

Rapport d'activité 2016

—
pour la période du 1^{er} janvier
au 31 décembre 2016



ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

Autorité cantonale de la transparence et de la protection des données
Rue des Chanoines 2, CH-1700 Fribourg
T. +41 26 322 50 08, F + 41 26 305 59 72
www.fr.ch/atprd

Mai 2017

—
Imprimé sur papier 100% recyclé

**AU GRAND CONSEIL
DU CANTON DE FRIBOURG**

Monsieur le Président,
Mesdames et Messieurs les Député-e-s,

Nous avons l'honneur de vous adresser le rapport 2016 de l'Autorité cantonale de la transparence et de la protection des données. Après un bref rappel de quelques généralités concernant les bases de fonctionnement de l'Autorité (I), il convient de distinguer les activités de la Commission proprement dite (II) de celles des Préposées à la transparence et à la protection des données (III). Nous continuerons avec quelques remarques au sujet de la coordination des deux champs d'activité (IV) pour aboutir à des considérations finales (V).

Nous vous en souhaitons bonne lecture et vous prions d'agréer, Monsieur le Président, Mesdames et Messieurs les Député-e-s, l'expression de notre haute considération.

Fribourg, avril 2017

Le Président
de la Commission

L. Schneuwly

La Préposée
à la transparence

A. Zunzer Raemy

La Préposée
à la protection des données

A. Reichmuth Pfammatter

Table des matières

Table des abréviations et termes utilisés	6
I. TÂCHES ET ORGANISATION DE L'AUTORITÉ	7
A. En général	7
B. Collaboration supracantonale	9
C. Engagement dans la formation	10
D. Relations avec le public	10
II. ACTIVITÉS PRINCIPALES DE LA COMMISSION	11
A. Sujets communs	11
1. Prises de position	11
1.1 En général	11
1.2 Quelques exemples de prises de position	11
2. Autres activités	14
B. Transparence	14
1. Evaluation du droit d'accès	14
C. Protection des données	14
1. Décisions et recours	14
III. ACTIVITÉS PRINCIPALES DES PRÉPOSÉES	16
A. Transparence	16
1. Points forts	16
1.1 Médiations	16
1.2 Demandes	17
1.3 Adaptation de la Llnf à la Convention d'Aarhus	18
2. Statistiques	19
B. Protection des données	19
1. Points forts	19
1.1 Demandes	19
1.2 Contrôles	28
1.3 FRI-PERS et vidéosurveillance	29
1.4 ReFi – registre des fichiers	31
1.5 Echanges	32
2. Statistiques	32
IV. COORDINATION ENTRE LA TRANSPARENCE ET LA PROTECTION DES DONNÉES	34
V. REMARQUES FINALES	34
ANNEXES: statistiques	35-38

Table des abréviations et termes utilisés

AFOCI	Association fribourgeoise pour l'organisation des cours interentreprises
AMICUS	Banque de données des chiens en Suisse
AP	Avant-projet
ATPrD	Autorité cantonale de la transparence et de la protection des données
AVS	Assurance-vieillesse et survivants
BCU	Bibliothèque cantonale et universitaire
CC	Code civil du 10 décembre 1907
CdC	Conférence des gouvernements cantonaux
CMA	Commission des mesures administratives en matière de circulation routière
DSJ	Direction de la sécurité et de la justice
ECAB	Etablissement cantonal d'assurance des bâtiments
EMS	Etablissement médico-social
EPT	Equivalent plein temps
FRIAC	Application informatique Fribourg – Autorisation de construire
FRI-PERS	Plateforme informatique cantonale du contrôle des habitants
HESSO//FR	Loi du 15 mai 2014 sur la Haute Ecole spécialisée de Suisse occidentale//Fribourg
LAMal	Loi fédérale sur l'assurance-maladie du 18 mars 1994
LAVS	Loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants
LCo	Loi du 25 septembre 1980 sur les communes
LEDP	Loi du 6 avril 2001 sur l'exercice des droits politiques
LICD	Loi du 6 juin 2000 sur les impôts cantonaux directs
LInf	Loi du 9 septembre 2009 sur l'information et l'accès aux documents
LPD	Loi fédérale sur la protection des données du 19 juin 1992
LPrD	Loi du 25 novembre 1994 sur la protection des données
LRS	Loi du 20 mars 2015 sur les résidences secondaires
LVID	Loi du 7 décembre 2010 sur la vidéosurveillance
NAVS13	Numéro AVS à 13 chiffres
OGITAC	Ordonnance du 3 novembre 2015 sur la gestion de l'informatique et des télécommunications dans l'administration cantonale
OVID	Ordonnance du 23 août 2011 sur la vidéosurveillance
PFPDT	Préposé fédéral à la protection des données et à la transparence
Primeo	Application web relative à la gestion des écoles primaires
Privatim	Association des commissaires suisses à la protection des données
RdH	Registre des habitants
ReFi	Registre des fichiers
RegBL	Registre fédéral des bâtiments et des logements
RF	Registre foncier
RSD	Règlement du 29 juin 1999 sur la sécurité des données personnelles
SCC	Service cantonal des contributions
SIS	Système d'information Schengen
SITel	Service de l'informatique et des télécommunications
SPoMi	Service de la population et des migrants
SSF	Service des subsides de formation
TC	Tribunal cantonal
VPN	Virtual private network (Réseau privé virtuel)

I. Tâches et organisation de l'Autorité

A. En général

L'Autorité cantonale de la transparence et de la protection des données (ATPrD) est une autorité indépendante, rattachée administrativement à la Chancellerie. Elle gère aussi bien le domaine de la transparence que celui de la protection des données.

L'Autorité se compose d'une Commission, d'une Préposée à la transparence (50%) et d'une Préposée à la protection des données (50%). Elle compte aussi une collaboratrice administrative (80%) et une juriste (50%). Elle offre en outre la possibilité à de jeunes diplômés d'effectuer un stage juridique de 6 mois (100%) dans les deux domaines. L'Autorité relève que ses tâches de protection des données et de sécurité informatique sont difficiles à remplir de manière satisfaisante étant donné les moyens dont elle dispose. L'évolution des nouvelles technologies et les projets informatiques toujours plus complexes requièrent de pouvoir disposer de ressources supplémentaires.

Les tâches de la **Commission cantonale de la transparence et de la protection des données** sont définies dans l'art. 40b de la Loi fribourgeoise du 9 septembre 2009 sur l'information et l'accès aux documents (LInf)¹ et dans l'art. 30a de la Loi fribourgeoise du 25 novembre 1994 sur la protection des données (LPrD)². Il s'agit essentiellement des tâches suivantes:

- assurer la coordination entre l'exercice du droit d'accès aux documents officiels et les exigences de la protection des données;
- diriger l'activité du ou de la Préposé-e à la transparence et du ou de la Préposé-e à la protection des données;
- donner son avis sur les projets, notamment d'actes législatifs, qui ont un impact sur la protection des données et/ou sur le droit d'accès aux documents officiels ainsi que dans des cas prévus par la loi;
- évaluer régulièrement l'efficacité et les coûts de la mise en œuvre du droit d'accès aux documents et en faire état dans son rapport au Grand Conseil;
- mettre en œuvre la procédure prévue à l'art. 22a LPrD, à savoir inviter l'autorité compétente à prendre les mesures nécessaires, en cas de violation ou de risque de violation de prescriptions légales et, le cas échéant, interjeter recours auprès du Tribunal cantonal contre une décision de rejet de la part d'un organe public.

En 2016, la Commission était présidée par M. *Laurent Schneuwly*, Président du Tribunal civil de la Sarine. Les autres membres de la Commission étaient: M^{me} *Christiana Fountoulakis*, professeure ordinaire de droit privé à l'Université de Fribourg (en congé maternité), M. *Philippe Gehring*, ingénieur en informatique EPFL, M^{me} *Madeleine Joye Nicolet*, ancienne journaliste, M. *André Marmy*, médecin, et M^{me} *Annelise Meyer-Glauser*, ancienne Conseillère communale.

La Commission a tenu neuf séances en 2016. Un procès-verbal rédigé par la collaboratrice administrative fait état des délibérations et des décisions prises par la Commission.

¹ <https://bdlf.fr.ch/frontend/versions/4692>

² <https://bdlf.fr.ch/frontend/versions/4691>

Hors séances, le Président a assuré le suivi des dossiers, la correspondance, les discussions avec les Préposées durant 120 heures sur l'ensemble de l'année.

Tâches des Préposées

Conformément à l'art. 41 c LInf, la **Préposé-e à la transparence** est chargée essentiellement des tâches suivantes:

- informer des modalités d'exercice du droit d'accès la population et les personnes qui souhaitent faire valoir leur droit;
- assurer l'information et la formation des organes publics sur les exigences liées à l'introduction du droit d'accès;
- exercer les fonctions de médiation qui lui sont attribuées par la présente loi;
- exécuter les travaux qui lui sont confiés par la Commission;
- rendre public le résultat final des principaux cas ayant fait l'objet d'une procédure de médiation ou de décision;
- faire rapport à la Commission sur son activité et ses constatations.

Conformément à l'art. 31 LPrD, la **Préposé-e à la protection des données** est chargée essentiellement des tâches suivantes:

- contrôler l'application de la législation relative à la protection des données, notamment en procédant systématiquement à des vérifications auprès des organes concernés;
- conseiller les organes concernés, notamment lors de l'étude de projets de traitement;
- renseigner les personnes concernées sur leurs droits;
- collaborer avec le Préposé fédéral à la protection des données et à la transparence (PF PDT) ainsi qu'avec les autorités de surveillance de la protection des données des autres cantons et avec celles de l'étranger;
- examiner l'adéquation du niveau de protection assuré à l'étranger, au sens de l'art. 12a al. 3;
- exécuter les travaux qui lui sont confiés par la Commission;
- tenir le registre des fichiers (ReFi).

S'y ajoutent des tâches figurant dans d'autres législations, par ex.:

- les tâches de préavis FRI-PERS en matière d'accès à la plateforme informatique contenant les données des registres des habitants et de contrôle des autorisations en collaboration avec le Service de la population et des migrants (Ordonnance du 14 juin 2010 relative à la plateforme informatique contenant les données des registres des habitants)³;
- les tâches de préavis LVID en matière d'autorisation d'installation de systèmes de vidéosurveillance avec enregistrement (Loi du 7 décembre 2010 sur la vidéosurveillance; Ordonnance du 23 août 2011 y relative).⁴

La loi ne répartit pas de manière stricte les tâches de surveillance entre la Commission et la Préposée à la protection des données. Comme jusqu'ici (cf. les rapports annuels précédents⁵), reviennent à la Commission les tâches liées à des affaires de caractère **législatif** et les dossiers dans lesquels il importe de définir une **politique générale** de protection des données. S'y ajoute la mise en œuvre de la procé-

³ <https://bdlf.fr.ch/frontend/versions/4597>

⁴ <https://bdlf.fr.ch/frontend/versions/3089> et <https://bdlf.fr.ch/frontend/versions/3090>

⁵ http://www.fr.ch/atprd/fr/pub/protection_des_donnees/publications/rapports_activite.htm

ture en cas de violation des prescriptions sur la protection des données (art. 30a al. 1 let. c, art. 22a et art. 27 al. 2 LPrD avec le pouvoir de recours contre les décisions des organes publics auprès du Tribunal cantonal).

B. Collaboration supracantonale

La Préposée à la transparence et la Préposée à la protection des données s'attachent à collaborer avec le PFPDT et avec les autorités en la matière dans les autres cantons. Ensemble, elles prennent part aux réunions du *Groupe des préposés latins à la protection des données et à la transparence* qui, en général deux fois par an, permettent aux préposés de Suisse romande de discuter des thèmes actuels et d'échanger leurs expériences en détail.

Dans le domaine de la transparence, le groupe de travail sur le principe de la transparence, auquel participent aussi les collaborateurs concernés du PFPDT et les préposés intéressés, se réunit environ deux fois par an et aborde principalement les questions de la médiation et les thèmes relatifs au principe de la transparence.

La Préposée à la protection des données a également des contacts formels et informels avec le PFPDT. L'Accord d'Association à Schengen, ratifié par la Suisse en mars 2006 et entré en vigueur le 1er mars 2008, prévoit la participation de la Suisse au Système d'Information Schengen (SIS). Cet accord requiert l'instauration d'une autorité nationale de contrôle en matière de protection des données dans tous les Etats participants à la coopération Schengen. En Suisse, ces activités de surveillance sont assurées par le PFPDT et les autorités cantonales de protection des données dans le cadre de leurs compétences respectives. Le *Groupe de coordination des autorités suisses de protection des données*, institué dans le cadre de la mise en œuvre de l'Accord d'Association à Schengen, a été réuni deux fois durant l'année 2016 par le PFPDT⁶. Les thèmes traités lors des séances ont porté notamment sur les dernières évolutions de la législation européenne ainsi que sur la création d'un guide commun pour le contrôle des fichiers de consignment du système d'information de Schengen SIS. Par ailleurs, la Préposée à la protection des données a pris part à plusieurs séances du groupe de travail «protection des données» dans le cadre de l'organisation d'accompagnement Schengen/Dublin de la Conférence des gouvernements cantonaux (CdC); il s'agissait en l'occurrence des travaux de révision et de mise en œuvre qui attendent les cantons dans le cadre de l'exécution des instruments juridiques européens.

Comme les autres autorités cantonales, la Préposée à la protection des données fait en outre partie de l'Association des commissaires suisses à la protection des données **privatim**⁷. L'Autorité a pu profiter également en 2016 des travaux effectués par privatim sur des questions générales d'importance internationale, nationale et intercantonale. Cette *collaboration est très utile*, voire indispensable, pour se forger des opinions et prendre des positions ou au moins des points de vue si possible coordonnés (notamment pour les réponses à des procédures de consultation). L'assemblée générale du printemps s'est déroulée dans la ville d'Appenzell. La Conférence a traité en priorité du thème de la collaboration des organes publics dans le domaine informatique. L'assemblée générale d'automne a eu lieu à Liestal (Bâle-Campagne). A la suite de celle-ci, la révision du paquet européen relatif à la protection des données a été présentée, et ce sous l'angle du besoin d'adaptation des législations cantonales.

⁶ <http://www.edoeb.admin.ch/index.html?lang=fr>

⁷ <http://www.privatim.ch/fr/page-daccueil.html>

Le Président de privatim est, depuis la mi-2016, le Préposé à la protection des données du canton de Bâle-Ville.

C. Engagement dans la formation

La Préposée à la transparence ainsi que la juriste de l'Autorité ont donné des cours dans le cadre de la formation des apprentis et des stagiaires 3+1 (cours AFOCI). La Préposée à la protection des données a présenté quant à elle un cours à l'HEG à l'occasion des formations continues proposées par l'Etat de Fribourg et a dirigé une séance de formation continue d'une demi-journée sur le sujet de la protection des données dans un service social régional et dans un service officiel des curatelles. D'autre part, elle a aussi participé, sur invitation d'un office cantonal, à une séance d'information ayant pour but de discuter des questions des collaborateurs.

D. Relations avec le public

L'Autorité poursuit une politique d'information active, p. ex. par le biais de son site Internet et de publications telles que newsletters, communiqués de presse, guides pratiques et actualités⁸. En mai 2016, l'Autorité cantonale de la transparence et de la protection des données a tenu sa traditionnelle **conférence de presse**.

Dans ses newsletters semestrielles⁹, l'Autorité a fait connaître son travail à un public plus large et a abordé des thèmes d'actualité en lien avec la transparence et la protection des données. De plus, l'Autorité publie chaque année un guide actualisé à **l'attention spécifique des communes**. Ce guide vise à leur fournir des informations et des conseils s'appliquant à des cas concrets.¹⁰

⁸ http://www.fr.ch/atprd/fr/pub/protection_des_donnees/publications.htm

⁹ <http://www.fr.ch/atprd/fr/pub/transparence/publications/newsletter.htm>

¹⁰ http://www.fr.ch/atprd/fr/pub/protection_des_donnees/publications/guide_pratique.htm

II. Activités principales de la Commission

A. Sujets communs

1. Prises de position

1.1. En général

La Commission s'est prononcée sur les différents projets législatifs du **Canton** et sur certains de la **Confédération**. L'Autorité a constaté également en 2016 que la transparence et la protection des données sont souvent **prises en compte** dans les nouvelles dispositions légales. Les projets de loi lui sont normalement communiqués, mais elle remarque que les projets d'ordonnances ne lui parviennent pas dans tous les cas (voir page 13 «Ordonnance modifiant le règlement sur la détention des chiens»).

Eu égard au fait que le respect des principes de la protection des données et de la transparence ne peut se faire de manière efficace que si le législateur intègre ces principes dès le début des travaux législatifs, la Commission souhaite que les rapports explicatifs et messages accompagnant les projets soumis à l'Autorité reflètent le résultat de l'**analyse aux niveaux de la transparence et de la protection de données** (analyse qui, pour la protection des données, relève de la responsabilité des organes publics, art. 17 LPrD).

La Commission reçoit également d'autres projets relativement éloignés de la protection des données ou de la transparence; elle se limite alors à une prise de position ponctuelle. Elle estime cependant qu'il est très important d'être informée et consultée largement car les projets de loi dans les domaines les plus divers ont souvent une influence sur les solutions que la Commission ou les Préposées préconisent dans d'autres dossiers; en outre, il est nécessaire que l'Autorité soit au courant de l'évolution législative générale dans le canton.

Dans un souci de transparence, la Commission **publie** une bonne partie de ses prises de position sur le site Internet¹¹.

1.2. Quelques exemples de prises de position

Reprise des nouvelles normes européennes relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

L'Autorité a été amenée à prendre position sur les projets de développement de l'acquis Schengen en Suisse. Le premier projet concerne le règlement sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et sur la libre circulation de ces données. Le second projet traite de la directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données. L'Autorité partage l'idée que la Suisse doit s'accorder avec les nouvelles normes européennes (directive et règlement), et garantir un niveau de protection suffisant pour un transfert de données personnelles de l'Union européenne vers la Suisse. D'une part, la Suisse doit reprendre la nouvelle directive pour éviter le risque de dissolution des accords d'association et, d'autre part, le secteur public ainsi que l'économie privée ont un intérêt à ce que la Commission établisse un niveau de protection adéquat des données à caractère personnel. La Commission est d'avis que le canton devrait adapter sa base légale formelle, c'est-à-dire réviser la Loi cantonale du 25 novembre

¹¹ <http://www.fr.ch/atprd/fr/pub/transparence/consultations.htm>

1994 sur la protection des données. Elle conseille également, dans l'intérêt d'une harmonisation entre les cantons, de proposer à la CdC de mettre sur pied des lignes directrices relatives à l'adaptation de la législation cantonale à la nouvelle directive.

Avant-projet de loi modifiant la loi sur l'aménagement du territoire et les constructions

Le projet de loi vise à adopter les bases légales nécessaires à l'introduction d'une nouvelle application pour la gestion électronique de la procédure de permis de construire. Selon l'application FRIAC, tous les dossiers de demandes de permis de construire devront être déposés puis traités de manière électronique et tous les acteurs de la procédure se verront obliger de l'utiliser. Sous l'angle de la protection des données, la Commission constate que le projet ne donne aucune indication concernant la gestion des données stockées. Dès lors, elle souligne l'importance de préciser dans la loi la manière dont les données seront gérées et stockées.

Avant-projet de loi modifiant la loi sur la gestion des déchets

L'avant-projet de loi modifiant la loi sur la gestion des déchets prévoit une sensibilisation de la population à la gestion des déchets et à la lutte contre les déchets sauvages. À ce titre, il prévoit des contraventions pour les personnes qui, intentionnellement ou par négligence, éliminent des déchets hors des installations prévues à cet effet. Sous l'angle de la protection des données, la Commission demande qu'il soit précisé que le nom du contrevenant ne doit pas être inscrit sur la quittance et indique que les informations liées à la personne concernée ne peuvent pas être conservées au-delà du paiement. De plus, la Commission est d'avis qu'il est nécessaire de rappeler au personnel chargé de prononcer les amendes d'ordre l'obligation de respecter le secret de fonction.

Avant-projet de loi et ordonnance sur la cyberadministration

En 2014, le Conseil d'Etat a approuvé la «Stratégie de cyberadministration de l'Etat de Fribourg» qui énumère les conditions-cadres légales de la cyberadministration et les prérequis juridiques à réaliser dans ce domaine. Ces exigences ont donc été concrétisées dans les avant-projets de loi et d'ordonnance y relatives. Consultée dans ce cadre lors de l'utilisation de l'identifiant, l'Autorité insiste sur la nécessité de séparer les activités privées des administrés de leurs activités professionnelles et sur l'exigence que ces derniers ne soient pas discriminés lorsque les procédures sont informatisées, ce d'autant plus que l'utilisation de la cyberadministration est facultative. En outre, elle relève que certains points doivent encore être clarifiés, notamment: la «journalisation» qui renvoie au Règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD), la modification du titre de la disposition relative à la conservation des données qui ne lui correspond pas, le rappel de la responsabilité des organes traitant des données personnelles, conformément à l'article 17 de la Loi du 25 novembre 1994 sur la protection des données (LPrD). En outre, l'Autorité salue l'effort de renoncer à l'utilisation du numéro AVS comme identificateur unique. Enfin, elle rappelle que la LPrD ne prévoit pas l'appariement ou l'interconnexion de données personnelles de différentes bases de données et que, le cas échéant, une législation spéciale devrait contenir des règles spécifiques.

Modification de la loi sur les bourses et les prêts d'études

Cette modification permettra au Service des subsides de formation (SSF) d'accéder, par une procédure d'appel, aux données du Service cantonal des contributions (SCC) relatives aux conditions de revenu et de fortune. En effet, ces données sont nécessaires au calcul du revenu déterminant du requérant et des personnes légalement tenues à son entretien. Sous l'angle de la protection des données, la Commission souligne combien il est important que l'accès aux données fiscales ne soit pas systématique; le SSF en fera usage uniquement dans le cas où la personne demandeuse est dans l'impossibilité de se procurer l'avis de taxation de ses parents.

Ordonnance du 14 décembre 2015 approuvant le règlement du personnel de la Haute Ecole spécialisée de Suisse occidentale//Fribourg

Dans sa réponse du 25 septembre 2012 à la consultation concernant la Loi sur la Haute Ecole spécialisée de Suisse occidentale//Fribourg (HESSO/FR), la Commission avait informé la Direction de l'économie et de l'emploi de l'importance d'être consultée dans le cadre de l'établissement du Règlement d'école. Or, elle a été surprise de constater que ce règlement était entré en vigueur sans qu'elle ait été consultée. Elle le regrette car il est très important que l'Autorité de la transparence et de la protection des données apporte son regard avant l'adoption des projets. En outre, le respect des principes de la protection des données ne peut se faire de manière efficace que si le législateur intègre ces principes dès le début des travaux législatifs. Toutefois, aucune remarque sur le contenu de ce règlement n'a été relevée.

Introduction du numéro AVS dans l'ordonnance modifiant le règlement sur la détention des chiens

L'introduction du numéro AVS dans la banque de données AMICUS recensant les chiens et leurs détenteurs est prévue dans l'ordonnance modifiant le règlement sur la détention des chiens. Or l'Autorité n'a pas été consultée à ce sujet, et la question de la légitimité de l'insertion du numéro AVS mérite d'être analysée. Selon la Loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS), l'utilisation du numéro AVS est normalement réservée aux institutions dont le but est lié aux assurances sociales. D'autres services et institutions peuvent l'utiliser à condition qu'une loi cantonale le prévoie. Étant donné qu'aucune loi cantonale ne le prévoit, la Commission conclut que l'introduction du numéro AVS dans la banque de données AMICUS n'est pas nécessaire, même si celle-ci est régie par un acte législatif au sens formel. Partant, elle a demandé au Conseil d'Etat une modification du Règlement sur la détention des chiens, et celui-ci y a donné suite.

Brochure «Politique de Sécurité de l'Information de l'Etat de Fribourg»

Le Service de l'informatique et des télécommunications de l'Etat de Fribourg (SITel) s'est adressé à notre Commission concernant la brochure «Politique de Sécurité de l'Information de l'Etat de Fribourg», brochure qui détaille le champ d'application, les objectifs, les responsabilités et les principes généraux de sécurité de l'information de l'Etat de Fribourg. La Commission est d'avis notamment d'introduire la mention de la protection des données en plus de la protection des informations, mais aussi de rappeler que l'organe public est responsable de ses données ainsi que de leur sécurité. Enfin, concernant les attributions de l'Autorité, la Commission propose de mentionner les compétences d'examen et de préavis des requêtes et d'émission des recommandations, la Loi du 25 novembre 1994 sur la protection des données étant réservée.

Directive de conduite des audits des systèmes d'information

La Commission constate que le point de la directive traitant des attributions de l'Autorité doit être supprimé. En effet, elle n'est pas soumise à cette directive dans la mesure où l'Autorité est indépendante. Ses attributions, telles que gestion autonome de ses audits, sont régies par la LPrD, en particulier son article 31 al. 2 let. a. Concernant la distribution des rapports d'audit, il est rappelé que ces rapports sont des documents officiels dont l'accès est réglé par les articles 20ss de la LInf. De plus, la Commission relève que, selon l'art. 4 let. a de l'Ordonnance du 3 novembre 2015 sur la gestion de l'informatique et des télécommunications dans l'administration cantonale (OGITAC), la compétence d'édicter des directives appartient à la Direction des finances et non au SITel.

2. Autres activités

La Commission, respectivement l'un ou l'autre de ses membres à titre individuel ou son Président, a eu en outre de nombreuses autres activités ponctuelles. Les exemples suivants peuvent être cités: la question de la collecte, la communication et la conservation de données personnelles sensibles par les organes publics est régulièrement à l'ordre du jour des travaux de la Commission. De manière régulière, la Commission, respectivement l'un de ses membres ou le Président, discute et prend position sur certains dossiers gérés par les Préposées à la transparence et à la protection des données et qui soulèvent des questions de principe (par ex. dans le cas des recommandations rédigées par la Préposée à la transparence, du suivi d'un contrôle dans le domaine de la protection des données ou encore de transmissions de communications systématiques des données par les autorités cantonales).

B. Transparence

1. Evaluation du droit d'accès

Selon les chiffres communiqués à l'Autorité, 39 demandes d'accès ont été déposées auprès des organes publics fribourgeois en 2016. Dans 26 cas, les organes publics ont accordé un accès complet et dans 3 cas un accès restreint. Dans 1 cas, l'accès a été différé. Dans 7 cas, l'accès aux documents a été refusé. Dans 2 cas, la demande d'accès a été retirée. Les domaines les plus concernés étaient les domaines des constructions, de l'administration, de l'agriculture et de l'environnement.

L'évaluation reflète le nombre de demandes d'accès annoncées par les organes publics auprès de l'Autorité. Comme au niveau fédéral, l'Autorité cantonale part de l'idée qu'en réalité ce nombre est nettement inférieur à la réalité, mais que les demandes d'accès adressées aux organes publics ne sont pas toujours reconnues comme telles et, en conséquence, pas traitées sous l'aspect de la LInf ni annoncées dans le cadre de l'évaluation. Une sensibilisation constante des organes publics semble dès lors très importante.

Le temps consacré au droit d'accès en général, et partant les coûts de la mise en œuvre du droit d'accès aux documents, varie sensiblement. Certains organes publics ont annoncé moins d'une heure consacrée au droit d'accès en 2016 tandis que d'autres ont investi jusqu'à 10 heures.

C. Protection des données

1. Décisions et recours (art. 30a al. 1 let. c, 22a, 27 LPrD)

Une tâche légale de la Commission concerne la mise en œuvre de la procédure prévue à l'art. 22a en cas de violation ou de risque de violation des prescriptions sur la protection des données. Elle consiste à inviter l'autorité compétente à prendre les mesures nécessaires et, le cas échéant, à interjeter recours auprès du Tribunal cantonal contre une décision de rejet de la part d'un organe public. Durant l'année 2016, la Commission a reçu une copie de 12 décisions dont 11 de la Police cantonale (principalement des demandes d'effacement de données et d'accès) et 1 du TC, relatives essentiellement aux demandes citées ci-dessus. La Commission n'a pas interjeté de recours parce que les décisions lui ont paru conformes à la législation en vigueur. L'Autorité salue notamment la Police cantonale qui lui transmet régulièrement ses décisions.

Durant l'année, la Commission a fait trois recommandations. L'une d'elle était destinée à une corporation ecclésiastique cantonale, dans la perspective de la création de sa plateforme informatique comprenant ses données. Elle portait en particulier sur les catégories des données personnelles que l'Etat doit fournir pour ce pool de données, l'utilisation du NAVS13, les réglementations et les exigences en matière de sécurité des données. Les démarches et entretiens entre les responsables de projet et les services impliqués sont en cours pour une réalisation conforme à la protection des données.

Deux autres recommandations concernaient la plateforme informatique destinée aux données des registres des habitants (voir également ci-dessous III.B.1.3). Ces recommandations étaient adressées à la Direction de la sécurité et de la justice (DSJ), laquelle décide en tant qu'autorité responsable des demandes d'accès. Dans le premier cas, la Commission a recommandé à la DSJ de refuser la demande des tribunaux d'arrondissement concernant l'accès étendu aux données personnelles des habitants de tout le canton, et de limiter cet accès aux données des habitants de l'arrondissement relevant de la compétence du tribunal; cette procédure est en cours. Dans le deuxième cas, la DSJ a accordé aux communes l'accès à toutes les données de la plateforme informatique en ce qui concerne tous les habitants du canton, accès qui autorise aussi d'établir des listes et de suivre la chronologie des diverses mutations. Ceci aurait permis par exemple de suivre sur des années les déménagements de particuliers ou les modifications de l'état civil, et ce sans preuve d'un intérêt spécial. Simultanément, la Commission a déposé un recours contre cette décision de la DSJ auprès du Tribunal cantonal, afin d'éviter une éventuelle perte des voies de droit. Dans sa nouvelle décision, la DSJ n'a certes pas appliqué toutes les recommandations de la Commission, mais a cependant limité l'accès à des données sélectionnées et a refusé aux communes l'accès à l'historique des données ainsi qu'à la possibilité d'établir des listes.

Dans la procédure d'autorisation d'accès aux données de la plateforme informatique et de la formulation subséquente d'une recommandation, la lourdeur de la procédure a été mise en évidence du fait que la prise de position de l'autorité exprimée dans le cadre de cette procédure n'a en soi pas de valeur de recommandation.

III. Activités principales des Préposées

A. Transparence

1. Points forts

1.1. Médiations

En 2016, sept demandes en médiation ont été adressées à la Préposée à la transparence. Quatre cas ont débouché sur un accord de médiation, et la Préposée a émis une recommandation dans un cas.

La **première demande en médiation** portait sur l'accès à une **décision de la Commission des mesures administratives en matière de circulation routière (CMA)** suite à un accident de la circulation impliquant un policier, ce que la presse avait relevé. Consulté par la CMA, le policier s'y est opposé. Dans sa détermination, la CMA a donc proposé de ne divulguer que le dispositif anonymisé de la décision. Ce n'était pas suffisant pour le requérant, qui a déposé une demande en médiation. Lors de la séance subséquente, le requérant et le représentant de la CMA ont convenu de remettre un résumé de la décision pour autant que le tiers concerné y consente. Consulté par la Préposée à la transparence, le policier ne s'est pas opposé à la solution de compromis. Le résumé a pu être remis au requérant.

Dans le **deuxième** cas, il s'agissait de l'accès aux **paiements par la Bibliothèque cantonale et universitaire (BCU) à différentes maisons d'édition**. La BCU avait globalement refusé une demande d'accès correspondante au motif que la plupart des contrats d'abonnement et accords de licence comportaient des clauses de confidentialité et qu'elle voulait les respecter. Elle a en outre fait valoir qu'il y aurait divulgation de secrets d'affaires et qu'un tel accès pouvait compromettre son pouvoir de négociation. Selon elle, le requérant pouvait obtenir les chiffres souhaités en l'absence de clauses de confidentialité. La Préposée à la transparence a estimé qu'il n'est pas possible d'invoquer lesdites dérogations prévues par la LInf dans le cas présent et, dans sa recommandation¹², elle s'est donc prononcée en faveur de l'accès aux paiements. En dépit de la recommandation, la BCU a maintenu sa position. Le requérant a alors déposé un recours auprès de la Direction de l'instruction publique, de la culture et du sport. Celle-ci a approuvé le recours et ordonné à la BCU de communiquer les paiements souhaités au recourant.

La **troisième et la quatrième demande en médiation** portaient sur un **rapport qui contenait des mesures du vent** pour un projet éolien. Des opposants à l'énergie éolienne demandaient à la commune Le Flon l'accès au rapport remis par l'entreprise énergétique en charge du projet. Comme la commune n'a pas répondu dans les délais prévus par la LInf, le requérant a déposé une demande en médiation. Avant que la séance de médiation puisse avoir lieu, le directeur de l'entreprise énergétique a soustrait le document au dossier de la commune. Les opposants ont alors déposé directement une seconde demande d'accès auprès de l'entreprise énergétique, qui relève du champ d'application de la Convention d'Aarhus et, partant, qui est aussi soumise au droit d'accès. Elle non plus n'a pas répondu dans les délais impartis, ce qui a donné lieu à une seconde demande en médiation. La Préposée à la transparence a joint les deux médiations pour des raisons d'économie de procédure, car il s'agissait du même document et des mêmes parties. Lors de la séance de médiation, les trois parties se sont entendues pour que le directeur de l'entreprise présente le contenu du document recherché lors d'une séance d'information invitant les membres de l'association, des spécialistes et les membres du conseil communal.

¹² <http://www.fr.ch/atprd/fr/pub/transparence/publications/recommandations.htm>

Dans le cinquième cas, il s'agissait de l'accès au **plan d'aménagement local du quartier du Schönberg en Ville de Fribourg**, tel qu'il avait été soumis fin 2014 aux services cantonaux compétents pour examen préalable. Suite à la détermination négative de la Ville de Fribourg, l'association de quartier intéressée a déposé une demande en médiation. Lors de la séance subséquente, les parties ont convenu de repousser l'accès aux documents souhaités et aux préavis des services cantonaux, qui n'étaient pas encore rendus à ce moment-là, jusqu'aux séances d'information organisées dans le cadre de la mise à l'enquête publique du plan d'aménagement local.

Une autre demande en médiation a été déposée par un citoyen qui contestait la réponse de la Direction de l'instruction publique, de la culture et du sport à une **demande de renseignements** à la suite d'une demande d'accès. La Préposée à la transparence a signalé au citoyen que la LInf ne prévoit aucune possibilité de médiation pour les demandes de renseignements. Cette possibilité n'existe que pour les demandes d'accès à des documents officiels. Dans le cas présent, le citoyen avait déjà obtenu les documents souhaités. Par conséquent, la Préposée à la transparence n'a pas pu entrer en matière sur la demande en médiation.

Le septième cas portait sur divers documents concernant la **gestion** de la corporation de droit public du **Caravaning** de Gletterens, documents auxquels une propriétaire de plusieurs parcelles avait demandé l'accès. Aucune prise de position n'ayant fait suite à l'accusé de réception, la propriétaire a déposé une demande en médiation. Ce cas était encore pendant fin de l'année 2016.

1.2 Demandes

Comme les années précédentes, des organes publics ont aussi régulièrement contacté la Préposée à la transparence en 2016 lorsqu'ils étaient confrontés à une demande d'accès. Des **tiers** étaient souvent impliqués et les organes publics voulaient se renseigner sur la procédure à suivre. Une demande d'accès à des plans de liquidités de remontées mécaniques a été déposée dans une commune, qui en disposait en vertu de sa participation. Dans une autre commune, il s'agissait de l'accès aux postes budgétaires qui détaillaient les rémunérations des employés communaux et du conseil communal. Et dans un autre cas, le requérant cherchait à consulter la décision du conseil communal relative à la composition d'une commission.

La Préposée à la transparence a signalé aux différents organes publics qu'en général, en cas de demande d'accès, il est nécessaire de prendre contact avec le tiers concerné et de lui demander son avis (art. 32 al. 2 LInf). Si le tiers donne son accord et que l'organe public compétent ne s'exprime pas contre la publication du document, l'accès doit être accordé. Si le tiers s'y oppose, l'organe public doit analyser le cas afin de déterminer s'il refuse l'accès ou s'il souhaite l'autoriser au motif que selon lui l'intérêt public prime. Dans ce dernier cas, le tiers doit être informé de la volonté de l'organe public d'accorder l'accès et a la possibilité de déposer une requête en médiation auprès de la Préposée à la transparence (art. 32 al. 3 et art. 33 al. 1 LInf).

La situation est un peu différente pour une demande d'accès à un procès-verbal du conseil communal comportant des données personnelles. D'après la LInf, les procès-verbaux des séances non publiques ne sont pas accessibles (art. 29 al. 1 let. b LInf). La loi sur les communes prévoit toutefois, à l'art. 103^{bis} al. 2 let. a, que le conseil communal peut autoriser, par une décision prise à l'unanimité, la consultation de tout ou partie des procès-verbaux de ses séances, des séances des commissions de l'assemblée communale et des séances de ses commissions administratives. Le cas échéant, les éventuelles données personnelles de tiers doivent être caviardées.

Comme en l'espèce il s'agissait de la composition d'une commission, la Préposée à la transparence a fait remarquer qu'on pouvait supposer que de toute manière les noms des membres de la commission étaient connus ou révélés. L'extrait du procès-verbal pouvant encore comporter d'autres éléments afférents aux exceptions prévues par la LInf, il est nécessaire au besoin de le vérifier et de caviarder les passages correspondants.

Par ailleurs, la Préposée à la transparence a été contactée à plusieurs reprises par les médias qui s'informaient de la **conformité de certaines pratiques avec la LInf**. Par exemple, une journaliste voulait savoir si une entreprise pouvait bel et bien exiger une somme à cinq chiffres pour qu'un groupement d'intérêts puisse consulter un document. L'entreprise avait mentionné cette somme sur demande, au motif qu'elle correspondait à la moitié des coûts de revient du rapport concerné. La Préposée à la transparence a signalé que la LInf ne s'appliquait pas dans le cas présent et a conseillé de se référer à la Convention d'Aarhus, car l'entreprise concernée entrait dans son champ d'application. Elle a en outre souligné que des émoluments ne peuvent être exclus pour certaines demandes d'accès, mais qu'ils n'étaient certainement pas justifiés dans une telle ampleur et pour lesdites raisons.

En 2016, la Préposée à la transparence a aussi rappelé régulièrement les limites de sa fonction dans les cas d'espèce qui lui ont été soumis. Elle peut fournir des **renseignements généraux** sur le domaine de la transparence, mais pas d'avis circonstancié au sujet d'un cas concret. La formulation d'une recommandation est réservée à une éventuelle phase de médiation, au sens de l'art. 33 LInf. En conséquence, la Préposée doit rester neutre lors de cette étape.

1.3. Adaptation de la LInf à la Convention d'Aarhus

Les travaux en vue de l'adaptation de la LInf à la Convention du 25 juin 1998 sur l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice en matière d'environnement (Convention d'Aarhus) ont pu se terminer en 2016 comme prévu. Dans sa session d'octobre, le Grand Conseil a consenti à une adaptation de la LInf aussi transversale que possible. Par contre, il n'a pas voulu aller aussi loin que le projet initial du Conseil d'Etat s'agissant des particuliers sans compétence décisionnelle qui accomplissent des tâches de droit public en dehors du domaine de l'environnement.

Dans certains domaines, la LInf n'a donc pas seulement été adaptée en matière d'environnement, mais dans sa globalité. Cela permet au canton de Fribourg de se rapprocher des autres cantons en la matière. Par exemple, la limitation dans le temps qui s'appliquait jusqu'ici aux demandes d'accès a été supprimée. Il est dès lors possible de faire valoir le droit d'accès pour des documents antérieurs à 2011.

Dans le domaine de l'environnement, les règles spéciales qui s'appliquent au droit d'accès vont plus loin que celles que prévoit la LInf de manière générale. Ces règles visent à ancrer davantage encore le principe de la transparence, s'agissant des activités exercées par des collectivités publiques ou par des personnes de droit privé qui leur sont proches et qui ont une influence directe sur l'état de l'environnement.

Les exceptions prévues dans la LInf et dans la législation spéciale en matière de droit d'accès doivent être interprétées dans l'esprit de la Convention d'Aarhus. Le principe de l'interprétation conforme signifie qu'en cas de demande d'accès se rapportant à une information sur l'environnement, les dispositions de la LInf doivent être interprétées et appliquées dans un sens qui respecte l'esprit et les objectifs poursuivis par la Convention d'Aarhus.

2. Statistiques

Durant la période considérée, 112 dossiers ont été introduits, dont 14 sont pendants au 1^{er} janvier 2017. 30 conseils et renseignements, 10 avis, 30 examens de dispositions législatives, 16 présentations, 12 participations à des séances et autres manifestations, 7 demandes en médiation et 7 demandes diverses. 56 dossiers concernent des organes cantonaux ou des institutions chargées de tâches publiques, 11 des communes et paroisses, 30 d'autres organismes publics (cantons, autorités de transparence et protection des données), 13 des particuliers ou institutions privées et 2 des médias (cf. statistiques annexées).

B. Protection des données

—

1. Points forts

1.1. Demandes

Des Directions, communes et organes d'institutions privées chargées de tâches de droit public aussi bien que des particuliers s'adressent à l'Autorité pour connaître son avis sur différents thèmes. La procédure de réponse reste informelle. Dans la mesure du possible, la Préposée sollicite des renseignements auprès des organes ou services demandeurs ou impliqués. La collaboration avec les Directions et les divers services est bonne dans la plupart des cas.

Dans le cadre de contrôles préalables de projets de traitement de données, les dossiers portaient notamment sur des projets élaborés dans le contexte de la mise en œuvre du guichet de cyberadministration, du portail scolaire «Primeo», de l'initiative sur les résidences secondaires, du dossier électronique de santé des détenus ou sur des projets communaux de traitement des données. Diverses demandes avaient pour objet la plateforme informatique cantonale contenant les données des registres des habitants FRI-PERS (cf. également 1.3).

Durant 2016, le projet informatique d'une corporation ecclésiastique cantonale pour la gestion d'un registre électronique (des membres, des électeurs et des contribuables ainsi qu'un registre pastoral) fut à nouveau un sujet important. Le projet se révèle être délicat dans la mesure où il prévoit la divulgation systématique de données personnelles provenant de la plateforme du registre des habitants ainsi que de données fiscales; par conséquent, des données sensibles sont également concernées. En sa qualité de responsable des données personnelles, l'Etat doit veiller à garantir le fait que les données ne soient utilisées qu'aux fins prévues. Règlements, documents et descriptifs de projets devaient donc faire l'objet d'un examen critique dans l'optique du traitement des données projeté, en particulier quelles données personnelles doivent être utilisées. Comme pour tout traitement de données effectué par des organes étatiques, il y a lieu d'observer les principes de la légalité, de l'utilisation conforme et de la proportionnalité. La Commission a traité plusieurs dossiers dans ses séances. A ce sujet, la Préposée à la protection des données ainsi que certains membres de la Commission ont pris part à plusieurs réunions (voir également ci-devant II.C).

Voici plusieurs exemples de réponses et de prises de position de la Préposée à la protection des données:

Communication de données par un service à un autre

Transmission de l'avis de taxation de l'ECAB au Service cantonal des contributions

Un administré a consulté l'Autorité afin de savoir si le Service cantonal des contributions (SCC) est en droit de requérir la communication de la valeur d'un bien immobilier, telle qu'estimée par l'ECAB, en vue de procéder à sa taxation. En matière de droit fiscal, il existe une réglementation spéciale qui l'emporte sur les dispositions de la protection des données, dont l'application conserve uniquement un caractère subsidiaire. Selon la loi, l'autorité fiscale est autorisée à entreprendre les vérifications qu'elle estime nécessaire pour vérifier le caractère complet et exact des éléments figurant dans la déclaration fiscale du contribuable (art. 157 al. 2 de la Loi sur les impôts cantonaux directs; LICD). Elle peut également demander des renseignements supplémentaires si nécessaire (art. 159 al. 2 LICD). En l'espèce, le SCC demande à pouvoir consulter l'estimation faite par l'ECAB d'un bien immobilier, soit la valeur à laquelle celui-ci est assuré. L'Autorité constate qu'il s'agit là d'une pratique habituelle dans la plupart des cantons en Suisse et qui est admissible du point de vue de la protection des données.

Statistiques des votes et résultats électoraux

La Préposée à la protection des données a été consultée au sujet de l'utilisation des données du scrutin électoral à des fins de statistique. Des motionnaires ont demandé l'adaptation de la Loi du 6 avril 2001 sur l'exercice des droits politiques (LEDP) « de manière à permettre que des statistiques en lien avec la participation aux scrutins et aux résultats électoraux soient possibles, en respectant la protection des données ». Le lien entre la participation et le choix de vote d'une personne identifiable est délicat car le secret des urnes et la sphère privée des citoyens doivent être garantis. La législation actuelle ne permet pas de faire un tel appariement. Toutefois et à des fins de statistique, elle permet la collecte de données ne se rapportant pas à des personnes. Cependant, des restrictions à la communication de ces données sont réservées, notamment si une obligation de garder le secret l'exige. En l'espèce, le secret des urnes existe. Par conséquent, il est nécessaire que les données soient anonymisées, de manière à ce qu'aucune identification ne soit possible par la suite. La législation actuelle ne permet donc pas d'établir les statistiques envisagées.

Voir aussi «Protection des données et assurances sociales» (p. 23).

Communication de données personnelles par les communes

Elections

Durant la période électorale, l'Autorité a été contactée par des communes souhaitant savoir si elles étaient en droit de transmettre les adresses de leurs citoyens aux partis politiques. Sauf si les données sont utilisées à des fins idéales dignes d'être soutenues, à savoir non commerciales, il n'est pas admissible que les communes transmettent ces données aux partis. Durant cette même période électorale, un citoyen a demandé si la Chancellerie d'Etat n'était pas dans l'obligation de communiquer la date de naissance complète (jour, mois, année) des candidats aux élections. En effet, dans le cadre de l'astrologie, cette donnée pourrait être utile pour élire les futurs candidats. L'Autorité a alors informé le requérant que ce n'est pas une tâche de la Chancellerie de communiquer cette donnée.

Communication du détail de certains comptes à la commission financière

Une commune a abordé l'Autorité afin de savoir si sa commission financière était bien autorisée à connaître le montant des salaires alloués par personne à son personnel administratif et d'exploitation ainsi que les taux d'activité occupés, respectivement le nombre d'EPT engagés. Dans la mesure où la structure de cette dernière est relativement modeste, la communication par fonction anonymisée permettrait de facto d'identifier les personnes concernées. Dans le cadre d'une communication systématique, il faut impérativement qu'une base légale la prévoit. Or, l'Autorité a constaté que le droit d'accès aux renseignements de la commission financière est sensiblement restreint, en vertu de l'art. 97^{bis} de la loi du 25 septembre 1980 sur les communes (LCo). En effet, il est prévu que celle-ci ne reçoive que les documents nécessaires à l'exercice de ses attributions, c'est-à-dire à l'examen du budget, la prise de position sur le plan financier ainsi que ses mises à jour. Les bases légales étant formulées de manière vague, l'Autorité est d'avis qu'on ne peut raisonnablement admettre qu'elles constituent des bases suffisantes pour permettre l'accès aux informations relatives au salaire du personnel. Une réserve pourrait être formulée dans un cas exceptionnel de soupçon, d'abus ou de nécessité de faire des économies importantes. Cependant, il devrait s'agir d'un cas concret, formulé par écrit et dûment motivé, respectant ainsi les exigences du principe de proportionnalité.

«Commission d'impôt» d'une commune et consultation des déclarations fiscales

Un citoyen a abordé l'Autorité afin de savoir si une commune a le droit de constituer sa propre «commission d'impôt», formée de citoyens chargés de reprendre les déclarations d'impôts et leurs annexes ou l'avis de taxation dans le but d'effectuer des contrôles et des pointages «locaux» qui permettraient de trouver des fraudeurs.

De la législation en vigueur, il ressort que le conseil communal a la compétence de nommer les membres de la commission d'impôt. Toutefois, ces derniers doivent avoir l'exercice des droits civils. Cependant, depuis l'entrée en vigueur de la Loi du 6 juin 2000 sur les impôts cantonaux directs (LICD), les contribuables doivent retourner leur déclaration d'impôt directement au Service cantonal des contributions (SCC) et non plus au bureau communal. Toutefois, la commune a toujours la possibilité d'émettre un préavis sur les dossiers qu'elle souhaite consulter, compétence pouvant être déléguée à une commission d'impôt. Il apparaît clairement que cette commission n'a pas les mêmes compétences que la commune puisque ses compétences sont limitées au préavis communal uniquement. De plus, conformément au principe de proportionnalité, le conseil communal ou la commission d'impôt ne peut pas consulter la déclaration fiscale de tous les citoyens de la commune, car la consultation d'une déclaration fiscale doit être requise en cas de motif valable, dans un cas déterminé, et non de manière générale et automatique. De plus, l'Autorité estime que la recherche des fraudeurs est une tâche dévolue au SCC, et ne peut donc pas être déléguée à la commission d'impôt. La question du bienfondé de maintenir cette commission se pose, puisque les déclarations ne sont plus envoyées directement à la commune. En outre, il est mentionné que les communes ont accès à l'avis de taxation des citoyens de leur commune uniquement. En effet, les communes étant également des autorités fiscales, elles peuvent demander à pouvoir consulter la déclaration fiscale et ses annexes dans un cas particulier.

Transmission des dossiers de naturalisation aux membres de la commission communale

Dans le cadre des procédures de naturalisation, une commune s'est adressée à l'Autorité afin de connaître la manière la plus appropriée de communiquer aux membres de la commission de naturalisation les dossiers des candidats, dossiers qui contiennent de nombreuses données personnelles et sensibles.

Selon la jurisprudence, il est non seulement licite de collecter des données détaillées sur les candidats, mais encore indispensable de procéder à une telle collecte pour mener à bien ces procédures. Etant donné le large éventail des données collectées, leur traitement représente une sérieuse atteinte au droit à l'autodétermination en matière d'information qui n'est justifiée que par l'existence d'une base légale spécifique et par le fait que le candidat à la naturalisation consent par sa demande à un tel traitement de ses données. Conformément aux principes de bonne foi et de finalité, le candidat qui consent à ce qu'un groupe de personnes définies et autorisées prennent connaissance de ses données personnelles ne s'attend pas à ce que celles-ci puissent être consultées par des tiers. Ainsi, il est en droit d'exiger que ses données privées ne soient pas communiquées à des personnes non autorisées. C'est pourquoi les autorités compétentes sont tenues de prendre toutes les mesures organisationnelles et sécuritaires nécessaires afin de prévenir tout risque de divulgation de données. Ce devoir est encore renforcé dans la commission de naturalisation par le fait que ses membres ont été assermentés et sont soumis au secret de fonction.

En l'espèce, la requérante a définitivement abandonné l'envoi des documents concernés par voie électronique sur l'adresse mail privée des membres de la commission préférant ainsi, pour des raisons essentiellement pratiques, la remise des dossiers en mains propres et contre signature avec obligation de restitution une fois la procédure terminée et de destruction des dossiers.

L'Autorité est d'avis que la solution choisie est déjà appropriée, toutefois elle relève que la consultation des dossiers à l'administration communale et la mise à disposition des dossiers sur un espace informatique protégé permettent une meilleure protection de la personnalité des personnes concernées. En effet, il convient d'éviter que des données sensibles soient conservées au domicile privé des membres de la commission. Le cas échéant, ces derniers doivent prendre les mesures adéquates afin de garantir la confidentialité des dossiers de naturalisation, à savoir de les conserver dans un lieu inaccessible aux tiers. Les documents contenus dans les dossiers doivent obligatoirement être déposés dans un porte-document qui ne laisse pas apercevoir son contenu. La solution adoptée étant provisoire et devant être remplacée par l'utilisation d'un espace informatique protégé, l'Autorité émet certaines recommandations à la plateforme informatique, telles que la mise en place d'un code d'accès et d'un accès sécurisé par VPN, le contrôle des droits d'accès, la destruction des dossiers à la fin de la procédure, l'interdiction d'imprimer les documents chez soi, la consultation dans un lieu sûr, le changement de code d'accès plusieurs fois par année et, en cas de gestion externe de la plateforme, une clause de confidentialité signée avec l'entreprise.

Voir aussi «Protection des données et école» (p. 25).

Protection des données et travail

Transmission et utilisation des numéros de téléphone privés dans le cadre du travail

Un service a contacté l'Autorité afin de savoir si l'employeur est autorisé à demander à ses employés leur numéro de téléphone privé pour un usage professionnel. Un des principes de la gestion des ressources humaines est le respect de l'intégrité de l'employé. Il ressort du Code des obligations, applicable par analogie, que, dans les rapports de travail, l'employeur doit protéger et respecter la personnalité de l'employé. Il a également le devoir d'empêcher que des tiers ne portent atteinte à sa personnalité. Ainsi, l'employeur ne peut traiter des données concernant ses employés qu'avant la conclusion du contrat et pendant son exécution pour des questions visant à déterminer si les candidats sont aptes à occuper le poste en question, et pendant la durée de l'engagement pour les données relatives à l'employé et qui sont nécessaires à l'exécution du contrat de travail. De l'avis de l'Autorité, le numéro de téléphone privé d'un employé fait partie des données qui sont nécessaires à l'exécution

du contrat de travail. Même si cela doit rester l'exception, il peut se présenter dans toutes activités des situations particulières qui requièrent de la part de l'employeur la possibilité de joindre ses employés durant leur temps de repos, par exemple pour remplacer un collègue ou dans des situations d'urgence. La collecte du numéro de téléphone privé par l'employeur n'est donc pas une atteinte illicite aux droits de la personnalité de l'employé. Néanmoins et pour garantir les droits de la personnalité de ses employés, il est nécessaire que l'employeur prenne des mesures d'organisation et des mesures techniques appropriées contre tout traitement non autorisé des données, portant notamment sur la conservation, l'accès et la communication des données personnelles. Ainsi, les numéros de téléphone privés doivent être conservés en lieu sécurisé et ne peuvent pas être communiqués à des tiers sans le consentement des personnes concernées.

Protection des données et assurances sociales

Communication à la commune de domicile d'un patient ne disposant pas de couverture LAMal

Un prestataire de soins a approché l'Autorité afin de savoir s'il est licite que son département des finances prenne contact avec la commune de domicile d'un patient ne disposant pas d'une couverture LAMal dans le but de procéder à son affiliation en vue de la prise en charge des frais médicaux. En effet, toute personne qui réside en Suisse doit être affiliée auprès d'un assureur-maladie de base de son choix. C'est aux cantons qu'il incombe de veiller au respect de cette obligation et, s'il y a lieu, de procéder à une affiliation d'office d'une personne.

Dans le canton de Fribourg, le contrôle incombe à la commune du domicile de la personne concernée.

L'Autorité est d'avis que la communication envisagée est conforme à la protection des données, dans la mesure où l'information est nécessaire à la commune pour accomplir ses obligations. De plus, il existe un intérêt public de la collectivité de bénéficier d'une assurance obligatoire et universelle et un intérêt privé de la personne concernée d'être au bénéfice d'une assurance qui prendra en charge ses frais médicaux. Toutefois, le prestataire de soins doit se contenter d'indiquer à la commune que la personne concernée ne dispose pas d'une couverture LAMal et de lui demander de procéder à une affiliation d'office. En aucun cas, il n'est en droit de communiquer d'autres renseignements sur le patient qui permettraient de tirer des conclusions même indirectes à son sujet (ex: éléments se rapportant à la facturation des prestations fournies, à la durée de traitement ou encore à son contenu).

Lorsque la commune de domicile n'est pas connue, le prestataire de soins peut se renseigner auprès de plusieurs communes afin de savoir si la personne concernée y est domiciliée. L'Autorité ajoute qu'en cas de factures impayées par un patient, le prestataire de soins peut être amené à engager des poursuites. Etant donné que ce type de démarche implique nécessairement la divulgation d'informations sensibles, il ne peut pas y recourir à moins d'avoir été dûment délié du secret médical par la personne elle-même ou par la Direction de la santé et des affaires sociales sur préavis du médecin cantonal. Dans ce dernier cas, la Direction doit procéder à une pesée des intérêts entre la protection des données personnelles de la personne concernée et de la communication des données nécessaires au recouvrement de la créance du prestataire de soins. L'intérêt du prestataire de soins est souvent privilégié car il permet à l'hôpital de continuer à prodiguer des soins de qualité au plus grand nombre.

Utilisation du numéro AVS en tant qu'identificateur universel

Dans le cadre de l'interfaçage de deux applications, un service de l'Etat a contacté l'Autorité afin de savoir s'il est autorisé d'utiliser le numéro AVS en tant qu'identificateur de personnes. Un identificateur constitue une séquence de caractères qui, réunissant un nombre indéterminé de données personnelles se rapportant à un individu, permet au final d'obtenir une description plus ou moins précise de la personne concernée en fonction de la quantité et de la nature des données regroupées.

Plus l'échantillon de données rassemblées est vaste, plus la description de la personne devient précise. Autrement dit, un identificateur constitue une «super-donnée» qui permet l'accès à un ensemble varié de données personnelles formant entre elles un profil de la personnalité.

A l'origine désigné spécifiquement à l'utilisation dans le cadre des assurances sociales, le numéro AVS est devenu un identificateur quasi universel utilisé par un nombre indéterminé d'organisations et qui rassemble un nombre incalculable de données sur une personne désignée. Or, l'auto-détermination informationnelle est un droit constitutionnel, garantissant à toute personne d'être protégée contre l'emploi abusif des données qui la concernent. Au-delà de sa portée individuelle, ce droit est aussi une exigence d'un Etat démocratique et peut, comme tout droit fondamental, être restreint. L'usage du numéro AVS comme identificateur universel en dehors du domaine des assurances sociales présente des risques d'atteinte à la personnalité. Il provoque pour la personne concernée la perte de la maîtrise de ses données personnelles, si bien qu'elle se retrouve dans l'incapacité d'exercer ses droits (droit d'accès, droit à l'exactitude des données et droit de rectification des données erronées). L'utilisation de plus en plus répandue du numéro AVS ouvre la voie à toutes sortes d'abus et autres usages illicites en raison des différentes possibilités d'appariement (ex: chantage, usurpation d'identité, vol et revente de données, etc.). C'est pourquoi le législateur fédéral a fixé les conditions d'usage du numéro AVS en tant que numéro de sécurité sociale, ainsi que dans les autres domaines qui lui sont étrangers (cf. la Loi fédérale du 23 juin 2006 sur l'assurance-vieillesse et survivants; LAVS).

Toutefois, on relève que même lorsqu'il est prévu au moyen d'une base légale, l'utilisation du numéro AVS par les différentes administrations dans des domaines autres que celui des assurances sociales n'en demeure pas moins risquée. Selon le PFPDT, l'extension du champ d'application de ce numéro d'assuré pour en faire un numéro universel comporte des risques importants touchant la sphère privée des citoyens en raison des connexions indésirables par comparaison des différentes bases de données. Pour cette raison, il recommande la création d'identificateurs sectoriels spécifiques aux tâches qui présentent entre elles un lien matériel, plutôt que de recourir au numéro AVS dans des domaines qui ne lui sont en rien liés. En l'espèce, le législateur cantonal n'a adopté aucune base légale qui permettrait de recourir au numéro AVS pour procéder à l'interfaçage de deux applications. Dès lors, son utilisation est interdite par le droit fédéral.

Protection des données et religion

Voir sous II.C.1 (p. 14) et III.B. 1.1 (p. 19)

Protection des données et santé

Dossier de santé informatisé du détenu

Le projet d'informatiser le dossier de santé du détenu a pour objectif de permettre aux institutions de disposer en permanence d'un dossier de santé d'un détenu, complet et à jour, ainsi que de le partager et d'y accéder en tout temps à distance. La solution informatique choisie est un logiciel d'une entreprise externe qui héberge les données et qui offre un support 7j/7 et 24h/24. Une séance a été organisée entre le SITel et l'Autorité pour discuter du projet. Il ressort de la discussion que le niveau d'authentification est faible, surtout dans la mesure où des données médicales à savoir des données sensibles sont traitées, que la clé de cryptage est détenue par le mandataire alors qu'elle devrait l'être par le mandant,

qu'une formation du personnel de la prison à l'utilisation de ce logiciel devra être effectuée et que la question de la sécurité des données doit être vérifiée de sorte que le concept de sécurité y relatif soit transmis à l'Autorité. Concernant la société hébergeuse, cette dernière a déjà fait l'objet d'un audit qui est confidentiel. On y relève que le dossier médical et le dossier psychiatrique ne sont pas liés et que les factures des médecins externes sont directement adressées à la prison et ne contiennent pas d'information sur le dossier médical. S'agissant de la conservation du dossier médical informatisé du détenu, la question n'est pas encore réglée. Proposition est faite de le détruire à la mort du détenu. A la réception du concept de sécurité et du contrat, l'Autorité pourra analyser le projet plus en détail.

Protection des données et données fiscales

Etendue du devoir de collaboration du contribuable à l'égard du Service cantonal des contributions

Un privé a écrit à l'Autorité afin de savoir si le SCC est en droit d'exiger, dans le cadre d'une procédure de réclamation en cours, la production de la liste de ses clients relatifs à l'exercice fiscal écoulé afin de déterminer si l'activité accessoire de ce dernier doit être considérée sous l'angle fiscal comme une activité lucrative ou comme un hobby. En matière de droit fiscal, les règles dérogent à la Loi du 25 novembre 1994 sur la protection des données (LPrD), qui ne s'applique que de manière subsidiaire. Pour déterminer si une activité accessoire doit être considérée comme une activité lucrative indépendante ou un hobby, le SCC se base sur un faisceau d'indices. Dans ce cadre, il est autorisé à entreprendre les vérifications nécessaires sur le caractère complet et exact des éléments figurant dans la déclaration fiscale du contribuable et peut, le cas échéant, lui demander des renseignements supplémentaires, dans les limites du secret professionnel légalement protégé conformément à son devoir de collaborer.

Selon la jurisprudence fédérale, le contribuable doit remettre à l'autorité fiscale qui en fait la demande et conformément à son devoir de collaboration la liste des noms, prénoms et adresses de ses créanciers. Le pouvoir d'investigation de l'autorité fiscale est extrêmement large; elle doit pouvoir accéder à tous les écrits susceptibles de fournir des informations pertinentes pour la taxation. Toutefois, elle demeure soumise, dans l'exécution de ses tâches, au principe de proportionnalité. En l'espèce, l'Autorité considère que, si l'information requise n'est pas de nature à trancher à elle seule la question de l'activité accessoire indépendante ou du hobby, elle constitue toutefois certainement un des éléments du faisceau d'indices sur la base duquel le litige doit être résolu. Cette information permet en effet de savoir si la clientèle constituée se compose d'un cercle restreint de proches ou si elle s'étend à un nombre indéterminé de consommateurs. En outre, les données personnelles échangées dans le cadre de la procédure de taxation sont soumises au secret fiscal, lequel offre une protection plus étendue que celle du secret de fonction. La demande formulée par le SCC ne viole donc pas la législation sur la protection des données.

Voir également sous «communication de données par un service à un autre», p. 20.

Protection des données et école

Traitement des données des personnes en formation se trouvant en difficultés

Au sein d'une école professionnelle, les données personnelles relatives à des personnes en formation qui se trouvent en difficultés doivent être traitées en préservant le plus possible les droits de la personnalité des personnes concernées, ce d'autant plus que certaines de ces données sont sensibles au sens de l'art. 3 let. c LPrD. Dans le cas où la réussite de la formation d'une personne paraît compromise, les prestataires de la formation peuvent s'échanger les informations nécessaires après avoir consulté la personne concernée et, le cas échéant, son représentant légal. Tout échange d'informations doit

cependant respecter plusieurs règles, à savoir limiter l'échange aux informations qui ont un lien avec la formation (ex: prestations insuffisantes, comportement inadapté ou absentéisme exagéré et non fondé) et aux éléments extérieurs à la formation mais qui sont susceptibles d'avoir un impact sur celle-ci (ex: contexte familial difficile ou addiction à l'alcool ou aux drogues, automutilation, tentatives de suicide). Cependant, si ces informations sont sensibles, le traitement de ces dernières nécessite de prendre toutes les précautions afin de protéger les droits de la personnalité de l'intéressée. Ensuite, il faut définir le cercle des personnes autorisées à recevoir et à communiquer des données sur la personne concernée. Outre la personne concernée, ce cercle inclut le maître d'apprentissage, le personnel enseignant directement en contact avec elle, ainsi que, éventuellement, le médiateur scolaire. Les représentants légaux peuvent aussi être inclus sauf si la personne concernée s'y oppose. La question de l'intégration des parents est analysée au cas par cas. Enfin, avant toute communication, la personne concernée doit être consultée et associée au processus d'échange d'informations. Sa détermination vaut préavis. Même si elle n'est pas majeure, la personne concernée a droit à l'autodétermination informationnelle. En cas de refus de sa part de communiquer ses données à des tiers, y compris ses parents, sa décision doit être respectée.

Enfin, le cas d'une communication justifiée par la sauvegarde d'intérêts privés ou publics prépondérants est réservé, par exemple dans une situation où l'intégrité physique ou psychique de l'intéressée est mise en danger. Dans ce contexte, une communication est nécessaire, même si elle ne satisfait pas aux conditions précitées. Dans chaque cas traitant de données sensibles, il convient de procéder à une pesée des intérêts en présence entre la divulgation de l'information concernée et le maintien du secret.

Publication d'une liste d'élèves dans le bulletin communal

La Préposée à la protection des données a été abordée dans le cadre de la publication d'une liste d'élèves dans le bulletin communal. Publier une telle liste dans le bulletin communal constitue une communication systématique qui nécessite une base légale n'existant pas dans le cas d'espèce.

Protection des données et appariement

Mise en œuvre de la Loi fédérale sur les résidences secondaires

Suite à l'acceptation de l'initiative populaire « Pour en finir avec les constructions envahissantes de résidences secondaires », une nouvelle disposition constitutionnelle a été introduite, plafonnant ainsi le pourcentage de résidences secondaires à 20% au maximum du parc de logements et de la surface brute au sol habitable de chaque commune. Cette dernière est concrétisée par la Loi du 20 mars 2015 sur les résidences secondaires (LRS), dont la mise en œuvre incombe en premier lieu aux cantons et aux communes. C'est dans ce cadre que l'Autorité a été approchée par le service responsable, qui propose un projet d'ordonnance d'application de la LRS au niveau cantonal. Cela consiste à mettre en place un système d'informations permettant d'assurer notamment la transmission des données sur le séjour et les déplacements de logement des personnes dont le domicile est situé dans une commune qui compte un taux de résidences secondaires de plus de 20%. Ce système d'informations rassemble les données relatives à plusieurs registres, notamment celles du registre fédéral des bâtiments et des logements (RegBL), du registre des habitants (RdH) et du registre foncier (RF), afin de déterminer la proportion

de résidences secondaires de chaque commune. La Préposée à la protection des données a analysé ce projet et a fait part de ses remarques. En principe, la Loi fédérale du 23 juin 2006 sur l'harmonisation des registres ne permet pas d'utiliser les données récoltées autrement qu'à des fins statistiques. Or, la législation relative aux résidences secondaires constitue une exception puisqu'elle permet d'utiliser les données du RdH à d'autres fins. Il va de soi qu'en tant qu'exception, elle doit faire l'objet d'une interprétation stricte qui ne va pas au-delà du cadre légal établi.

Droit d'accès

Droit d'accès à des données de police

L'Autorité est souvent sollicitée sur le droit d'accès à des données de police. En effet, certains citoyens se sont vu restreindre l'accès aux données les concernant contenues dans le protocole d'intervention ou dans le journal de police, dans la mesure où ces derniers sont réservés à l'usage interne du service et ne peuvent dès lors être communiqués. Toutefois, il ressort de la jurisprudence actuelle que le principe de proportionnalité commande, plutôt que de refuser tout accès au dossier, d'autoriser l'accès limité aux pièces dont la consultation ne compromettrait pas les intérêts en cause. Ainsi, l'Autorité est d'avis que les requérants disposent du droit de consulter le protocole d'intervention ou le journal de police, dans la mesure où des données les concernant y sont traitées. Mais par souci de proportionnalité et de protection de la sphère privée des tiers, le caviardage, l'anonymisation, voire des suppressions partielles doivent être effectuées au préalable par la Police cantonale.

Divers

Publication de photos sur le site Internet d'une association

Fréquemment, l'Autorité reçoit des demandes de personnes privées, par exemple au sujet de la publication de photos sur le site Internet d'une association. Dans ces cas, l'Autorité n'étant matériellement pas compétente dans la mesure où cela est du ressort du PFPDT, sa réponse est donnée en règle générale à titre indicatif. Dans le cas d'espèce, il s'agit de savoir quelles sont les règles générales applicables à la publication de photographies d'individus sur le site Internet d'une association. Toute personne est titulaire du droit à l'image qui lui permet de s'opposer à la fixation et à la diffusion de son image ou de soumettre son utilisation à des conditions. Il est donc essentiel d'informer préalablement la personne concernée et d'obtenir son consentement exprès avant de publier la photo. Le consentement est révocable en tout temps, ce qui entraîne l'obligation d'annuler la publication, pour autant que ce soit encore possible. En cas de «photo-portrait», la personne concernée doit donner son consentement exprès, après examen de la photo. Pour les photos où la personne ne se démarque pas en particulier (par exemple photo de groupe), une information générale suffit. La personne peut cependant demander à consulter la photo et s'opposer à sa publication. Si la photo a pour sujet des mineurs ou des personnes incapables de discernement, le consentement des représentants légaux est obligatoire.

«Transparence du financement de la politique»

L'initiative «Transparence du financement de la politique» prévoit la publication de l'identité des personnes morales participant au financement politique, ainsi que des personnes physiques à partir d'une contribution de CHF 5'000.-- par année civile. Un député a abordé l'Autorité afin de savoir si cette initiative est conforme à la protection des données. Après analyse, il apparaît que l'initiative ne contient pas d'élément non conforme aux règles en matière de protection des données personnelles. De manière générale, le fait que les opinions politiques soient des données sensibles n'empêche pas l'adoption d'une telle initiative. En revanche, il conviendra d'être particulièrement attentif aux modalités de mise en œuvre du texte constitutionnel en cas d'acceptation. On veillera notamment à ce que les donateurs potentiels soient renseignés préalablement et de manière claire et univoque sur le fait que leur identité peut être révélée publiquement et à quelles conditions. L'information devrait figurer de manière lisible dans tous les matériels mis à disposition des partis politiques. Une attention particulière doit être portée sur la manière dont l'identité des donateurs est révélée. Il est fortement recommandé d'éviter une publication sur Internet. L'Autorité recommande que les listes de donateurs soient déposées auprès d'un organe public où elles peuvent être consultées gratuitement. La période de consultation doit être limitée dans le temps et les listes détruites ensuite. Cela se justifie notamment par le fait que les opinions politiques sont susceptibles d'évoluer avec le temps et qu'au regard du principe d'exactitude, les données doivent être exactes et mises à jour. En outre, l'Autorité s'étonne que la limite de contribution de CHF 5'000.--/an permettant de ne pas publier l'identité des personnes physiques ne soit pas également appliquée aux personnes morales. Un contrôle au hasard pouvant entraîner une sanction en cas d'abus serait une solution plus en conformité avec le principe de proportionnalité. En cas d'acceptation de l'initiative, toutes les mesures d'organisation et les mesures techniques devront être prises afin de garantir la fiabilité des données collectées, leur protection et l'exercice des droits des personnes concernées (notamment droit d'accès, droit de rectification, indication des coordonnées du maître du fichier).

1.2 Contrôles

D'entente avec la Commission, la Préposée à la protection des données a procédé à un contrôle de grande envergure en matière de protection des données. Il s'agissait en l'occurrence de contrôler un établissement autonome de droit public dans le domaine des assurances sociales, doté de sa propre personnalité juridique. Le contrôle s'est déroulé sur plusieurs jours, dans les secteurs de la direction, des services généraux, des demandes, de la facturation et du service informatique. A nouveau le contrôle a été confié à une société externe mais la Préposée à la protection des données a été présente jusqu'à la fin du contrôle.

Il a été démontré que l'ensemble des collaborateurs sont sensibilisés aux questions du droit de la protection des données. Il convient de relever la bonne coopération des responsables et des collaborateurs de l'établissement. Le contrôle n'a pas pu être achevé à la fin de l'année, et la mise en œuvre des recommandations sera vérifiée au moyen de contrôles subséquents.

En outre, le suivi des contrôles de l'année 2015 a été poursuivi auprès des organes contrôlés, notamment en leur sollicitant des prises de positions relatives aux mesures engagées. En ce qui concerne le suivi des contrôles antérieurs à 2015, il n'a malheureusement pas pu se faire par manque de temps. Ce suivi devra se poursuivre et aboutir dans les meilleurs délais.

Faute de ressources, la Préposée à la protection des données a renoncé à effectuer un contrôle sur un organe public en tant qu'utilisateur du Système d'information Schengen dans le cadre des obligations européennes et fédérales (art. 54 de l'Ordonnance du 7 mai 2008 sur la partie nationale du Système d'information Schengen, N-SIS et sur le bureau SIRENE, ordonnance N-SIS).

1.3. FRI-PERS et vidéosurveillance

FRI-PERS

L'État de Fribourg exploite une plateforme centrale, FRI-PERS, qui contient toutes les données personnelles inscrites dans les registres des habitants. Cette plateforme permet notamment l'échange de données personnelles entre les communes, en particulier en cas de départs ou d'arrivées, et la transmission de données à l'Office fédéral de la statistique ou à des organes et services cantonaux. En vertu de l'Ordonnance du 14 juin 2010 relative à la plateforme informatique contenant les données des registres des habitants, il incombe à l'Autorité, dans le cadre de la procédure d'autorisation, de donner un préavis sur les demandes d'accès à cette plateforme cantonale (art. 3 al. 1). Lors d'une demande, la Direction de la sécurité et de la justice (DSJ) se prononce sur la base du préavis de l'Autorité. Au cours de l'année sous revue, il s'est avéré une nouvelle fois que les services et organes publics déposent de plus en plus de demandes visant à élargir l'accès à d'autres données et catégories de données. Néanmoins, de telles demandes ne se justifient pas toujours. La présence de données personnelles et le fait qu'on puisse peut-être en avoir besoin ne justifient pas encore l'autorisation à l'accès. Au contraire, la demande d'accès à certaines données et/ou catégories de données doit se fonder notamment sur les besoins du service et sur le principe de la proportionnalité.

Dans le cadre de la révision du formulaire et de la mise en œuvre de diverses demandes, plusieurs entretiens ont eu lieu avec les personnes responsables du SPoMi, du SITel ainsi que, de temps à autre, avec des responsables d'organes publics qui ont demandé un accès systématique aux données de la plateforme. Ces entretiens ont servi à clarifier les bases légales respectives et les besoins réels d'un accès.

Extension de l'accès

Dans le cadre de l'accomplissement de leurs tâches, notamment en matière pénale, de conciliation, de privation de liberté à des fins d'assistance, d'exercice des droits politiques, de légalisation des signatures, les Préfectures ont obtenu un accès aux données de la plateforme informatique cantonale FRI-PERS limité aux données des habitants du district concerné. Cependant, depuis la mise en œuvre de la législation relative aux résidences secondaires, les Préfectures ont requis une extension de leur accès aux données FRI-PERS ainsi qu'à l'historique des données portant sur tout le territoire du canton de Fribourg. En effet, les données d'arrivée et de départ lors des deux dernières années des habitants de tout le canton sont nécessaires afin de définir si elles concernent une résidence secondaire ou occupée. Après discussion, il ressort que les Préfectures ont besoin uniquement de l'accès aux données administratives des habitants de tout le canton complétées par la date d'arrivée et de déménagement ainsi que l'accès à l'historique des deux dernières années. La Préposée à la protection des données a, d'une part, confirmé l'accès octroyé aux données des habitants du district concerné aux collaborateurs des Préfectures qui en ont besoin, et d'autre part, émis un préavis favorable à l'accès aux données administratives portant sur tout le territoire du canton de Fribourg complétées par la date d'arrivée et de déménagement ainsi qu'à l'historique des données des deux dernières années mais octroyé uniquement à 3 collaborateurs par Préfecture qui traitent des dossiers relatifs aux résidences secondaires et aux dénonciations en matière pénale et d'absence scolaire. La DSJ a entièrement suivi notre préavis.

Dans deux cas, la Commission a émis des recommandations (voir sous II.C.).

Vidéosurveillance

La Préposée à la protection des données doit être informée au préalable lors de demandes d'installation de vidéosurveillance de systèmes sans enregistrement (art. 7 LVID). De plus, il entre dans ses tâches d'émettre des préavis sur les demandes d'installation de vidéosurveillance avec enregistrement (art. 5 al. 2 de la Loi du 7 décembre 2010 sur la vidéosurveillance; LVID).

Les demandes de particuliers à propos de la vidéosurveillance ont fortement augmenté. Nombre d'entre eux s'inquiètent au sujet des multiples vidéosurveillances, que ce soit sur le domaine privé avec ou sans prise de vue du domaine public, ou que ce soit dans des locaux privés ou sur des terrasses. La vidéosurveillance par des particuliers et sans champ de vision sur le domaine public relève de la loi fédérale sur la protection des données et par conséquent, entre dans le domaine de compétence du PFPDT.

La collaboration avec les préfets est bonne. Ceux-ci suivent généralement nos prises de position. Actuellement deux recours sont en suspens devant le TC, contre une décision de refus de la préfecture; l'un émane d'une commune et l'autre d'un particulier. Le 30 décembre 2015, le TC a rejeté le recours d'un particulier contre la décision du préfet qui avait refusé l'installation d'une vidéosurveillance et ordonné l'enlèvement des caméras déjà installées.

La liste des installations de vidéosurveillance est disponible sur les sites Internet des préfectures, conformément à ce que prévoit l'art. 9 de l'Ordonnance du 23 août 2011 sur la vidéosurveillance (OVID).

Caméras de vidéosurveillance soumises ou non à la LVID

Un établissement médico-social (EMS) a déposé une demande d'installation de vidéosurveillance avec enregistrement ainsi qu'une annonce de vidéosurveillance sans enregistrement auprès du lieutenant de préfet de la Sarine. Au vu de la complexité de la demande, une vision locale a permis de déterminer quelles caméras filment le domaine public et sont ainsi soumises à la Loi du 7 décembre 2010 sur la vidéosurveillance (LVID) et lesquelles d'entre elles enregistrent les images. En outre, il a également fallu définir les buts de cette vidéosurveillance. Il ressort de l'analyse que les caméras enregistrant des images de l'entrée principale et du parking extérieur principal filment le domaine public et sont soumises à la LVID, puisque c'est un immeuble ouvert au public et affecté à l'administration publique. Alors que les caméras permettant de visionner en temps réel (sans enregistrement) les couloirs des deux nouvelles unités de soins (gériatrie et psychogériatrie) ainsi que le jardin thérapeutique ne sont pas soumises à la LVID mais à la LPrD ainsi qu'aux règles spécifiques du Code civil du 10 décembre 1907 (CC) traitant de la protection de l'adulte. Dans le cas d'espèce, l'installation de vidéosurveillance poursuit deux buts: d'une part, la surveillance de la réception principale et du parking extérieur afin d'éviter les atteintes aux biens (vols, déprédations) et, d'autre part, la recherche de résidents désorientés ou ayant fugué. La surveillance doit se limiter à ce qui est strictement nécessaire. Ainsi, l'Autorité a rendu un préavis favorable concernant les caméras filmant le domaine public sous réserve de certaines conditions telles que, par exemple, l'installation d'un système de floutage des images, le visionnement des enregistrements uniquement en cas de délits avérés, le champ de prise de vue des caméras qui ne doit pas être dirigé contre des immeubles, maisons privées ou arrêt de bus et le bref délai de conservation des enregistrements. La Préfecture de la Sarine a entièrement suivi notre préavis.

Transmission d'enregistrements vidéo d'une station-service à la Police

Suite à l'oubli d'un conducteur de payer son essence (environ CHF 10.--), la station-service a dénoncé le cas à la Police cantonale en lui transmettant les enregistrements vidéo. Un agent de police a contacté le concierge de la résidence du conducteur afin d'obtenir le numéro de téléphone de ce dernier. La personne concernée a alors abordé l'Autorité afin de savoir si la durée de conservation des enregistrements de vidéosurveillance de la station-service, la méthode de dénonciation à la Police cantonale et le rôle joué par cette dernière sont conformes à la protection des données. L'Autorité relève que l'utilisation par des particuliers de caméras vidéo à des fins de protection contre les atteintes aux biens et aux personnes tombe sous la Loi fédérale du 19 juin 1992 sur la protection des données (LPD), lorsque la personne est identifiée ou identifiable. Ainsi, l'Autorité n'est pas compétente pour traiter de ce point. Cependant, il ressort des recommandations du PFPDT que les données personnelles enregistrées ne doivent pas être divulguées, sauf à des fins de dénonciation aux autorités de poursuites pénales et doivent être effacées dans un délai particulièrement bref. S'agissant de la dénonciation de la station-service, cette dernière a agi en conformité avec la législation. En effet, ne disposant pas des pouvoirs de police, elle n'a d'autres moyens que de faire appel aux autorités compétentes pour identifier l'auteur, à moins que le client soit un habitué et que la station lui communique personnellement son oubli lors de l'une de ses prochaines visites. Une fois le numéro d'immatriculation relevé sur les enregistrements vidéo, la Police cantonale est en droit de rechercher l'identité du conducteur. Toutefois, l'Autorité est d'avis que, sous l'angle de la proportionnalité et compte tenu du faible montant en jeu, il n'était pas objectivement nécessaire que la Police cantonale s'adresse au concierge pour lui demander la communication du numéro du conducteur. En effet, d'autres moyens plus respectueux des droits de sa personnalité auraient permis de parvenir au même résultat.

1.4. ReFi – registre des fichiers¹³

L'Autorité doit tenir un registre des fichiers qui contient l'ensemble des déclarations de fichiers, sauf celles des communes qui ont leur propre autorité de surveillance. Pour les organes publics, la déclaration des fichiers est une obligation légale (art. 19 ss LPrD). Ce registre constitue un outil important pour les différents partenaires de la protection des données et sert la transparence. Il révèle quels fichiers sont collectés par quel service. Le registre est public et peut être consulté sur le site Internet de l'Autorité¹⁴.

Après la mise à jour de l'application informatique intervenue en 2015 et 2016, il était devenu impératif de mettre à jour la documentation à l'attention des différentes catégories d'utilisateurs (organes publics, internautes et administrateurs) et de procéder à diverses mesures de sensibilisation. D'abord, les personnes de contact ont été informées, et tous les organes publics ont reçu une invitation écrite à vérifier et/ou à réaliser leurs déclarations de fichiers. D'autre part, trois séances d'information ont été organisées à l'intention des communes (deux en français et une en allemand). Un groupe de travail composé de représentantes et représentants d'une préfecture, des communes, du Service des communes ainsi que de l'Autorité est en train de déterminer les fichiers existants dans une commune et de mettre au point des annonces-types. Le résultat des travaux de ce groupe sera disponible au début de l'année.

¹³ http://www.fr.ch/atprd/fr/pub/registre_des_fichiers/introduction.htm

¹⁴ <http://appl.fr.ch/refi/etat/client/index.aspx>

1.5. Echanges

En sus des rencontres entre collègues dans le cadre de privatim et du Groupe des Préposés latins, l'échange est important aussi avec la vingtaine de personnes dites «personnes de contact en matière de protection des données» des directions et établissements, qui ont aussi été invitées par la Préposée à la protection des données pendant l'année sous revue pour des échanges d'informations et de points de vue. Des informations leur sont fournies de manière ponctuelle sur différents thèmes (p. ex. newsletter, manifestations).

2. Statistiques

Protection des données en général

Durant la période considérée, 285 dossiers en matière de protection des données (sans les demandes FRI-PERS et vidéosurveillance, voir ci-dessous) ont été introduits, dont 68 sont pendants au 1^{er} janvier 2017. 122 conseils et renseignements, 43 avis, 30 examens de dispositions législatives, 12 communications de décisions (art. 27 al. 2 LPrD), 1 recommandation, 5 contrôles et inspection ou suivis de contrôle, 10 présentations, 29 participations à des séances et autres manifestations et 33 demandes diverses. 124 dossiers concernent des organes cantonaux ou des institutions chargées de tâches publiques, 39 des communes et paroisses, 72 d'autres organismes publics (cantons, autorités de protection des données), 43 des particuliers ou des institutions privées et 7 des médias. Pour les dossiers pendants des années précédentes, 47 dossiers ont été réglés. De plus, et pour information, l'Autorité a été sollicitée à plusieurs occasions pour des questions pour lesquelles elle n'était pas compétente. Les organes publics ou les particuliers ont dès lors été dirigés auprès des services compétents.

FRI-PERS

Au 31 décembre 2016, 18 dossiers ont été ouverts. 14 demandes ont été soumises à la Préposée à la protection des données pour préavis: 6 demandes d'accès, 4 demandes d'extension de l'accès, 4 demandes d'interfaçage par webservices (avec ou sans réception d'événements). De ces requêtes, 8 demandes sont toujours en traitement, nécessitant des renseignements supplémentaires, et 6 ont obtenu un préavis positif. La Commission a également émis des recommandations dans deux cas (voir ci-dessus II. C.) et a fait un recours qui est devenu sans objet suite à la nouvelle décision de la DSJ. De plus, notre Autorité a été invitée à réexaminer une décision de la DSJ. La collaboration avec la DSJ est bonne, de sorte que cette dernière a suivi les préavis de l'Autorité, pratiquement dans tous les cas. L'évolution des technologies permet de développer les modes d'utilisation de la plateforme FRI-PERS, et les requêtes deviennent de plus en plus complexes (pointues). Ainsi, la procédure et les documents sont constamment évalués par les services concernés.

Vidéosurveillance

Durant l'année 2016, la Préposée à la protection des données a reçu 13 demandes d'installation de vidéosurveillance avec enregistrement pour préavis et 1 annonce d'installation de vidéosurveillance sans enregistrement et a dû se déterminer à 3 reprises dans des procédures de recours. De ces requêtes, 8 préavis positifs ont été émis, 1 préavis défavorable, 3 n'ont pas abouti car la LVID n'était pas applicable, alors que les 2 dernières sont encore en cours de traitement. Tous les préavis positifs étaient assortis de conditions, notamment de satisfaire à l'exigence de signalisation des systèmes de vidéosurveillance. Par ailleurs, 4 demandes émanaient des services de l'Etat ou de communes et 10 de privés. Conformément à ce que prévoit l'art. 9 OVID, la liste des installations de vidéosurveillance est disponible sur les sites Internet des préfectures.

De ces statistiques, l'Autorité peut constater le peu de demandes adressées aux préfetures et s'en étonner, d'autant plus que la vidéosurveillance a fait plusieurs fois parler d'elle dans les médias. L'Autorité a notamment été contactée à plusieurs reprises à ce sujet durant cette année 2016. En outre, l'Autorité relève que les demandes sont toujours plus complexes. En effet, des requêtes de caméra mobile ou d'enregistrements de domaines publics communs sont en augmentation. Ainsi, après l'analyse juridique, des tests et des visions locales doivent être effectués avant toute autorisation.

IV. Coordination entre la transparence et la protection des données

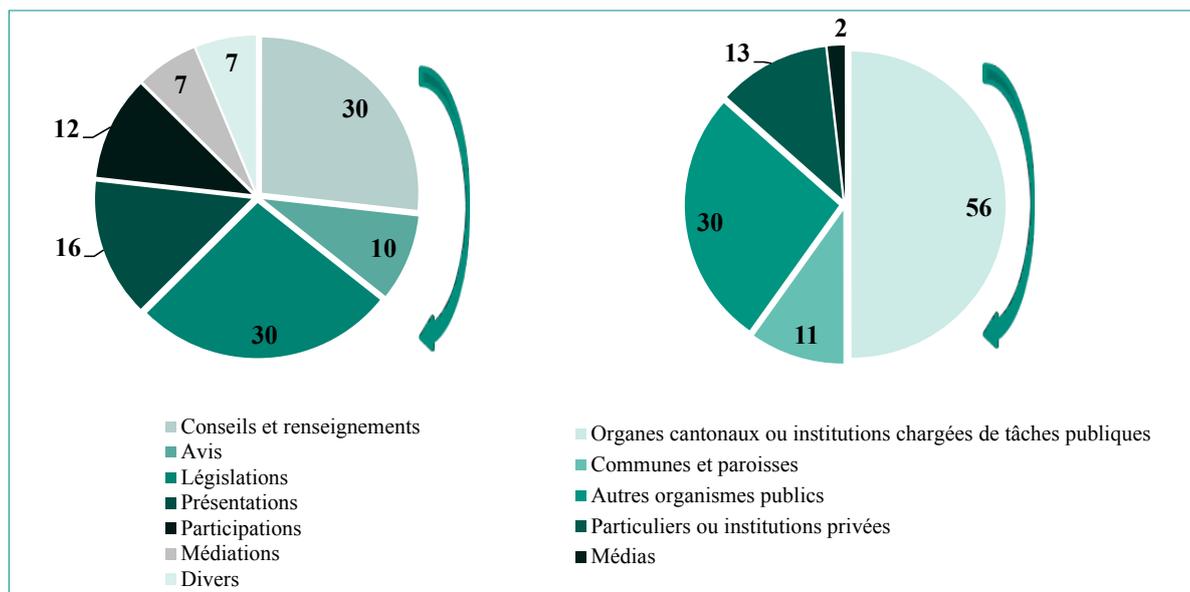
La bonne collaboration entre les deux Préposées s'est poursuivie en 2016. Plusieurs mesures avaient été prises dès le début pour la préservation de cette coopération. Les séances de la Commission, auxquelles les deux Préposées participent, traitent régulièrement les dossiers portant sur les deux domaines. Les Préposées se voient fréquemment pour les échanges nécessaires. Enfin, les contacts avec le Président favorisent également la coordination.

V. Remarques finales

L'Autorité cantonale de la transparence et de la protection des données **remercie** tous les organes publics pour la collaboration développée jusqu'ici, pour l'intérêt manifesté envers le droit d'accès à l'information ainsi qu'envers leur obligation de respecter les dispositions légales sur la protection des données personnelles et par là les personnes. Ces remerciements s'adressent en particulier aux personnes de contact au sein de l'administration et des établissements cantonaux qui aident efficacement les Préposées dans l'accomplissement de leurs tâches.

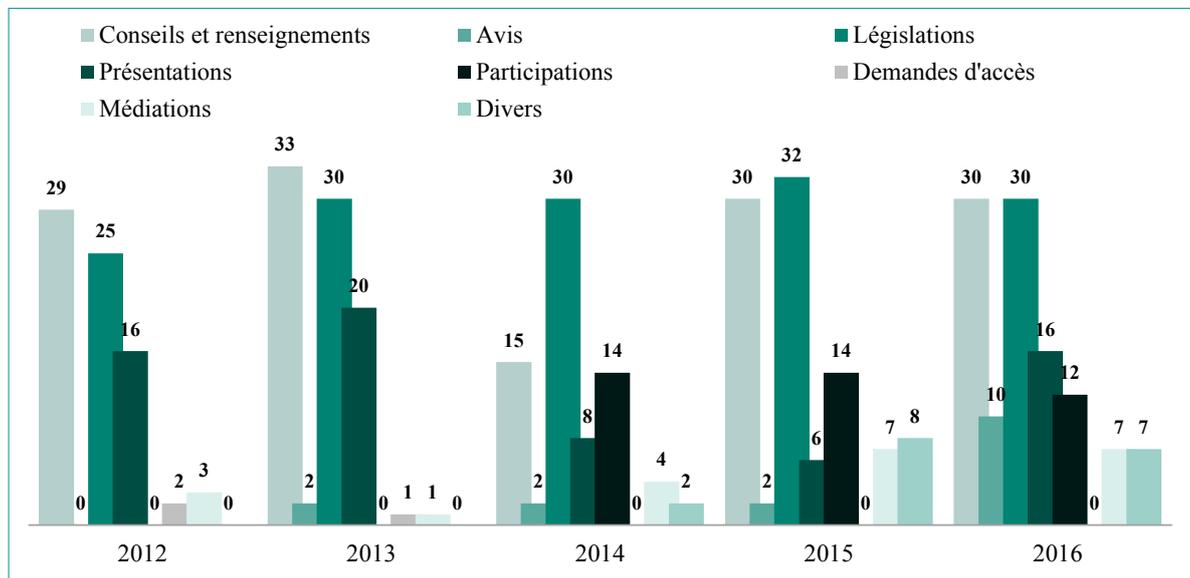
Statistiques de la transparence

Demandes / interventions en 2016



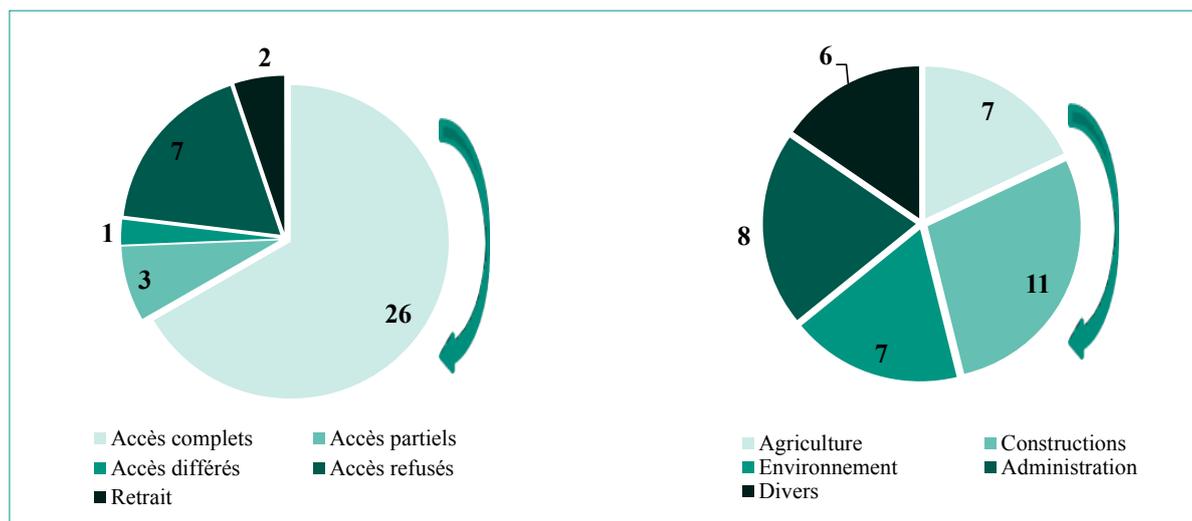
- > Les «conseils et renseignements» sont donnés par la Préposée à la transparence.
- > Le terme «législations» comprend les travaux de réflexion sur des dispositions législatives et les réponses aux consultations.
- > La notion de «présentations» recouvre par ex. les exposés dans le cadre de la présentation du droit d'accès, les formations continues organisées par l'Etat de Fribourg et celles pour les apprenti-es et les «stagiaires 3+1».
- > La notion de «participations» recouvre par ex. les séances (groupes de travail), les conférences et les colloques.
- > Parmi les 112 dossiers ouverts en 2016, 52 dossiers sont communs avec ceux de la protection des données, dont 30 consultations.

Comparatif



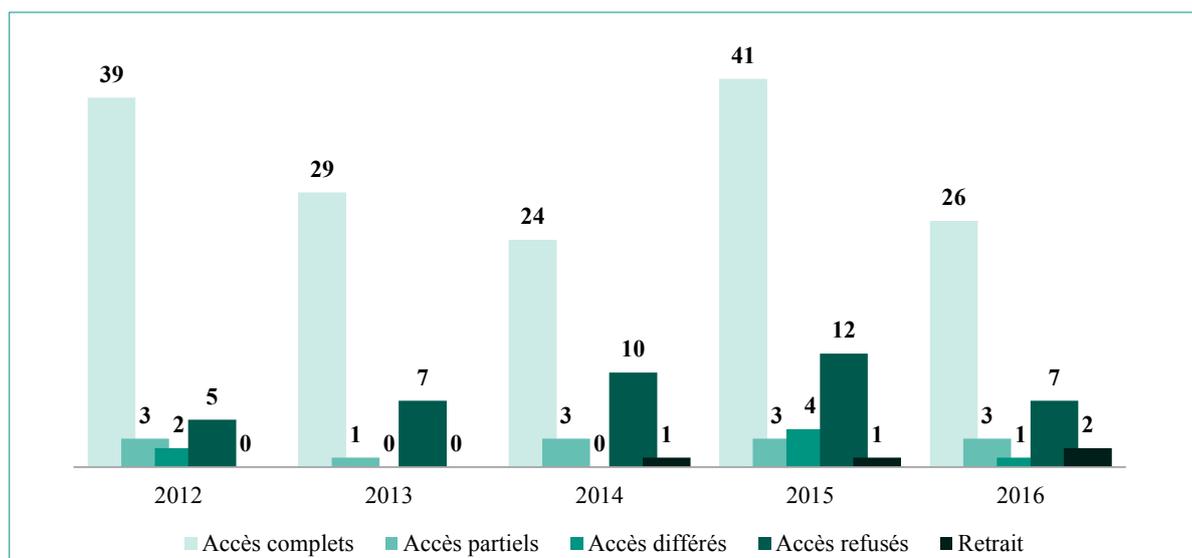
Evaluation du droit d'accès en 2016

—



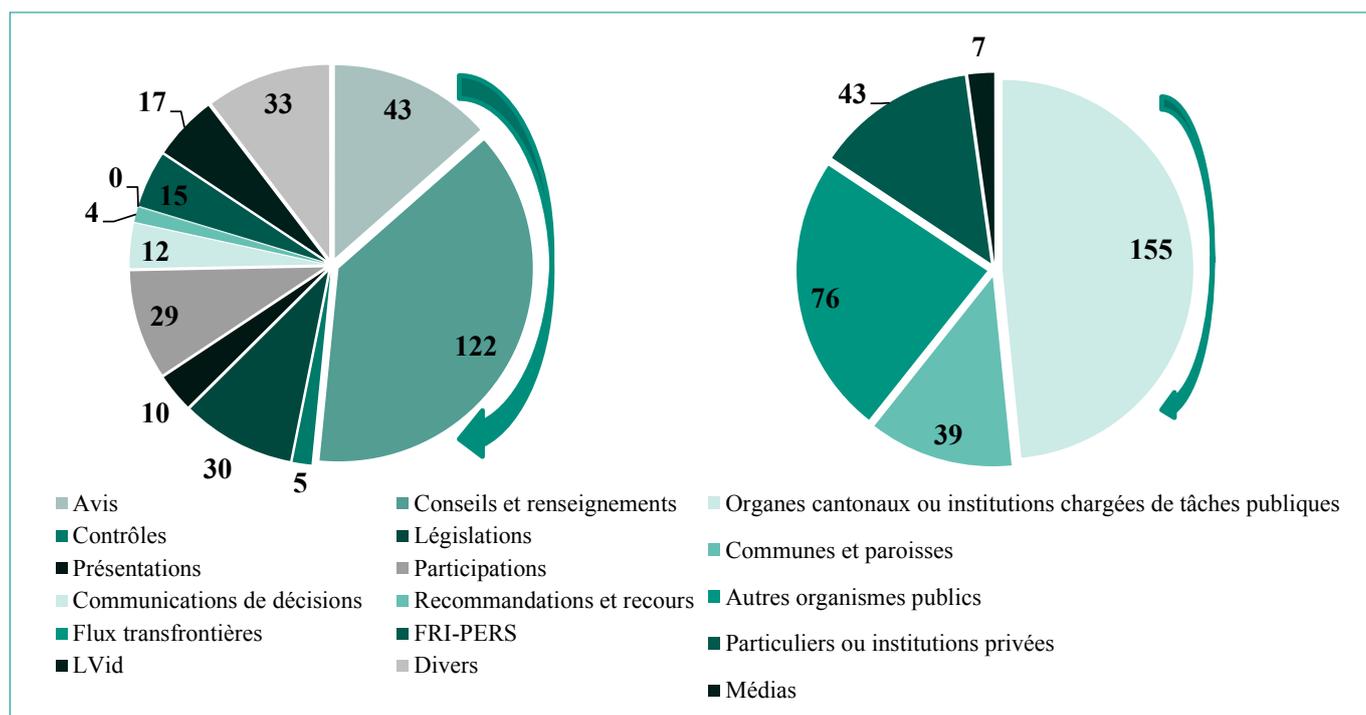
Comparatif

—



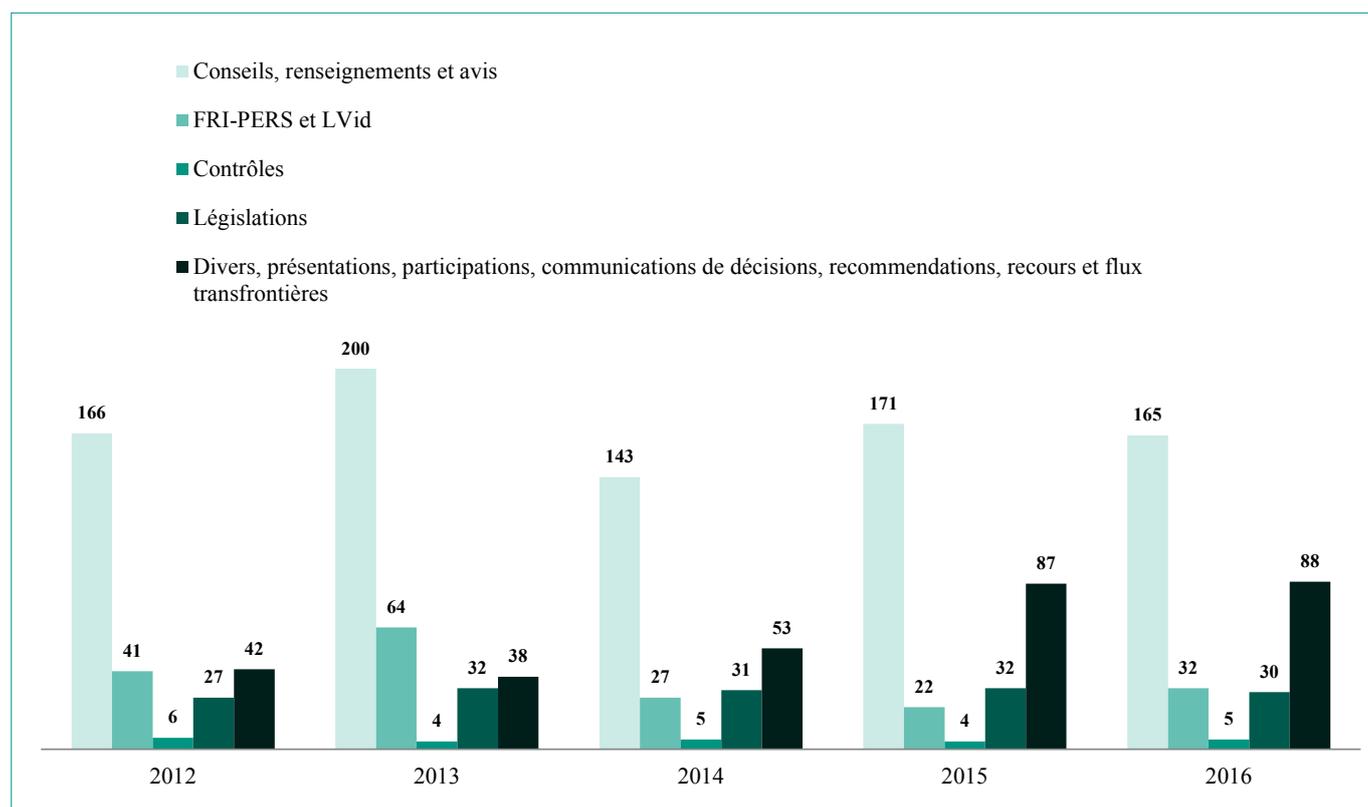
Statistiques de la protection des données, FRI-PERS et LViD

Demandes / interventions en 2016



- > Les «conseils et renseignements» concernent des questions posées par les organes publics ou par les particuliers concernés, ainsi que des questions relatives à leurs droits.
- > Les «avis» sont rendus par la Préposée à la protection des données; ils comprennent les prises de position/conseils de la Préposée, établis sur la base d'une publication, d'un projet ou d'une proposition soumis par les organes publics ou par un particulier.
- > Les «contrôles» comprennent les vérifications de l'application de la législation relative à la protection des données par la Préposée ainsi que leurs suivis.
- > Le terme «législations» comprend les travaux de réflexion sur des dispositions législatives et les réponses aux consultations.
- > La notion de «présentations» recouvre par ex. les exposés, les rapports et les formations continues organisées par l'Etat de Fribourg et celles pour les apprenti-es et les stagiaires 3+1.
- > La notion de «participations» recouvre par ex. les séances (groupes de travail), les conférences et les colloques.
- > Pour les «communications» de décisions, voir art. 27 al. 2 let. a LPrD.
- > Pour les «recommandations», voir art. 30a LPrD.
- > Pour les «flux transfrontières», voir art. 12a LPrD.
- > Parmi les 320 dossiers ouverts en 2016, 50 dossiers sont communs avec ceux de la transparence, dont 30 consultations.

Comparatif



Demandes / interventions

Années	Avis	Conseils et renseignements	Contrôles	Législations	Présentations	Participations	Communications de décisions	Recommandations et recours*	Flux transfrontières	FRI-PERS**	LVID**	Divers	Total
2016	43	122	5	30	10	29	12	4	0	15	17	33	320
2015	58	113	4	32	4	23	22	0	0	17	5	38	316
2014	37	106	5	31	5	25	3	0	1	9	18	19	259
2013	34	166	4	32	33	0	2	1	1	16	48	1	338
2012	95	71	6	27	16	0	1	0	0	13	28	25	282
2011	107	80	9	36	5	0	2	0	0	30	0	0	269

* dont 2 recommandations et 1 recours FRI-PERS

** dont 14 préavis FRI-PERS et 13 préavis LVID