aux intéressés (cf. chap. 1.3).

Violations de la sécurité des données

Au cours de la période sous revue, 363 violations de la sécurité des données ont été signalées au PFPDT, dont 344 au moyen du formulaire en ligne. 19 annonces ont été transmises au PFPDT par le biais d'autres canaux, tels que le courrier électronique ou postal. Dans 26 cas, le signalement était volontaire.

Pour cette période, on a également calculé le temps qui s'écoule entre la survenance d'une violation de la sécurité des données et la notification auprès du PFPDT : dans environ 40 % des cas, la notification a eu lieu dans les 6 jours. Après 21 jours, environ 80 % des violations de la sécurité des données ont été annoncées.

Tableau 10: Annonce des violations de la sécurité des données

Annonces	363
dont volontaires	26
dans les 6 jours	40%
dans les 21 jours	80%

Tableau 9: Activités de surveillance et campagnes (cf. p. 22)

Dénonciations	1053
dont	1023 contre des privés 30 contre la Confédération 788 traitées 265 pendantes
Interventions à bas seuil	108
dont	90% ont été volontairement suivies
Enquêtes préliminaires	20
Enquêtes	9
dont	6 ouvertes 3 clôturées avec des mesures administratives
Décisions pendantes devant le TAF	2
Campagnes	2
dont	1 à l'intention des autorités fédérales 1 à l'intention des entreprises privées

Information

Les ressources utilisées pour le groupe de prestations « Information » ont pu être à nouveau réduites au cours de l'année de référence, avec une valeur de 15,1% par rapport à l'année précédente. (17,8%).

Législation

Les changements induits par la transformation numérique des offices fédéraux en matière de traitement des données nécessitent un grand nombre de nouvelles dispositions ou de révisions du droit fédéral, sur lesquelles le PFPDT est appelé à se prononcer dans le cadre des diverses procédures de consultation. L'investissement des différentes équipes du PFPDT ne doit pas être négligé dans la mesure où la majeure partie des consultations nécessitent une analyse interdisciplinaire par ces derniers (protection des données, informatique,

international et principe de la transparence). En outre, lorsque ces projets sont associés à de grands projets informatiques ou que le traitement envisagé est susceptible d'entraîner un risque résiduel élevé pour la personnalité ou les droits fondamentaux de la personne concernée, des analyses d'impact doivent également être passées en revue. Au cours de l'année sous revue, nous avons participé à 271 consultations des offices.

Tableau 11: Consultations des offices

Total	274
dont closes	250

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

Les effectifs pour les médiations et les recommandations en vertu de la loi sur le principe de la transparence restent inchangés, avec 6 postes à plein temps. Le Préposé continuera à œuvrer pour que les retards de traitement dus au nombre toujours élevé de demandes de médiation soient résorbés. La rapidité avec laquelle cela pourra être réalisé dépendra de l'évolution quantitative des demandes en médiation et de leur complexité.

Tableau 12: Effectifs affectés aux questions relatives à la LTrans

2023	5,4
2024	6,2
2025	6,2

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 2024 : CAJ-E sur la loi fédérale sur l'identité électronique et autres moyens de preuves électroniques (loi sur l'e-ID)
- Avril 2024 : sous-commissions CDF-E et CDF-N sur les comptes 2023
- Avril 2024 : CIP-E sur la loi fédérale sur le système national de consultation des adresses des personnes physiques (loi sur le service national des adresses, LSAdr)
- Mai 2024 : CIP-N sur la loi sur la protection des données. Ajouter une disposition sur les décisions automatisées qui se fondent sur l'intelligence artificielle
- Juin 2024 : CIP-E sur la loi fédérale sur le système national de consultation des adresses des personnes physiques (loi sur le service national des adresses, LSAdr)
- Juin 2024 : Sous-commission CdG-E/N sur le Rapport d'activités du PFPDT 2023/2024
- Juin 2024 : CIP-N sur la loi fédérale sur les données relatives aux passagers aériens
- Juin 2024 : CAJ-E sur la loi fédérale sur l'identité électronique et autres moyens de preuves électroniques (loi sur l'e-ID)
- Août 2024 : CPS-N sur la loi fédérale sur les données relatives aux passagers aériens
- Août 2024 : CIP-E sur la loi fédérale sur l'identité électronique et autres moyens de preuves électroniques (loi sur l'e-ID)
- Août 2024 : CdG-N visite de notre service par la sous-commission DFJP/ChF
- Octobre 2024 : sous-commissions CDF-E et CDF-N sur le budget 2025
- Octobre 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, LSAdr)
- Octobre 2024 : CIP-N sur la loi sur le personnel fédéral de la Confédération (LPers)

Visite de service de la sous-commission DFJP/ChF de la Commission de gestion du Conseil National

Les Commissions de gestion (CdG) exercent, sur mandat des Chambres fédérales, la haute surveillance sur la gestion du Conseil fédéral et de l'administration fédérale, des tribunaux fédéraux et des autres organes chargés de tâches de la Confédération.

C'est dans ce cadre que, le 27 août 2024, la sous-commission DFJP/ChF s'est entretenue avec le Préposé fédéral ainsi que les cadres du PFPDT sur les missions, les tâches et les compétences du PFPDT ainsi que les affaires en cours. Cette visite a notamment permis d'échanger sur les défis actuels et de s'informer sur la satisfaction des employés.

L'opportunité a également été offerte au PFPDT de présenter les sujets importants actuels en rapport avec le principe de transparence et la protection des données.

Conseiller à la protection des données du PFPDT

Le conseiller à la protection des données de notre autorité 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.

Au cours de la période sous revue, seize demandes d'information et une demande d'effacement sont parvenues au conseiller à la protection des données. Ce dernier a fourni les renseignements à 6 personnes concernées dans le délai imparti. Les autres demandes concernaient des données personnelles que le PFPDT ne possédait pas ou n'avait pas accès. En effet, il arrive souvent que des citoyennes et citoyens croient que le PFPDT a un accès à toutes les bases de données et données personnelles de l'administration fédérale. Ce n'est toutefois pas le cas.

17:32

5G 53

Abbrechen

Fotos

Sammlungen

Fertig

Q Mediathek durchsuchen ...



Beschränkter Zugriff auf deine Mediathek

„Instagram“ kann nur auf die Objekte zugreifen, die du auswählst. Die App kann Inhalte zu deiner Mediathek hinzufügen, selbst wenn keine Objekte ausgewählt sind.



3.2 Communication

Le PFPDT a publié en 2024 15 brèves et 5 communiqués de presse. Dans le domaine de la LTrans, il a émis et publié sur son site 30 recommandations. Côté justice, le principe de la transparence dans l'administration a été évoqué dans 14 arrêts du Tribunal administratif fédéral et dans un arrêt du Tribunal fédéral. Certains services de l'administration fédérale poursuivent leurs efforts pour soustraire du champ d'application de la LTrans tout ou partie des activités des autorités. Le PFPDT tient une liste à ce sujet, disponible sur son site internet.

Communiqués de presse

Le PFPDT accompagne généralement la clôture de ses procédures formelles d'un communiqué de presse. En 2024, ce fut le cas pour les procédures d'établissement des faits menées contre deux offices fédéraux, fedpol et l'OFDF, dans le domaine de l'administration, et contre les entreprises Xplain, Digitec Galaxus et la plateforme de vente aux enchères Ricardo dans le secteur privé. Toutes ces procédures ont été menées à bien selon l'ancien droit.

Brèves

Sept brèves étaient consacrées à la protection transfrontalière des données dans le domaine international. Le PFPDT est par exemple intervenu auprès du groupe Meta, qui souhaitait utiliser les données de ses utilisateurs en Suisse sans leur consentement afin d'améliorer son IA. Compte tenu des préoccupations croissantes suscitées par l'extraction massive des données sur les plateformes de réseaux sociaux (moissonnage ou data scraping), notamment pour alimenter les systèmes d'IA, le PFPDT a cosigné avec seize autres autorités nationales de protection des données une déclaration finale sur les moyens dont disposent les entreprises de médias sociaux pour mieux protéger les données personnelles.

Information et sensibilisation

Depuis la refonte de son site internet en 2023, le PFPDT a élaboré divers guides et aide-mémoire concernant notamment les nouveautés découlant de l'entrée en vigueur de la LPD révisée ou la transformation numérique et les phénomènes technologiques qui l'accompagnent tels que l'IA. Mentionnons également le guide relatif aux traitements de données au moyen de cookies et de technologies similaires, le guide relatif à l'annonce des violations de la sécurité des données et l'information des personnes concernées en vertu de l'art. 24 LPD, l'aide-mémoire relatif aux enquêtes concernant des violations des prescriptions de protection des données ouvertes par le PFPDT ou encore l'aide-mémoire « Planifier et motiver les accès en ligne aux données personnelles ».

Site internet

Le site web a fait peau neuve lors de la migration sur un nouveau logiciel et propose désormais une assistance rapide et disponible à tout moment sous la forme d'une foire aux questions détaillée. Les nouveaux formulaires de contact

offrent aux usagers un moyen aussi simple que spécifique de soumettre leurs requêtes au PFPDT. Le recours aux portails de notification reste soutenu (cf. statistiques). Tous les guides et les aide-mémoire sont disponibles à la rubrique « Documentation ».

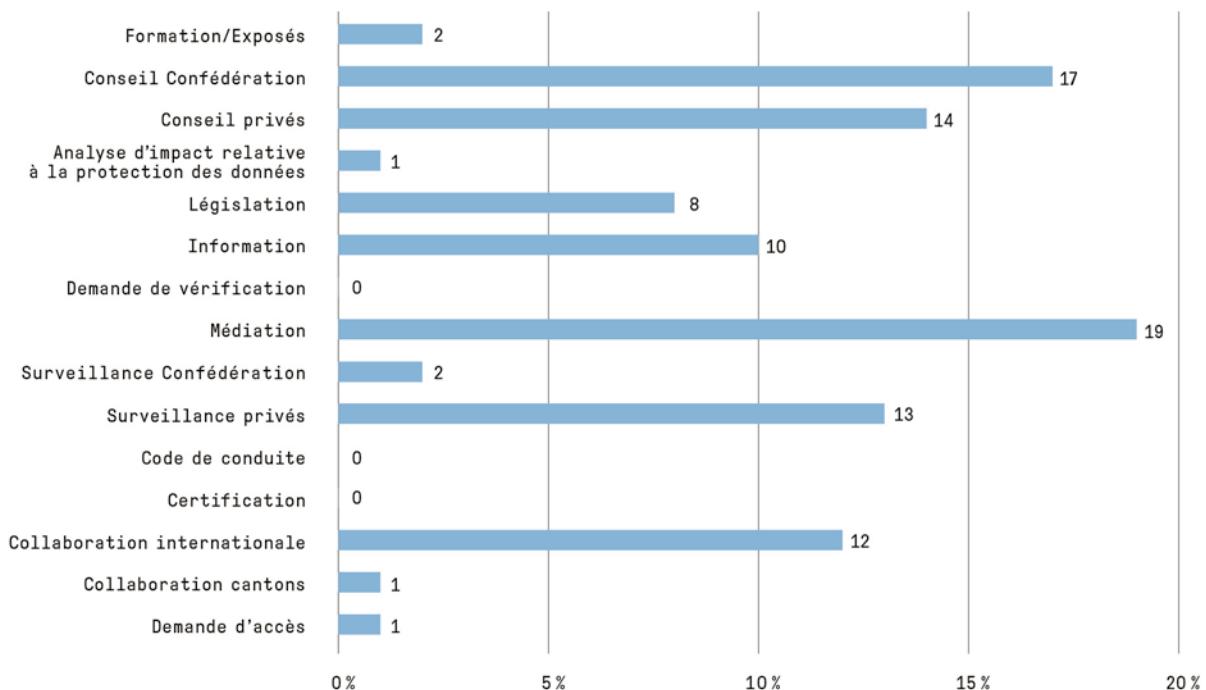
Travail de presse

Le PFPDT a répondu l'an dernier à environ 200 demandes émanant de journalistes. La couverture média de sujets d'actualité liés à la protection et à la sécurité des données ou à la LTrans et au principe de la transparence dans l'administration contribue à la sensibilisation de la population et constitue une part importante du travail de communication du PFPDT, même s'il donne parfois lieu à des controverses, ou peut-être précisément à cause de cela. Le Préposé intervient ainsi régulièrement dans les médias pour défendre les intérêts des citoyens concernés en publiant des prises de position critiques.

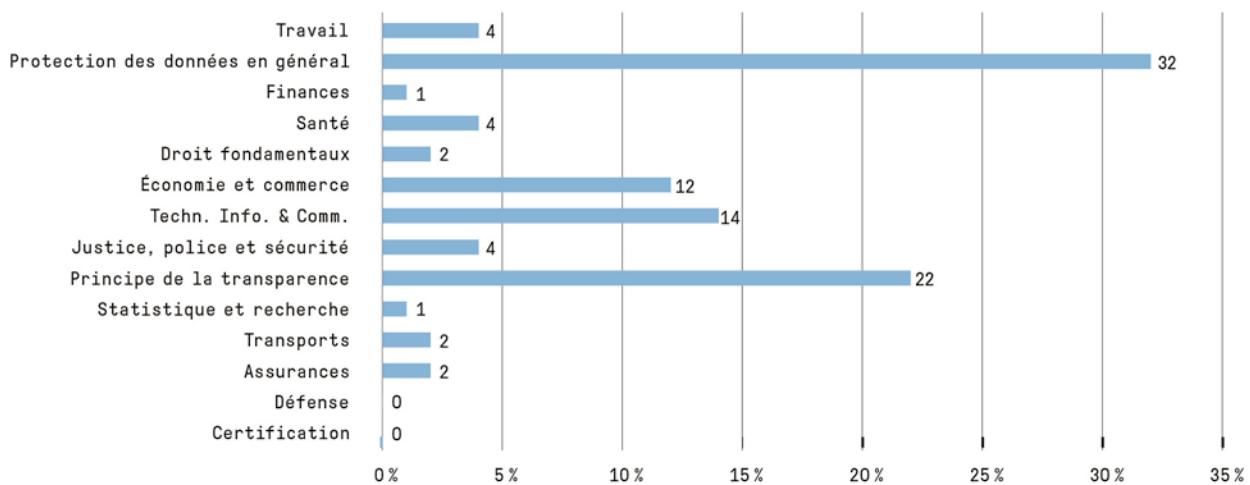
3.3 Statistiques

Statistiques des activités du PFPDT du 1^{er} avril 2024 au 31 mars 2025

Charge de travail par tâche en %



Charge de travail par domaine in %

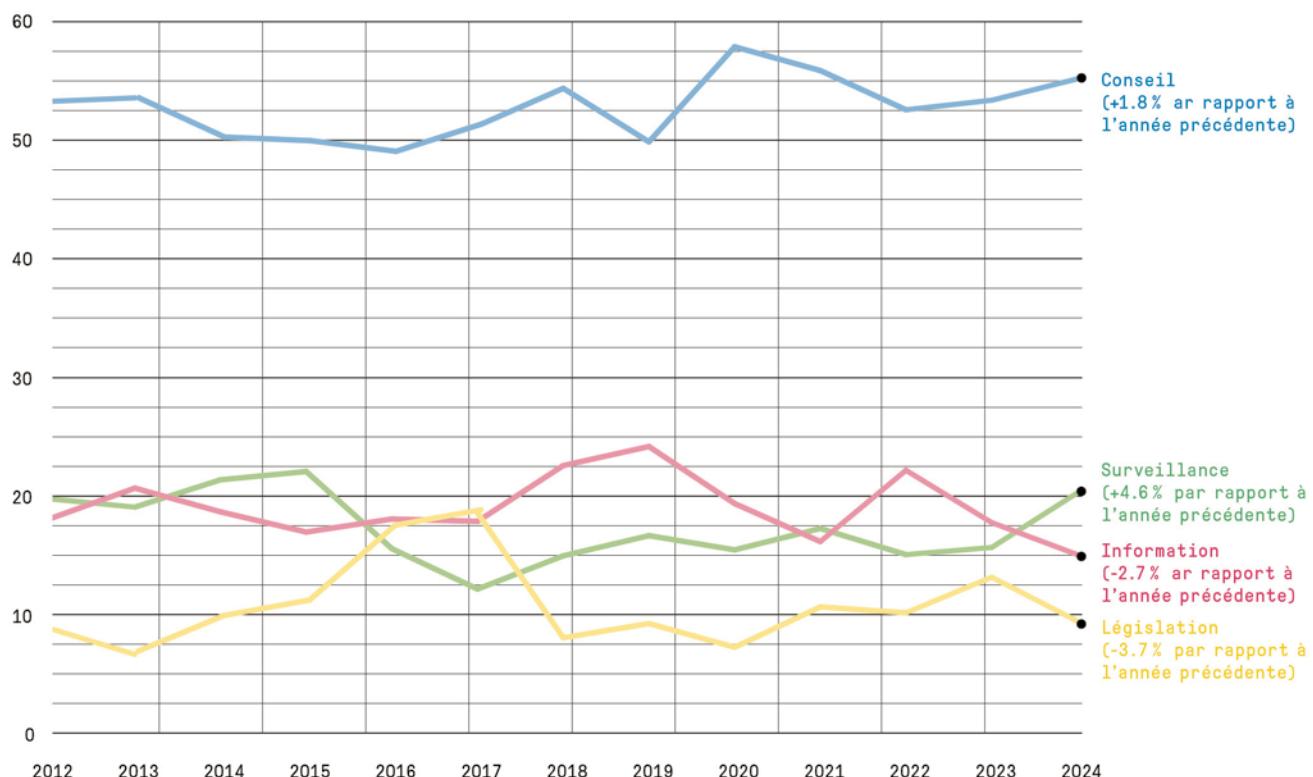


Nombre d'opérations d'affaires

Procédures de médiation	184
Consultations des offices	274
Conseils	1248
Enquêtes sur dénonciation	1087
Procédure de recours	9
Conférences et événements	49
Demandes médias	170
Demandes par téléphone (hotline)	1180
Demandes via formulaire de contact	1823
Demandes par courriel	914
Entrées par courrier postal	604
Total des entrées de personnes physiques	3668
Total des refus standard	584
Pourcentage de refus standard	16%

Comparaison pluriannuelle

(en pourcentage)



**Vue d'ensemble des demandes d'accès selon la loi sur la transparence
du 1^{er} janvier au 31 décembre 2024**

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	123	68	12	30	1	8	4
DFAE	306	137	27	77	6	15	44
DFI	292	131	17	79	19	25	21
DFJP	212	111	20	37	10	3	31
DDPS	527	366	23	90	10	8	30
DFF	145	54	28	43	4	5	11
DEFR	290	146	25	35	63	13	8
DETEC	324	142	23	82	20	22	35
MPC	8	3	2	0	0	3	0
SP	5	1	2	1	0	0	1
Total 2024 (%)	2232	1159	(52)	179	(8)	474	(21)
Total 2023 (%)	1738	(100)	830	(48)	176	(10)	402
Total 2022 (%)	1180	(100)	624	(53)	99	(8)	236
Total 2021 (%)	1385	(100)	694	(50)	126	(9)	324
Total 2020 (%)	1193	(100)	610	(51)	108	(9)	293
Total 2019 (%)	916	(100)	542	(59)	86	(9)	171
Total 2018 (%)	647	(100)	355	(55)	66	(10)	119
Total 2017 (%)	586	(100)	325	(56)	108	(18)	106
Total 2016 (%)	554	(100)	299	(54)	88	(16)	105
Total 2015 (%)	600	(100)	320	(53)	99	(17)	128
Total 2014 (%)	582	(100)	302	(52)	124	(21)	124
						15	(3)
						17	(3)
							-
							-
							-
							-

**Statistique des demandes d'accès selon la loi sur la transparence
du 1^{er} janvier au 31 décembre 2024**

		ChF	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
			dont soumis les années précédentes						
Chancellerie fédérale ChF	ChF	94	0	50	11	26	1	2	4
	PFPDT	29	0	18	1	4	0	6	0
	Total	123	0	68	12	30	1	8	4
Département fédéral des affaires étrangères DFAE	DFAE	306	0	137	27	77	6	15	44
	Total	306	0	137	27	77	6	15	44
Département fédéral de l'intérieur DFI	SG DFI	22	0	13	2	4	0	1	2
	BFEG	8	1	8	0	0	0	0	0
	OFC	15	0	9	2	2	0	2	0
	AFS	2	1	2	0	0	0	0	0
	MeteoSuisse	3	0	3	0	0	0	0	0
	BN	0	0	0	0	0	0	0	0
	OFSP	85	0	21	4	41	4	13	2
	OFS	4	0	4	0	0	0	0	0
	OFAS	32	0	21	0	6	1	0	4
	OSAV	42	0	23	2	8	3	3	3
	MNS	0	0	0	0	0	0	0	0
	swissmedic	70	8	25	5	18	11	3	8
	Suva	7	0	2	2	0	0	1	2
	compenswiss	2	0	0	0	0	0	2	0
Total		292	10	131	17	79	19	25	21
Département fédéral de justice et police DFJP	SG DFJP	34	1	19	0	6	1	0	8
	OFJ	54	2	25	10	4	2	0	13
	fedpol	35	0	9	10	11	0	2	3
	METAS	2	0	2	0	0	0	0	0
	SEM	61	0	39	0	12	6	0	4
	Service SCPT	2	0	1	0	1	0	0	0
	ISDC	4	0	3	0	0	0	0	1
	IPI	4	0	4	0	0	0	0	0
	CFMJ	6	0	4	0	0	1	1	0
	CAF	2	0	2	0	0	0	0	0
	ASR	5	0	2	0	3	0	0	0
	CSI	3	0	1	0	0	0	0	2
	CNPT	0	0	0	0	0	0	0	0
Total		212	3	111	20	37	10	3	31

		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	87	5	19	7	39	5	5	12
	Défense	38	0	9	0	19	3	0	7
	SRC	16	0	2	1	10	0	0	3
	AS-Rens	12	1	2	7	2	1	0	0
	armasuisse	18	1	2	4	9	1	2	0
	OFSPPO	317	0	311	2	0	0	1	3
	OFPP	8	0	4	0	4	0	0	0
	swisstopo	4	0	3	0	0	0	0	1
	OA	2	0	2	0	0	0	0	0
	SEPOS	23	0	11	2	7	0	0	3
	OFCS	2	0	1	0	0	0	0	1
Total		527	7	366	23	90	10	8	30
Département fédéral des finances DFF	SG DFF	27	1	9	6	8	1	0	3
	AFF	11	0	6	2	2	0	1	0
	OPPER	5	0	4	0	1	0	0	0
	AFC	20	0	7	3	8	0	1	1
	OFDF	32	5	8	9	10	0	3	2
	OFCL	12	0	7	4	1	0	0	0
	OFIT	4	0	2	0	1	0	0	1
	CDF	18	0	8	4	3	2	0	1
	SFI	11	0	1	0	7	0	0	3
	PUBLICA	4	0	1	0	2	1	0	0
	CdC	1	0	1	0	0	0	0	0
Total		145	6	54	28	43	4	5	11

		Nombre de demandes d'accès	dont soumis les années précédentes	Accès accordé	Accès refusé	Accès accordé partiellement/différemment	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	20	0	6	2	4	2	4	2
	SECO	51	1	16	10	16	8	1	0
	SEFRI	11	0	6	2	1	0	0	2
	OFAG	22	2	12	2	3	2	0	3
	Agroscope	3	0	2	0	0	0	1	0
	OFAE	0	0	0	0	0	0	0	0
	OFL	4	0	4	0	0	0	0	0
	SPR	8	0	3	1	4	0	0	0
	COMCO	16	0	9	1	3	0	2	1
	CIVI	3	0	3	0	0	0	0	0
	BFC	1	0	1	0	0	0	0	0
	FNS	4	1	1	2	1	0	0	0
	IFFP	0	0	0	0	0	0	0	0
	Conseil EPFL	143	0	81	5	2	50	5	0
	InnoSuisse	4	0	2	0	1	1	0	0
Total		290	4	146	25	35	63	13	8

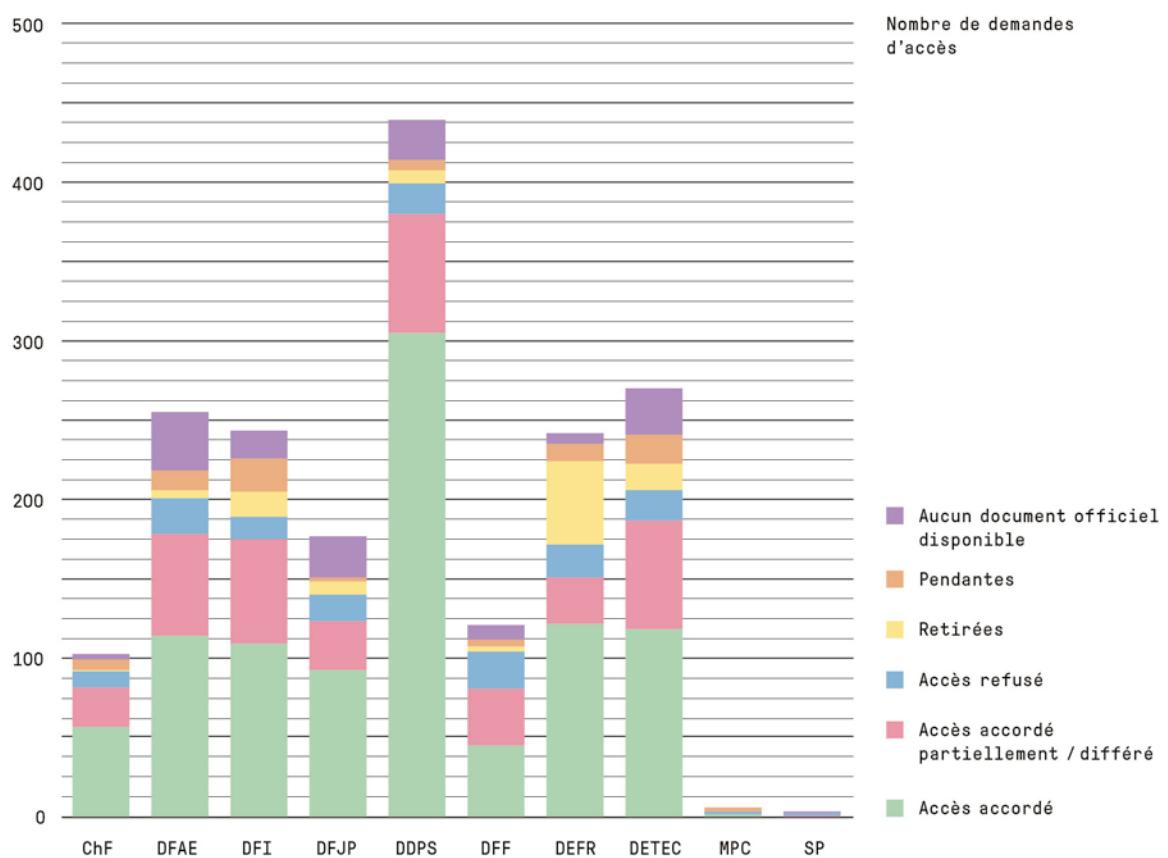
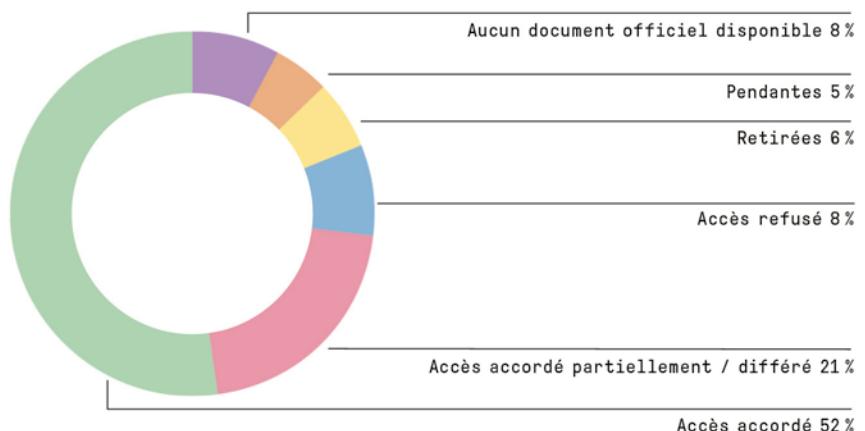
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC	SG DETEC	31	1	13	2	3	0	1	12
	OFT	19	0	9	0	5	1	2	2
	OFAC	26	2	10	4	6	3	0	3
	OFEN	19	1	9	0	6	2	2	0
	OFROU	27	0	23	0	2	1	0	1
	OFCOM	34	2	7	2	11	5	3	6
	OFEV	144	5	58	14	43	8	11	10
	ARE	9	0	8	1	0	0	0	0
	ComCom	2	0	1	0	1	0	0	0
	IFSN	7	3	2	0	3	0	2	0
	ESTI	1	0	0	0	0	0	1	0
	PostCom	3	2	1	0	2	0	0	0
	AIEP	0	0	0	0	0	0	0	0
	IFFP	0	0	0	0	0	0	0	0
	SUST	2	0	1	0	0	0	0	1
Total		324	16	142	23	82	20	22	35

		Nombre de demandes d'accès	dont soumis les années	Accès accordé	Accès refusé	Accès accordé partiellement/différé	Demandes d'accès retirées	Demandes d'accès pendantes	Aucun document officiel disponible
	MPC	8	0	3	2	0	0	3	0
	Total	8	0	3	2	0	0	3	0
Ministère public de la Confédération	MPC	8	0	3	2	0	0	3	0
Services du Parlement	SP	5	0	1	2	1	0	0	1
SP	Total	5	0	1	2	1	0	0	1
	Somme totale	2232	46	1159	179	474	133	102	185

Nombre de demandes en médiation par catégories de requérants

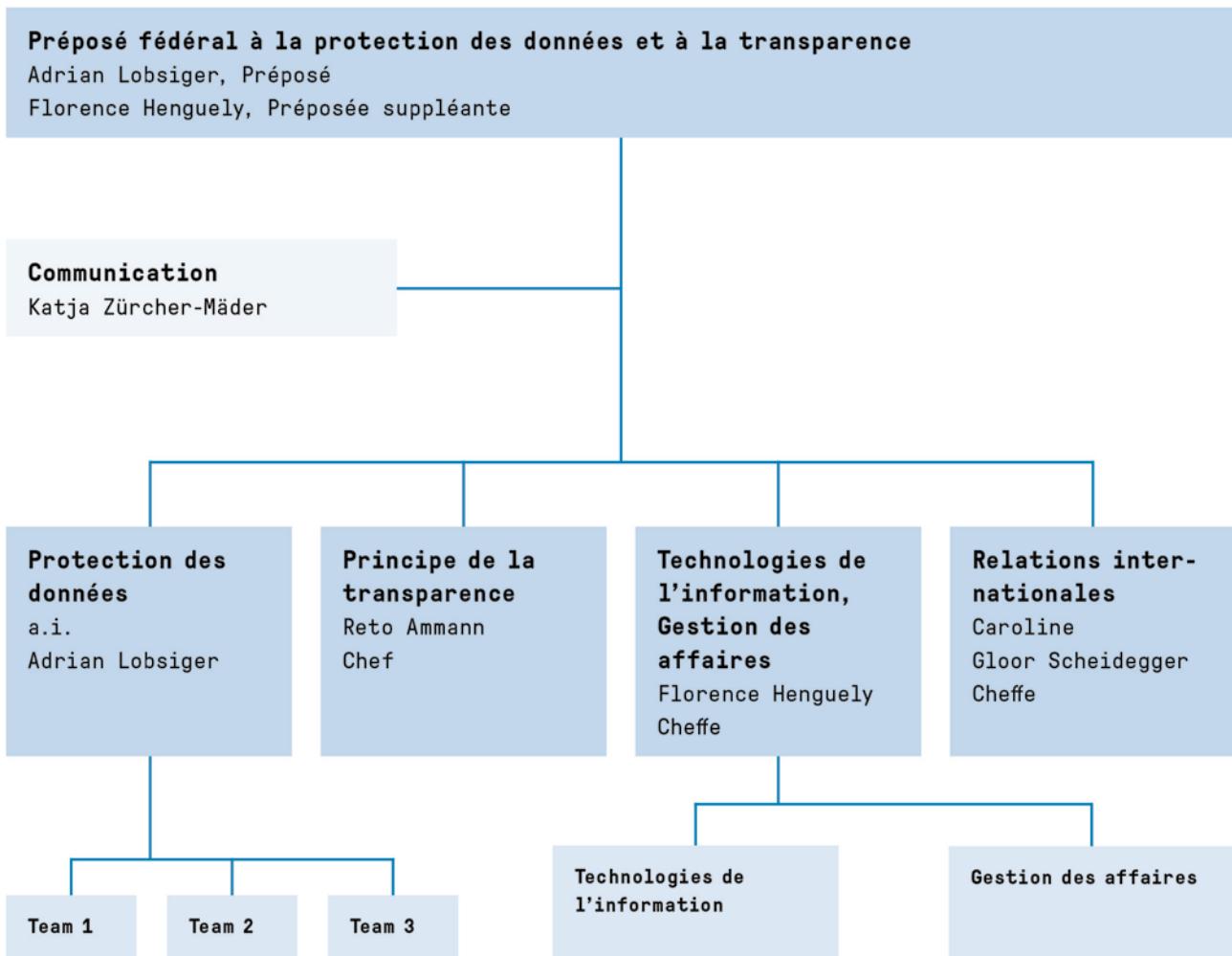
Catégorie des requérants	2024	2023	2022	2021	2020	2019	2018	2017
Médias	61	74	47	53	31	34	24	21
Personnes privées (ou requérants ne pouvant pas être attribués de manière précise)	66	31	37	49	42	40	26	35
Représentants de milieux intéressés (associations, organisations, sociétés etc.)	16	8	9	16	5	7	9	14
Avocats	45	16	27	12	7	5	4	2
Entreprises	14	3	9	19	7	47	13	7
Universités	0	0	0	0	1	0	0	0
Total	202	132	129	149	93	133	76	79

**Demandes d'accès de l'ensemble de l'administration fédérale
du 1^{er} janvier au 31 décembre 2024**



3.4 Organisation du PFPDT (État au 31 mars 2025)

Organigramme



Personnel du PFPDT

Nombre d'employés	44		
EPT	37.2		
par sexe	Femmes	22	50 %
	Hommes	22	50 %
par pourcentage d'emploi	1-89 %	29	65.91 %
	90-100 %	15	34.09 %
par langue	Allemand	31	70.45 %
	Français	12	27.27 %
	Italien	1	2.27 %
par âge	20-49 ans	25	56.82 %
	50-65 ans	19	43.18 %
Postes dirigeants	Femmes	5	55.56 %
	Hommes	4	44.44 %
	Total	9	

Liste des abréviations

AIPD Analyse d'impact relative à la protection des données	LCF Loi sur le Contrôle fédéral des finances	OTrans Ordonnance sur la transparence
AMVP Assemblée mondiale pour la protection de la vie privée	LDEP Loi fédérale sur le dossier électronique du patient	PFPDT Préposé fédéral à la protection des données et à la transparence
ANS Administration numérique suisse	LDPa Loi sur les données relatives aux passagers aériens	PNR Données des passagers des compagnies aériennes
CEPD Comité européen de la protection des données	LPD Loi sur la protection des données	Privatim Conférence des Préposé(e)s suisses à la protection des données
CEPD Contrôleur européen de la protection des données	LPers Loi sur le personnel de la Confédération	RA Rapport annuel du PFPDT
CPN Comité de la politique du numérique de l'OCDE	LRens Loi fédérale sur le renseignement	RGPD Règlement général sur la protection des données
DataReg Registre des activités de traitement des organes fédéraux	LSI Loi sur la sécurité de l'information	SIS II Système d'information Schengen de deuxième génération
DEP Dossier électronique du patient	LTPM Loi sur la transparence des personnes morales	SRC Service de renseignement de la Confédération
e-ID Identité électronique	LTrans Loi fédérale sur le principe de la transparence dans l'administration	TIC Technologies de l'information et de la communication
Fedpol Office fédéral de la police	OFCS Office fédéral de la cybersécurité	TNI Secteur Transformation numérique et gouvernance de l'information de la Chancellerie fédérale
IA Intelligence artificielle	OFDF Office fédéral de la douane et de la sécurité des frontières	VIS Système d'information sur les visas
LA Loi fédérale sur l'aviation	OPDo Ordonnance sur la protection des données	
LAVS Loi fédérale sur l'assurance-vieillesse et survivants		

Table des illustrations

Graphiques	Tableaux	
Graphique 1: Demandes d'accès – évolution depuis 2011 p. 69	Tableau 1: Solutions amiables p. 73	Tableau 9: Activités de surveillance et campagnes..... p. 91
Graphique 2: Émoluments prélevés depuis l'entrée en vigueur de la LTrans p. 71	Tableau 2: Durée des procédures de médiation p. 74	Tableau 10: Annonce des violations de la sécurité des données..... p. 91
Graphique 3: Demandes en médiation depuis l'entrée en vigueur de la LTrans p. 72	Tableau 3: Procédures de médiation pendantes p. 75	Tableau 11: Consultations des offices p. 92
	Tableau 4: Dispositions spéciales au sens de l'art. 4 LTrans p. 84-85	Tableau 12: Effectifs affectés aux questions relatives à la LTrans..... p. 92
	Tableau 5: Dispositions ne constituant PAS des dispositions spéciales aus sense de l'art. 4 LTrans p. 86	
	Tableau 6: Effectifs affectés aux questions relatives à la LPD p. 90	
	Tableau 7: Prestations Protection des données..... p. 90	
	Tableau 8: Objectifs du PFPDT en matière de protection des données...p. 90	

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. 410.032.F

Mise en page : Ast & Fischer AG, Wabern

Photographie : Monika Flückiger

Police d'écriture : Pressura, Documenta

Impression : Ast & Fischer AG, Wabern

Papier : PlanoArt®, sans bois, extra blanc



Chiffres clés

Prestations protection des données

55.1% 20.3% 15.1% 9.5%

Conseil

Surveillance

Information

Législation

Surveillance

108 19 9 2

Intervention à
bas-seuil

Enquêtes
préliminaires

Enquêtes selon
l'art. 49 LPD

pendant devant le
TAF

Demandes d'accès au PFPDT

18 4 1 0 6 0

accordées

accordées
partiellement /
différées

refusé

retirées

pendantes

aucun document
officiel disponible

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

Téléphone : +41 (0)58 462 43 95 (lu–ve, 10h–11h 30)

Télifax : +41 (0)58 465 99 96