Rapport d'activité 2017

—

pour la période du 1er janvier
au 31 décembre 2017

ETAT DE FRIBOURG
STAAT FREIBURG

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

EC 918

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 2018

—

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 2017 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 2018

Le Président de la Commission	La Préposée à la transparence	La Préposée à la protection des données
L. Schneuwly	A. Zunzer Raemy	A. Reichmuth Pfammatter

Table des matières

Table des abréviations et termes utilisés

AFin	Administration des finances
AFOCI	Association fribourgeoise pour l'organisation des cours interentreprises
AP	Avant-projet
ATPrD	Autorité cantonale de la transparence et de la protection des données
AVS	Assurance-vieillesse et survivants
CC	Code civil du 10 décembre 1907
CP	Code pénal du 21 décembre 1937
CPJA	Code de procédure et de juridiction administrative du 23 mai 1991
CPP	Code de procédure pénale du 5 octobre 2007
DFJP	Département fédéral de justice et police
DICS	Direction de l'instruction publique, de la culture et du sport
DSJ	Direction de la sécurité et de la justice
FRI-PERS	Plateforme informatique cantonale du contrôle des habitants
HESSO//FR	Haute Ecole spécialisée de Suisse occidentale//Fribourg
VIH	Virus de l'immunodéficience humaine
LACI	Loi du 25 juin 1982 sur l'assurance chômage
LCH	Loi du 23 mai 1986 sur le contrôle des habitants
LCo	Loi du 25 septembre 1980 sur les communes
LESS	Avant-projet de loi sur l'enseignement secondaire supérieur
LInf	Loi du 9 septembre 2009 sur l'information et l'accès aux documents
LMéd	Loi du 25 juin 2015 sur la médiation administrative
Loi e-ID	Loi fédérale sur les moyens d'identification électronique reconnus
LP	Loi fédérale du 11 avril 1889 sur la poursuite pour dettes et la faillite
LPD	Loi fédérale du 19 juin 1992 sur la protection des données
LPers	Loi du 17 octobre 2001 sur le personnel
LPGA	Loi fédérale du 6 octobre 2000 sur la partie générale du droit des assurances sociales
LPrD	Loi du 25 novembre 1994 sur la protection des données
LVid	Loi du 7 décembre 2010 sur la vidéosurveillance
NAVS13	Numéro AVS à 13 chiffres
N-SIS	Partie nationale du système d'information Schengen
OAD	Ordonnance du 14 décembre 2010 sur l'accès aux documents
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
ReFi	Registre des fichiers
RSD	Règlement du 29 juin 1999 sur la sécurité des données personnelles
SCC	Service cantonal des contributions
SeCa	Service des constructions et de l'aménagement
SIRENE	Service de contact, de coordination et de consultation de l'Office fédéral de la police pour l'échange d'information en rapport avec les signalements dans le SIS
SIS	Système d'information Schengen
SITel	Service de l'informatique et des télécommunications
SPoMi	Service de la population et des migrants
UE	Union européenne
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 donnés les moyens dont elle dispose. L'évolution des nouvelles technologies et les projets informatiques toujours plus complexes requièrent de disposer de ressources supplémentaires, en particulier dans le domaine de la sécurité de l'information.

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;
- rendre les décisions en matière de droit d'accès dans les cas où la demande d'accès a été adressée à une personne privée ou un organe d'institution privée qui accomplissent des tâches de droit public dans le domaine de l'environnement, même s'ils n'ont pas la compétence d'édicter des règles de droit ou de rendre des décisions;
- 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 2017, 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 (jusqu'à fin août 2017), M. *Philippe Gehring,* ingénieur en informatique EPFL, M^me^ *Madeleine Joye Nicolet,* ancienne journaliste (jusqu'à fin août 2017), M. *André Marmy,* médecin, et Mme *Annelise Meyer-Glauser,* ancienne Conseillère communale

[1] https://bdlf.fr.ch/frontend/versions/4692
[2] https://bdlf.fr.ch/frontend/versions/4691

(jusqu'à fin août 2017). Ont été élus nouveaux membres de la Commission par le Grand Conseil: M^me^ *Anne-Sophie Brady,* avocate et Conseillère communale, M. *Jean-Jacques Robert,* ancien journaliste, M. *Luis Roberto Samaniego,* ingénieur en gouvernance et sécurité informatiques à l'HESSO Fribourg, et M. *Gerhard Fiolka,* Professeur associé à l'Université de Fribourg.

La Commission a tenu neuf séances en 2017. Un procès-verbal rédigé par la collaboratrice administrative fait état des délibérations et des décisions prises par la Commission.
Hors séances, le Président a assuré le suivi des dossiers, la correspondance, les discussions avec les Préposées durant 117 heures sur l'ensemble de l'année. Enfin, tant le Président que le Vice-président ont pris part sporadiquement à des entretiens.

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.

S'y ajoute la tâche de remplaçante du médiateur ou de la médiatrice cantonal-e inscrite dans l'article 8 de la Loi du 25 juin 2015 sur la médiation administrative (LMéd).

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 (PFPDT) 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];

[3] https://bdlf.fr.ch/frontend/versions/4597

› 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 précédents[5]), 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 procédure 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).

Le Médiateur cantonal est entré en fonction le 1er janvier 2017. La Loi sur la médiation administrative (LMéd) prévoit la collaboration du Médiateur cantonal avec l'Autorité. Divers entretiens ont donc été nécessaires pour clarifier la question des mesures à prendre sur le plan organisationnel. La garantie de la confidentialité a grandement préoccupé l'Autorité.

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 ainsi qu'à l'adjoint du PFPDT 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 une fois durant l'année 2017 par le PFPDT[6]. Les thèmes traités lors de la séance ont porté notamment sur les dernières évolutions de la législation européenne ainsi que sur la création d'un guide commun pour le contrôle de l'utilisation des fichiers de consignation du système d'information de Schengen SIS. Ce guide a été rédigé par un groupe de travail composé de collaborateurs du PFPDT et de préposés cantonaux à la protection des données. Durant l'année sous examen, la collaboration intercantonale s'est révélée très

[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
[6] https://www.edoeb.admin.ch/edoeb/fr/home.html

importante, sous l'angle de la rédaction de prises de position communes sur des thèmes touchant soit tous les cantons soit plusieurs d'entre eux. Ainsi la Préposée à la protection des données a été active au sein de l'organisation d'accompagnement à Schengen/Dublin (OASD) de la Conférence des directeurs cantonaux, qui a mis au point pour les cantons un Guide qui explique comment les lois cantonales sur l'information et la protection des données doivent être adaptées à la réforme de la protection des données adoptée par l'UE ainsi qu'à la modernisation de la convention STE 108 du Conseil de l'Europe.

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 2017 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 a eu lieu au printemps à Schaffhouse. Au premier plan, le thème du secret médical a été traité sur toile de fond de l'externalisation croissante des prestations informatiques, de l'administration et des archives. La question s'est posée de savoir si cet outsourcing des données de santé des patients est véritablement conciliable avec la protection des données (cf. Newsletter 1/2017 sur le site Internet de l'Autorité). L'assemblée plénière d'automne a eu lieu à Altdorf/UR. La séance d'information a été consacrée aux solutions cloud pour les écoles. Par ailleurs, privatim a organisé pour ses membres une séance d'information relative au dossier électronique du patient ainsi qu'une session de formation d'une journée portant sur la «Sécurité informatique pour les juristes».

Depuis la mi-2016, le Président de privatim est le Préposé de 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. De surcroît, sur invitation des Hautes Ecoles spécialisées de Suisse occidentale/Fribourg, elle a donné à quatre reprises un exposé sur le sujet de la protection des données dans le contexte académique. Invitée par une association professionnelle du secteur de l'énergie, elle a également participé à une session interne.

[7] https://www.privatim.ch/fr/

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 actualités . En mai 2017, l'Autorité cantonale de la transparence et de la protection des données a tenu sa traditionnelle **conférence de presse.**

Dans ses **newsletters** semestrielles , 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.

La Commission a publié une feuille d'information sur l'externalisation de traitements de données sur des clouds publics (accessible sur le site Internet de l'Autorité).
La Commission rappelle dans sa feuille informative les risques inhérents à l'externalisation, notamment relatifs au Cloud computing. Ces risques sont particulièrement liés à la perte de maîtrise du système d'informatisation (à l'accès d'autorités étrangères, à la captivité, à la perte de données, etc.), aux interventions à distance et à l'hébergement mutualisé, c'est-à-dire l'hébergement des données de plusieurs utilisateurs par le même système. La Commission relève l'absence de base légale concernant l'externalisation du traitement de données des organes dans un cloud. Elle préconise que, dans la mesure où l'Etat est responsable de la protection des données et traite des données sensibles soumises au secret de fonction/professionnel, un cloud étatique doit être développé afin de garder la maîtrise totale de toutes les données traitées par l'Etat. C'est ainsi que les données resteraient en main de l'Etat, lequel doit garantir l'effectivité des droits fondamentaux des personnes face au traitement de leurs données personnelles par des organes publics.

[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 2017 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.

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 Internet[11].

1.2 Quelques exemples de prises de position

Avant-projet de loi fédérale sur la révision totale de la Loi sur la protection des données et sur la modification d'autres lois fédérales

L'Autorité a été chargée de préparer une réponse à la procédure de consultation relative à l'avant-projet de loi fédérale sur la révision totale de la Loi sur la protection des données et la modification d'autres lois fédérales, à l'Arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'Union européenne sur la reprise de la directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données personnelles à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuite en la matière ou d'exécution de sanctions pénales, ainsi qu'à la révision de la Convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. L'avant-projet du Conseil fédéral se distingue avant tout par un renforcement de la protection des données et par la neutralité de cette protection au plan technique; en particulier, le traitement des données doit être plus transparent et les personnes concernées doivent obtenir davantage de contrôle sur leurs données. Selon l'avant-projet, les personnes morales doivent être exclues du champ d'application de la loi. La Commission a salué le renforcement de la protection des données notamment en incitant désormais les responsables de traitement à prendre en considé-

[11] http://www.fr.ch/atprd/fr/pub/transparence/consultations.htm

ration les enjeux de la protection des données dès la mise en place des systèmes de nouveaux traitements, d'exiger une base légale formelle concernant le traitement des données sensibles, le profilage ou la prise de décision individuelle automatisée ainsi que la mise en place par défaut de la solution la plus favorable à la protection des données *(Privacy by default)*. A également été relevée la neutralité technologique du projet, laquelle laisse une large interprétation aux développements technologiques futurs. La Commission a toutefois regretté la suppression des règles explicites relatives à la procédure d'appel (accès en ligne) et l'absence du droit à l'effacement des données (droit à l'oubli) traité dans le Règlement de l'Union européenne, ce qui affaiblit la position du citoyen suisse à l'égard des grands acteurs globaux. De même, la mise en échec de manière automatique du secret de fonction et du secret professionnel, notamment du secret médical, a été considérée comme problématique. Dans sa prise de position, la Commission a contesté que le secret professionnel et de fonction devrait être levé en ce qui concerne les données à caractère personnel de défunts; autrement dit, il n'y a plus besoin de libérer de ces secrets les professionnels qui y étaient liés du vivant de la personne concernée. Il a également été relevé que la possibilité pour le Préposé fédéral à la protection des données et à la transparence de faire des recommandations au sujet d'une bonne pratique n'était pas suffisante, car l'application de ces recommandations ne serait pas impérative. La création de nouvelles dispositions pénales en matière de protection des données a également été critiquée: ces dispositions délègueraient la poursuite pénale aux cantons, ce qui fait craindre une pratique non uniforme. Le Conseil fédéral a publié en septembre 2017 le Message y relatif, avec un projet remanié.

Avant-projet d'ordonnance modifiant l'Ordonnance sur l'accès aux documents (adaptation à la Convention d'Aarhus)
Suite à 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), l'Ordonnance sur l'accès aux documents (OAD) a été révisée en 2017. Dans le cadre de sa consultation, la Commission a approuvé les modifications prévues par le projet et a salué les ajustements qui tiennent compte de la pratique des premières années d'application de la LInf, notamment l'obligation de collaborer à la médiation et la clarification de ce qui n'est pas à considérer comme une demande d'accès (cf. III A 1.4).

Loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID)
Consultée dans le cadre de la procédure de consultation fédérale relative à la Loi fédérale sur les moyens d'identification électronique reconnus (loi e-ID), la Commission a d'abord signalé que, de manière générale, l'utilisation de l'e-ID dans le cadre de l'activité étatique ne peut pas concerner plus de données personnelles que dans le monde «réel». Si la Commission a salué les efforts de mise en œuvre d'un système d'identification électronique permettant de réduire les risques d'identité dans le cadre de relations commerciales ou avec l'Etat, elle a en revanche estimé que l'établissement de documents d'identité doit rester une tâche étatique, cela valant également pour l'identification électronique. L'Etat doit en rester le principal fournisseur. La Commission a par ailleurs estimé que le catalogue des données d'identification personnelle est trop long et contient des données biométriques, lesquelles sont des données sensibles. Cette liste n'étant pas exhaustive, elle offre la possibilité d'ajouter des données. La norme ne répond donc pas au principe de la proportionnalité. Enfin, la Commission s'est prononcée sur l'utilisation systématique du NAVS13 par le service d'identité à des fins d'identification de personnes dans le cadre de l'échange électronique de données avec les registres de personnes. L'utilisation du numéro AVS comporte un grand risque d'interconnexions de données personnelles dans les différents systèmes, risque augmenté si une utilisation systématique est envisagée. La Commission a ainsi exigé que ce numéro ne soit pas accessible à des particuliers et ne soit ni transmis aux fournisseurs ni stocké dans leurs systèmes et bases de données. Le numéro AVS ayant été prévu pour être utilisé dans

le domaine des assurances sociales, son utilisation systématique devrait en principe être autorisée uniquement aux organes et services chargés des tâches dans ce domaine.

Avant-projet de loi modifiant la Loi sur la santé
La Direction de la santé et des affaires sociales a ouvert une procédure de consultation concernant la révision partielle de la Loi sur la santé. S'agissant du registre des tumeurs, la Commission a estimé que la formulation de la disposition est beaucoup trop large. En outre, elle a demandé de préciser les maladies et les données personnelles qui doivent être collectées, en sus de celles mentionnées dans la législation fédérale. Il en va de même pour les données sensibles, d'autant plus que, le cas échéant, le secret professionnel devrait être levé.

Projet d'ordonnance d'application de la Loi sur l'exécution des peines et des mesures
Lors de la consultation relative au projet d'ordonnance d'application de la Loi sur l'exécution des peines et des mesures, la Commission a salué le fait que le règlement précise aux mains de qui se trouve le dossier médical du détenu. Elle a cependant demandé à ce que la disposition réglant le dossier de santé du détenu soit plus détaillée et a relevé que celui-ci doit respecter les règles de la Loi sur la santé, mais également celles sur la protection des données. A cet égard, il est important que l'accès des médecins externes se fasse par une authentification forte. L'Autorité a également précisé dans le règlement que le détenu doit donner son accord à l'utilisation de ses données, ainsi qu'à leur suppression après 12 mois de conservation, ce qui est conforme à la protection des données.

Projet de modification du Code civil – enregistrement de l'état civil et registre foncier
Lors de la procédure de consultation fédérale relative à la modification du Code civil, la Commission a relevé son désaccord concernant l'utilisation du numéro AVS par le registre foncier comme identifiant des personnes. En effet, le numéro AVS relève de l'assurance sociale et son utilisation étendue comme identifiant des personnes est problématique au niveau de l'Etat de droit. L'utilisation d'un unique identifiant des personnes dans tous les domaines, aussi bien au sein de l'administration que par les entreprises privées, comporte un risque croissant de violation des droits de la personnalité des personnes concernées, puisque les diverses données peuvent être facilement combinées et que des profils de personnalité illicites peuvent ainsi être générés. Si le numéro AVS est utilisé par le registre foncier, les propriétaires fonciers seront aussi exposés à ces risques. En revanche, l'utilisation d'un identifiant sectoriel de personnes permettrait, d'une part, d'identifier les propriétaires fonciers de manière fiable et, d'autre part, d'éviter des risques de combinaisons de données. Cette variante a été mise en œuvre aussi bien pour le registre du commerce que pour le dossier électronique du patient, si bien qu'il est difficile de comprendre pourquoi une telle solution ne devrait pas être appliquée au registre foncier. La Commission s'est également exprimée contre la création d'une banque centrale de données regroupant les propriétaires fonciers. En effet, en cas de mise en œuvre d'un identifiant sectoriel des personnes, aucune banque centrale n'est nécessaire. Une telle solution, sans banque centrale de données, répond au principe de la proportionnalité ainsi qu'aux exigences de la protection de la liberté personnelle et de la sphère privée.

Avant-projet de Loi sur l'enseignement secondaire supérieur LESS
Des travaux de révision de la Loi sur l'enseignement secondaire supérieur ont été entrepris afin de tenir compte des modifications intervenues sur le plan fédéral et cantonal ainsi que des nouvelles filières d'études ouvertes à Fribourg. Conçue comme une loi-cadre, la future loi définira les grandes orientations de l'école et fixera les grandes lignes des buts de l'enseignement et l'organisation des écoles. Au

stade de la procédure de consultation y relative, la Commission a rappelé que les données ou fichiers des élèves traités afin d'établir des statistiques ou de servir à des fins de recherches scientifiques doivent être anonymisés, conformément aux dispositions de la Loi sur la protection des données. La Commission estime que la disposition relative au contenu, aux modalités d'accès, de transmission et de destruction des banques de données ou des fichiers est trop vague, ne satisfaisant pas les exigences d'une base légale formelle. Concernant la procédure d'appel, la Commission souligne qu'il s'agit d'un mode de communication automatisé des données qui nécessite des mesures techniques et organisationnelles supplémentaires, et doit être documentée dans un règlement d'utilisation. Ce dernier doit notamment préciser les personnes autorisées à accéder aux données, les données mises à leur disposition, la fréquence des interrogations, la procédure d'authentification, les autres mesures de sécurité ainsi que les mesures de contrôle.

Droit d'exécution relatif à la Loi fédérale sur l'enregistrement des maladies oncologiques
Dans le cadre de la consultation fédérale concernant le droit d'exécution relatif à la Loi sur l'enregistrement des maladies oncologiques, la Commission a rappelé que l'organe public qui fait traiter des données personnelles par un tiers demeure responsable de la protection des données et doit notamment donner au mandataire les instructions nécessaires et veiller à ce que celui-ci n'utilise les données ou ne les communique que pour l'exécution du mandat. Elle a également souligné la nécessité et l'importance du chiffrement des données lors de leur transmission et stockage, notamment dans la mesure où des données sensibles sont traitées et que la clé de chiffrement doit se trouver auprès du mandant et non du mandataire. En outre, si le patient n'a pas fait opposition à la transmission de ses données dans les trois mois suivant l'information du médecin, il peut demander, en tout temps, la radiation de ses données du registre concerné.

Révision de la LPers – contrôle du casier judiciaire avant l'engagement – amendement Commission parlementaire
Dans le cadre du projet de révision de la Loi sur le personnel (LPers), l'Autorité a pris position une première fois lors de la procédure de consultation. En effet, l'entrée en vigueur le 1er janvier 2015 de l'article 371a du Code pénal (CP) a introduit un extrait «spécial» du casier judiciaire sur la base duquel les employeurs peuvent vérifier si une interdiction d'exercer une activité professionnelle a été prononcée à l'encontre du candidat ou de la candidate retenu-e pour un poste en lien avec des mineurs. Dans son Message, le Conseil d'Etat incorpore dans la LPers l'obligation de consulter cet extrait «spécial» du casier judiciaire avant l'engagement de tout employé de l'Etat ayant une activité impliquant des contacts réguliers avec des mineur-e-s. À titre de solution transitoire, il recommandait une période de dix ans pendant laquelle le candidat ou la candidate à un poste en lien avec des mineur-e-s devrait produire un extrait «ordinaire» de son casier judiciaire, en plus de l'extrait «spécial»[12]. De l'avis de l'Autorité, la durée de dix ans du régime transitoire consistant à un contrôle systématique du casier judiciaire ordinaire pour le personnel travaillant avec des mineurs est problématique et contraire aux principes de finalité et de proportionnalité. Lors de la séance de la Commission parlementaire, un amendement a été voté selon lequel cette période devait être prolongée (de 15 ans) pour atteindre 25 ans en tout. Dans sa réponse à la consultation, la Commission a reconnu l'intérêt de l'Etat-employeur à avoir connaissance des infractions commises en incompatibilité avec la fonction envisagée et d'instaurer une période transitoire. Cependant, l'Autorité est d'avis que la prolongation de la période de transition de 10 à 25 ans est contraire au principe de la proportionnalité et par là non conforme à la législation sur la protection des données.

[12] http://www.parlinfo.fr.ch/dl.php/fr/ax-59d476768b681/fr_MES_2016-DFIN-16.pdf

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.

Durant l'année sous rapport, le projet d'une corporation ecclésiastique dans la perspective de la création d'une plateforme électronique vouée à la gestion des divers registres ecclésiastiques a été à nouveau un dossier important. Faisant suite à sa propre recommandation de 2016, la Commission s'est occupée du projet remanié au cours de plusieurs séances. Elle a approuvé sur le fond la création de la plateforme, à condition que le numéro AVS (NAVS13) ne soit pas utilisé pour la consultation et la mise en lien des registres respectifs; le NAVS13 ne peut être indiqué et consulté que dans le registre des membres. En outre, la Commission exige que la plateforme mentionnée soit hébergée par le SITel, et que la corporation, dans le cadre de son activité de surveillance, définisse et contrôle les exigences que doivent remplir les diverses communes ecclésiastiques en matière de sécurité informatique. L'accompagnement du projet mentionné et des dossiers par les spécialistes informatiques de la Commission s'est révélé extrêmement précieux, car il faut également prendre en compte des aspects techniques en matière de projets informatiques.

L'utilisation du NAVS13 fut à nouveau un thème crucial pour la Commission. Celle-ci est préoccupée par les tendances à l'utilisation universelle du numéro prévu initialement à des fins relevant exclusivement du droit des assurances sociales. Aujourd'hui, le NAVS13 est non seulement utilisé dans le domaine des assurances sociales, mais aussi - notamment - dans ceux de l'école, de l'aide sociale, des statistiques, du contrôle des habitants, des impôts ou du registre foncier. Dans un courrier adressé au Conseil d'Etat, la Commission a fait remarquer que l'utilisation du NAVS13 en tant que facteur d'identification universel comporte un grand risque d'atteinte à la personnalité des individus concernés. Ainsi, le NAVS13 permettrait aisément de relier entre eux les divers registres et d'établir de véritables profils personnels.

Enfin, la Commission s'est exprimée au sujet de l'externalisation de traitements de données dans des clouds. Elle est d'avis qu'une base légale suffisante fait défaut pour une externalisation dans l'esprit mentionné. Pour le traitement et l'hébergement des données, elle recommande de développer, pour des organes publics, des clouds fribourgeois, romands ou nationaux. Ce n'est que de la sorte que l'Etat gardera la maîtrise et le contrôle de toutes les données qu'il traite. Les citoyens ont l'obligation de confier leurs données à l'Etat; c'est pourquoi celui-ci devrait veiller au traitement de ces données en conformité avec le droit et à la garantie de leur sécurité en tout temps. Enfin, l'organe public demeure responsable, envers le citoyen concerné, du respect des dispositions du droit de la protection des données et répond de toute violation éventuelle.

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, 48 demandes d'accès ont été déposées auprès des organes publics fribourgeois en 2017. Dans 33 cas, les organes publics ont accordé un accès complet et dans 4 cas un accès restreint. Dans 2 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 de l'environnement, de l'administration et des constructions.

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 2017 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 2017, la Commission a reçu une copie de 13 décisions, toutes émanant de la Police cantonale (principalement des demandes d'effacement de données et d'accès). 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.

2. Recommandations

La Commission n'a fait aucune recommandation durant l'année sous rapport.

III. Activités principales des Préposées

A. Transparence

1. Points forts

1.1 Médiations dans le domaine du droit d'accès

En 2017, onze requêtes en médiation ont été déposées auprès de la Préposée à la transparence. Dans sept cas, un accord est intervenu et dans un autre, la Préposée a émis une recommandation.

La première requête en médiation émanait d'un citoyen qui avait exigé, à la commune de Cottens, l'accès aux **documents de soumission** déposés par quatre entreprises, dans le cadre d'un projet de construction communal. La commune avait refusé l'accès car, à son avis, il s'agissait de garantir la confidentialité de tels documents, selon le Règlement sur les marchés publics (RMP) et l'Accord intercantonal sur les marchés publics (AIMP). A réception de la requête en médiation, il était connu que trois des quatre documents avaient déjà été détruits par le bureau d'ingénieurs chargé du projet. Au cours de la séance de médiation, les parties se sont finalement mises d'accord sur l'accès à une partie des documents se trouvant encore dans le dossier.

La deuxième requête en médiation fut émise par un journaliste qui désirait l'accès à un document permettant de constater quel était le **rapport entre la Police cantonale fribourgeoise et ses informateurs privés,** ainsi que la façon dont était réglée la rémunération de ces derniers. De plus, le journaliste exigeait de pouvoir consulter le **budget annuel** y relatif de la Police cantonale. Sa demande d'accès fut rejetée au motif que la consultation des documents exigés portait atteinte à la sécurité publique. Aux yeux de la Préposée à la transparence dans le cas concret, la disposition d'exception de la LInf citée ne justifiait cependant pas un refus total de la demande d'accès. Dans sa recommandation, elle a relevé au contraire que certaines parties du document en question devaient être rendues accessibles et que la Police cantonale devait caviarder les passages tombant sous le coup de la disposition d'exception. Quant au budget annuel de la Police cantonale pour la rémunération de ses informateurs privés, la Préposée à la transparence a recommandé d'y accorder l'accès intégral. La Police cantonale est restée sur sa position, raison pour laquelle le journaliste a déposé recours.

La troisième requête en médiation provenait d'une journaliste qui, s'agissant de la centrale d'appel sanitaire d'urgence 144 du canton de Fribourg, avait reçu une réponse négative de l'organe public à sa demande d'accès à **l'index de la banque de données du système de gestion des appels de la centrale.** Durant la séance de médiation, les parties se sont finalement entendues sur l'accès à l'index d'une seule statistique qui se trouve dans la banque de données mentionnée.

La quatrième requête en médiation émanait d'un citoyen désirant l'accès à des **plans d'un arrêt de bus** en ville de Fribourg, plans datant des années 1907 et 1937. La ville a rejeté la demande et le citoyen a donc déposé une requête en médiation. La Préposée à la transparence a pris contact avec le service compétent de la ville à la suite de quoi, celui-ci s'est déclaré prêt à accorder l'accès. Les plans en question étaient tellement anciens, et vu que le délai de protection des archives était échu, ce n'était pas la LInf qui était applicable, mais bien la Loi sur l'archivage et les Archives de l'Etat.

Dans un autre cas, il s'agissait de la **copie d'un enregistrement audio** que la commune de Cressier avait effectué à l'occasion d'une séance d'information concernant la fusion du cercle scolaire avec la commune de Morat. La commune avait communiqué aux citoyens concernés qu'elle ne pouvait remettre aucune copie en raison des tierces personnes impliquées, mais que l'enregistrement pouvait

être écouté à la commune. Suite à cette réponse, le citoyen a déposé une requête en médiation. La Préposée à la transparence a expliqué au citoyen que les particuliers intéressés dans le présent cas pouvaient s'opposer effectivement à l'accès au document. Le citoyen s'est déclaré satisfait avec les passages de l'enregistrement concernant les représentants de la commune et du canton.

Deux autres requêtes en médiation ont été déposées par deux journalistes qui avaient exigé de la Direction de l'économie et de l'emploi un accès à un **rapport d'audit** relatif aux remontées mécaniques de Val-de-Charmey. La Direction de l'économie et de l'emploi voulait caviarder certains passages afin de tenir compte de la protection de la personnalité et du secret d'affaires. Les journalistes n'étaient pas d'accord avec ce mode de faire et se sont donc adressés à l'Autorité. Lors de la séance de médiation, les parties ont fini par se mettre d'accord sur un caviardage plus léger que prévu initialement par la Direction de l'économie et de l'emploi.

Dans le huitième cas, il s'agissait de l'accès aux **procès-verbaux** des **séances du conseil communal** de Val-de-Charmey portant sur une certaine période. La présidente d'une association de loisirs avait demandé ces procès-verbaux, car durant cette période, une décision concernant cette association avait été rendue. Dans sa réponse de refus, la commune se référait au fait que des protocoles de séances non publiques n'étaient pas accessibles selon la LInf. La Préposée à la transparence a confirmé ce point de vue, mais a indiqué à l'association que, se basant sur la Loi sur la protection des données, elle pouvait exiger l'accès au passage la concernant.

La neuvième requête en médiation a été déposée par un journaliste qui avait exigé de toutes les communes fribourgeoises l'accès à leur **règlement d'organisation** et avait essuyé un refus de celle de Ferpicloz. La Préposée à la transparence a fait remarquer à ladite commune que non seulement le règlement d'organisation devait être accessible en vertu du Règlement d'exécution de la Loi sur les communes, mais qu'il devait même figurer sur le site Internet des communes. Sur quoi, la commune a permis au journaliste d'accéder au document souhaité.

La dixième requête en médiation portait sur l'accès à des **dossiers de subventionnement** d'organisateurs de manifestations culturelles. Une association culturelle avait exigé de l'Agglomération de Fribourg l'accès à la liste de tous les bénéficiaires de subventions culturelles entre 2010 et 2017, ainsi qu'aux montants qui leur avaient été alloués, aux dossiers qu'ils avaient déposés et aux positions de refus partiel ou total notifiées durant la même période. Comme l'association en question n'a obtenu qu'une partie des documents désirés, elle a déposé via son avocat une requête en médiation. Le cas était encore pendant à la fin de l'année sous rapport.

Dans le onzième cas, il s'agissait de l'accès à une série de documents dans le **domaine environnemental** qu'une personne privée avait demandé à plusieurs organes de l'administration cantonale. N'ayant pas reçu de réponse dans le délai imparti par la loi, elle s'est adressée à l'Autorité. Ce cas était encore pendant à la fin de l'année sous rapport.

1.2 Médiation dans le cadre de la Loi sur la médiation administrative

En tant que remplaçante du Médiateur cantonal, la Préposée à la transparence a traité un dossier au vu de la récusation du Médiateur. Comme la rencontre avec les deux parties n'a pas abouti à une séance de médiation ni à un accord, la Préposée a analysé les documents à sa disposition et a donné au citoyen concerné, via son avocat, son appréciation du cas ainsi qu'un conseil.

1.3 Demandes

Durant l'année sous rapport, des citoyennes et citoyens de même que des organes publics ont à nouveau pris régulièrement contact avec la Préposée à la transparence afin d'obtenir des informations sur leurs droits et obligations en rapport avec le droit d'accès. L'éventail des documents suscitant de l'intérêt était très large, comme les années précédentes: ainsi s'est-il agi, hormis les documents déjà mentionnés en rapport avec les médiations, de procès-verbaux d'une commission, de dossiers de permis de construire, d'une convention intercommunale, d'une convention d'une commune avec un particulier au sujet d'un changement d'affectation de zones, des détails d'une comptabilité, des statuts d'une association, d'un rapport adressé à une commune par un bureau d'ingénieurs ainsi que du règlement d'organisation d'un conseil communal.

Souvent, des tiers étaient impliqués et les organes voulaient se renseigner sur la manière de procéder requise. La Préposée à la transparence a précisé aux organes publics qu'un tiers concerné par une demande d'accès devait généralement être consulté afin d'obtenir son point de vue (art. 32 al. 2 LInf). Si le tiers en question est d'accord et si rien ne s'oppose à la publication du document de la part de l'organe public, l'accès doit être accordé. Si par contre le tiers s'oppose, l'organe public doit examiner si l'accès doit donc être refusé, ou s'il voudrait quand même accorder l'accès parce que l'intérêt public à l'accès aux documents serait à son avis prépondérant. Le cas échéant, le tiers devrait être informé de l'intention de l'organe public d'accorder l'accès, et il aurait 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).

En 2017 encore, la Préposée à la transparence a souligné régulièrement, dans les cas particuliers qui lui étaient soumis, les limites de sa fonction. Elle peut donner des renseignements d'ordre général en matière de transparence, mais elle ne peut prendre une position détaillée dans des cas concrets. La formulation d'une recommandation demeure réservée à une éventuelle phase de médiation au sens de l'article 33 LInf. La Préposée à la transparence doit demeurer aussi neutre que possible avant cette étape.

1.4 Adaptation de l'Ordonnance sur l'accès aux documents

Après l'adaptation de la LInf à la Convention du 25 juin 1988 sur l'accès à l'information, la participation et l'accès à la justice en matière d'environnement (Convention d'Aarhus) en 2016, c'est l'Ordonnance sur l'accès aux documents (OAD) qui a été adaptée l'année suivante.

L'introduction dans la loi du principe de l'interprétation conforme à la Convention d'Aarhus a permis de faire l'économie de plusieurs modifications de détail dans l'OAD. Certaines adaptations restaient toutefois nécessaires, d'abord parce que les modifications apportées par le législateur n'étaient pas limitées au seul domaine de l'environnement, ensuite en raison des changements d'ordre procédural qui devaient être précisés au niveau de l'ordonnance. De plus, quelques ajustements de l'ordonnance tiennent compte de la pratique des six premières années d'application de la législation sur l'accès aux documents.

L'OAD ayant été conçue en fonction des notions d'*organes publics* au sens strict et de documents *officiels,* il a fallu introduire deux nouvelles dispositions permettant de faire le lien avec les notions nouvelles de *personnes privées assimilées à des organes publics* et *d'information sur l'environnement.* De même, l'attribution d'une compétence décisionnelle à l'Autorité cantonale de la transparence et de la protection des données et la question des délais spéciaux en lien avec les demandes d'accès à des informations sur l'environnement constituent des changements d'ordre procédural qu'il était nécessaire de concrétiser dans l'ordonnance.

Parmi les ajustements qui visent à tenir compte de la pratique et à simplifier le travail des organes publics se trouve l'accès facilité aux documents qui ont déjà fait l'objet d'une diffusion auprès du public. La notion de *document achevé* a été précisée de manière à ce qu'elle couvre également les documents émanant de tiers. De plus, la liste des exceptions à l'obligation de consulter les tiers concernés a été complétée et clarifiée. Finalement, une nouvelle disposition a été ajoutée qui concerne le devoir de collaboration des parties à la phase de médiation.

2. Statistiques

Durant la période considérée, 95 dossiers ont été introduits, dont 10 sont pendants au 1er janvier 2018. 26 conseils et renseignements, 2 avis, 29 examens de dispositions législatives, 12 présentations, 10 participations à des séances et autres manifestations, 11 demandes en médiation et 5 demandes diverses. 47 dossiers concernent des organes cantonaux ou des institutions chargées de tâches publiques, 8 des communes et paroisses, 19 d'autres organismes publics (cantons, autorités de transparence et protection des données), 14 des particuliers ou institutions privées et 7 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.
Divers dossiers concernaient des questions préliminaires du SITel à propos de projets actuels de traitement de données, par exemple dans le cadre de la mise en œuvre du guichet virtuel de cyberadministration, du portail scolaire «Primeo», de la refonte du concept de l'application destinée au registre fiscal, ou l'introduction d'une nouvelle version du système de recherche de la police pour les applications du DFJP ou de FRI-PERS. Des entretiens ont également eu lieu à propos de la participation générale de l'Autorité à des projets actuels de traitement de données ou à des projets informatiques. Diverses demandes avaient pour objet la plateforme informatique cantonale contenant les données des registres des habitants (FRI-PERS) (cf. également 1.3).
Sous le terme «Cybersanté», il faut entendre le projet de mise en œuvre de la Loi sur le dossier électronique du patient. Les unités d'organisation, les dénommées communautés et communautés de référence doivent définir les conditions techniques et organisationnelles de l'introduction du dossier électronique du patient. Le canton envisage d'apporter sa contribution à la création des conditions cadres nécessaires à cet effet. La Préposée à la protection des données est membre du groupe d'accompagnement du projet et a participé à plusieurs séances l'an passé.

Durant l'année sous rapport, 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. Règlements, documents, descriptifs de projet devaient être examinés de façon critique, dans l'esprit des recommandations de la Commission, en particulier sur le point de savoir si les exigences de celle-ci ont été prises en considération. La Commission a ainsi traité plusieurs dossiers lors de 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 intercantonale de données
Transfert des appels du 144 du Jura sur Fribourg
Suite à un appel d'offre, le canton du Jura a décidé d'externaliser ses appels sanitaires urgents (144) vers le canton de Fribourg. Dans ce contexte, l'Autorité a été approchée et le contenu de la Convention ainsi que de son avenant a été analysé. Il est relevé que la Convention doit notamment mentionner la confidentialité. En effet, chaque collaborateur du centre d'appels doit signer une clause de confidentialité. Quant à l'avenant, ce dernier règle les modalités relatives à l'hébergement des données, la durée de leur conservation, la finalité, la portabilité des données, la responsabilité, l'externalisation, l'accessibilité, le droit d'accès, les contrôles et la sécurité des données. Concernant les contrôles, les Préposés des deux cantons respectifs sont habilités à en faire. Toutefois, seul l'accès aux données des interventions effectuées sur leur territoire peut être octroyé. En outre, chaque canton déclare ses fichiers à l'Autorité cantonale compétente.

Communication de données par un service à un autre
Communication de données du Service cantonal des contributions à l'Office des poursuites
L'Office des poursuites (OP) souhaite obtenir un accès direct informatisé à certaines données du registre du Service cantonal des contributions (SCC) pour pouvoir consulter les renseignements relatifs aux débiteurs sans devoir au préalables requérir l'aide du service. Le SCC propose un accès direct informatisé aux avis de taxation via la plateforme informatique Platcom. En effet, l'article 91 alinéa 5 de la Loi sur la poursuite des dettes et la faillite dispose que le SCC est tenu de renseigner l'OP sur demande.

Dans ce cas d'espèce, l'Autorité est d'avis que l'accès direct informatisé via Platcom représente une procédure d'appel, soit un mode de communication automatisé des données par lequel les destinataires, en vertu d'une autorisation du responsable du fichier, décident de leur propre chef et, sans contrôle préalable, du moment et de l'étendue de la communication. Elle rappelle qu'une base légale au sens formel est nécessaire pour la mise en place de ce procédé, dans la mesure où les avis de taxation contiennent des données sensibles. En outre, toute procédure d'appel doit être documentée dans un règlement d'utilisation, lequel doit préciser notamment qui sont les personnes autorisées à accéder aux données, les données mises à disposition, la fréquence des demandes d'informations, la procédure d'identification, les mesures de sécurité et celles de contrôle. L'Autorité a conclu que la base légale faisait alors défaut.

Communication de données personnelles par les communes
Transmission à une assurance privée de la liste des habitants d'une commune par quartier et par rue
Le Service du contrôle des habitants d'une commune a contacté l'Autorité afin de savoir s'il est autorisé, du point de vue de la protection des données, à transmettre les adresses des personnes domiciliées dans sa commune par quartier et par rue à une assurance privée. En matière de contrôle des habitants, la Loi sur le contrôle des habitants (LCH) s'applique à la transmission des données et prévoit que la communication de données relatives à une pluralité de personnes définie par un critère général est interdite. Cependant, la communication des noms, prénom(s), date de naissance et adresse peut être autorisée par le conseil communal si l'utilisation de ces informations est destinée à des fins idéales dignes d'être soutenues. De l'avis de l'Autorité, l'intérêt de l'assurance privée étant, en

l'espèce, purement commercial, la condition de l'utilisation des données à des fins idéales dignes d'être soutenues n'est pas remplie. Par conséquent, la transmission des données sollicitées n'est pas admissible au regard de la protection des données.

Transmission à des entreprises de démarchage de données relatives à des projets de construction
L'Autorité a été consultée par une commune pour savoir s'il est conforme à la protection des données de fournir à une revue spécialisée dans la construction des informations au sujet de demandes de permis de construire en cours de procédure. L'Autorité l'informe que, selon l'avancée de la procédure, plusieurs cas de figure se posent entrainant ainsi l'application de différentes lois.

Lorsque la mise à l'enquête publique est terminée et que la procédure de permis de construire est en cours, l'autorité statue en première instance, de sorte que la LPrD s'applique. Les données ne peuvent être communiquées que dans les trois hypothèses suivantes: une disposition légale le prévoit; la personne privée qui demande la transmission des données justifie un intérêt à la communication primant sur celui de la personne concernée qui a avantage à ce que les données ne soient pas communiquées, la personne concernée a donné son consentement à la transmission. Si l'autorité statue sur recours, ce sont les dispositions du Code de procédure et de juridiction administrative (CPJA) qui sont applicables. Enfin, lorsque la procédure de permis de construire est close et que le permis est entré en force (il n'y a plus aucun moyen de recours contre cette décision), la LInf s'applique et l'accès se fait au moyen de la demande de renseignements (art. 8ss LInf). Cependant, dans le cas des données personnelles, le consentement de la personne concernée à ce que l'information soit communiquée doit être obtenu préalablement. Par mesure de simplification, l'Autorité souligne que les entreprises de démarchage peuvent obtenir ces informations directement auprès des personnes concernées.

Transmission des changements d'adresse des donateurs d'une organisation à but caritatif fribourgeoise
Le Service du contrôle des habitants d'une commune s'est adressé à l'Autorité pour savoir s'il est admissible, du point de vue de la protection des données, de communiquer à une association à but caritatif les nouvelles adresses de ses donateurs (suite à un changement d'adresse).

L'Autorité rappelle que le conseil communal peut autoriser la communication pour autant que les données de personnes définies par un critère général prévoient d'être utilisées à des fins idéales dignes d'être soutenues. En revanche, tout autre communication de données relatives à une pluralité de personnes définies par un critère général est interdite. L'Autorité est d'avis que dans la mesure où l'association caritative souhaite utiliser ces adresses dans un but commercial, la communication n'est pas admise.

Demande de consultation des archives communales
Une commune s'est adressée à l'Autorité pour savoir s'il est admissible, du point de vue de la protection des données, d'accorder un libre accès aux archives communales à un privé pour des recherches concernant sa famille entre 1850 et 1930. L'Autorité est d'avis qu'étant donné que, dans le cas d'espèce, les documents et archives visés remontent loin dans le temps, le délai de protection ordinaire de 30 ans est largement dépassé. Dès lors, la consultation de ces documents est libre, à l'exception des documents classés selon les noms de personnes ou contenant des données personnelles sensibles. En revanche, la demande de l'intéressé visant à obtenir les clés des archives communales afin de pouvoir parcourir librement les documents n'est pas recommandée. En effet, la commune reste responsable de l'accès à ses archives.

Accès aux décisions de la Commission sociale par les communes
L'Autorité a été consultée concernant l'accès de tous les conseillers communaux et du personnel administratif d'une commune aux décisions de la Commission sociale concernant l'attribution de l'aide matérielle.

Dans la mesure où les données figurant dans la décision de la Commission sociale sont des données sensibles soumises à un devoir de protection accrue et confidentielles, il appartient à la commune de domicile du bénéficiaire de l'aide sociale de s'assurer que la décision soit communiquée uniquement aux personnes traitant des affaires sociales et non à tout le personnel administratif et tous les conseillers communaux. Ainsi, peuvent avoir accès à ces décisions, le conseiller communal en charge des affaires sociales et le collaborateur administratif dont les tâches relatives aux affaires sociales sont fixées dans son cahier des charges (art. 72 LCo). Le fait de rendre ces décisions accessibles aux autres collaborateurs peut s'apparenter à une atteinte à la personnalité des personnes concernées et à une violation du secret de fonction.

Accès aux dossiers des candidatures de la Commission des naturalisations
Une commune s'est adressée à l'Autorité pour savoir si, lors de la procédure de naturalisation, des étudiants participant à un projet de recherche peuvent avoir accès aux dossiers de candidats, assister aux auditions, aux délibérations de la Commission des naturalisations ainsi qu'aux cours d'instruction civique dispensés aux candidats.

Selon l'Autorité, pour qu'un tel accès soit autorisé, il faut que plusieurs précautions soient prises en raison de la sensibilité des données à traiter. Premièrement, les chercheurs doivent fournir un descriptif de projet fournissant une série d'informations relatives notamment aux catégories de données traitées, à l'accès à celles-ci, à la liste des personnes y ayant accès ou aux mesures de sécurité prises, à la conservation etc. Deuxièmement, une clause de confidentialité doit être signée par les personnes responsables de la recherche ainsi que par le professeur. Troisièmement, dans le cas d'espèce, les données contenues dans les dossiers doivent être anonymisées et les personnes concernées doivent consentir à ce que les étudiants assistent à des entretiens.

Protection des données et travail
Transmission de documents du dossier personnel d'un ancien collaborateur à la Caisse publique de chômage
Une institution cantonale souhaite savoir s'il est admissible, du point de vue de la protection des données, de communiquer à la Caisse publique de chômage les documents concernant les motifs exacts de la perte d'emploi ainsi que les éventuels avertissements et procès-verbaux d'entretien d'un ancien collaborateur.

En application de la Loi sur la protection des données (LPrD), la communication de données personnelles est admissible uniquement si une base légale le prévoit. Bien que l'article 28 alinéa 3 LPGA dispose que le requérant est tenu d'autoriser, dans des cas particuliers, toutes les personnes et institutions notamment les employeurs à fournir des renseignements, pour autant que ceux-ci soient nécessaires pour établir le droit aux prestations, l'article 88 alinéa 1 lettre d LACI prévoit quant à lui que les employeurs se soumettent à leurs obligations légales d'informer et de renseigner. Ainsi, en dérogation de l'article 28 alinéa 3 LPGA, l'employeur peut être amené à devoir transmettre

des informations relatives aux rapports de travail à la Caisse de chômage sans avoir besoin du consentement préalable de la personne concernée. Cependant, l'ex-employeur devra appliquer le principe de la proportionnalité et fournir uniquement les informations et documents dont la Caisse de chômage a besoin pour établir ou déterminer le droit aux prestations de l'assuré.

Questions relatives au questionnaire médical à remplir lors d'un engagement à l'Etat de Fribourg
Les employés de l'Etat de Fribourg doivent répondre à toutes les questions contenues dans le questionnaire médical d'embauche afin que le médecin-conseil déclare si le candidat engagé présente un état de santé satisfaisant ou non et afin qu'il détermine son degré de risque accru d'incapacité et d'invalidité. Le questionnaire comporte une série de questions détaillées sur l'état de santé et les antécédents du candidat choisi.

Les données personnelles sur la santé sont des données sensibles (cf. art. 3 let. c LPrD), qui doivent être traitées avec un devoir de diligence accru (art. 8 LPrD). La législation sur le personnel de l'Etat ne règle pas spécifiquement le contenu du questionnaire médical. Selon le Code des obligations (art. 328b CO), l'employeur ne peut traiter les données concernant le travailleur que dans la mesure où celles-ci portent sur les aptitudes de celui-ci à remplir ses tâches ou sont nécessaires à l'exécution du contrat de travail.

Dans l'ensemble, l'Autorité est d'avis que l'Etat de Fribourg, en sa qualité d'employeur, respecte les exigences légales de la collecte des données. En effet, les données collectées au moyen d'un questionnaire l'ont été directement auprès de la personne concernée. De plus, une base légale au sens formel justifie le traitement des données sensibles et le principe de la finalité a été respecté. Toutefois, le candidat n'est pas obligé d'informer l'Etat de Fribourg s'il est porteur d'une maladie transmissible n'ayant aucune influence sur son travail (p.ex. VIH), s'il s'estime guéri d'anciennes maladies ou si les informations sont constatables visuellement par l'employeur. En outre, l'Autorité qualifie de non conformes les demandes relatives aux maladies antérieures guéries (ou non guéries, mais sans effet sur l'exercice de l'activité), aux hospitalisations et aux cures que le candidat a subies par le passé (cf. *Protection des données,* Philippe Meier, p. 670ss).

Procédure d'engagement
Dans le cadre de la mise au concours d'un poste de Directeur de foyer, une commune a consulté l'Autorité concernant la conformité du processus d'engagement prévu au regard de la protection des données.

En l'espèce, le processus d'embauche envisagé se déroule comme suit. Les postulations sont réceptionnées au bureau communal. Puis, la Commission administrative du foyer prend connaissance des dossiers et fait un premier tri des candidatures en vue des entretiens. Une fois les candidats choisis entendus, le conseil communal engage la personne retenue.

L'Autorité relève que la commune qui souhaite transmettre les dossiers de candidature sous forme électronique aux membres de la Commission, tout en sachant que la commune n'a pas d'accès sécurisé par VPN, doit préalablement s'assurer que les mesures organisationnelles et techniques sont respectées par chacun des membres de la Commission. En ce qui concerne la transmission des dossiers de candidature sous forme papier, passant d'un membre à l'autre de la Commission, il est nécessaire que chacun de ses membres respecte les mesures organisationnelles, dans le sens par exemple que les dossiers doivent être sous clé afin d'empêcher tout tiers d'y avoir accès.

Dans un pareil cas, l'Autorité recommande de faire consulter les dossiers de candidatures par les membres de la Commission directement dans les locaux du bureau communal. Enfin, l'Autorité est d'avis que la secrétaire communale est habilitée à ouvrir les candidatures en vue de la préparation d'un dossier, permettant ainsi une consultation plus aisée par les membres de la Commission.

Protection des données et santé

Communication de données fiscales à Spitex (organisation privée d'aide et de soins à domicile)

Une commune voulait savoir si elle pouvait répondre positivement à la demande de Spitex et lui remettre les données fiscales d'un citoyen. Les éclaircissements ont montré que dans le droit cantonal, il n'existe pas de base légale autorisant la communication de données fiscales à Spitex. Selon l'avis de l'Autorité, une communication sans précisions, à savoir sur quelle base légale l'organisation se fonde et à quelles fins elle a besoin de ces données, n'est pas admissible.

Enquête sur les motifs de l'hospitalisation d'habitants du canton dans des hôpitaux et établissements de santé hors canton

La Direction responsable entend adresser un questionnaire à une sélection de patients qui se sont fait soigner hors canton, afin de connaître les motifs de l'hospitalisation hors canton. L'enquête sera effectuée sous sauvegarde de l'anonymat et par une entreprise externe. Il a été demandé à l'Autorité si l'enquête envisagée tenait compte des exigences liées au droit de la protection des données. Afin de satisfaire à ces exigences dans une enquête anonymisée, celle-ci doit se fonder sur le caractère facultatif de la participation, et la Direction ne doit disposer d'aucune clé lui permettant de savoir qui a participé à l'enquête; la non-participation ne peut entraîner aucune sanction. Les personnes participant à l'enquête doivent être informées du but de celle-ci. Il y a lieu d'obliger la société externe mandatée à respecter la confidentialité.

Protection des données et sécurité informatique

Externalisation de l'hébergement, de l'exploitation et de la maintenance du site Internet du canton de Fribourg

Dans le cadre du projet du nouveau site Internet de l'Etat de Fribourg, l'Autorité a été abordée pour analyser la possibilité qu'un tiers externe à l'administration fribourgeoise héberge les données publiques traitées en lien avec le nouveau site Internet. En effet, il ressort du projet que l'hébergement de l'interface serait géré en partie par des tiers externes, le Service de l'informatique et des télécommunications de l'Etat de Fribourg ne traiterait que l'interface liée au guichet virtuel de cyberadministration. Sur la base de l'article 18 de la Loi du 25 novembre 1994 sur la protection des données, l'Autorité ne voit pas d'objection à ce que des données publiques soient externalisées. Cependant, en cas de traitement de données personnelles de la part du mandataire, le mandat devra être encadré et des clauses de confidentialité devront être conclues. En outre, il est impératif que les données soient hébergées en Suisse.

Concernant l'Intranet, il est relevé que certaines données ne sont pas publiques, mais confidentielles et soumises au secret de fonction. Ainsi, l'exigence de l'hébergement en Suisse est réitérée, dans la mesure où l'expertise de Wolfgang Wohlers met en évidence que la délocalisation à l'étranger des données personnelles traitées par l'Etat de Fribourg violerait le secret de fonction/professionnel auquel il est soumis.

Protection des données et données fiscales

Accès des paroisses à une plateforme informatique sécurisée cantonale d'échanges

La Commission a été contactée au sujet du projet offrant aux paroisses l'accès à la plateforme informatique sécurisée afin qu'elles puissent accéder aux informations des contribuables concernés. En l'occurrence, il s'agit d'une plateforme électronique qui permet à des services de l'Etat de mettre des informations à disposition de partenaires internes et externes comme les communes. L'accès est accordé sur la base d'une convention conclue entre le Service cantonal des contributions et les paroisses.

La Commission est d'avis que la communication du numéro AVS de l'administré concerné est possible, mais sous condition qu'il ne soit utilisé qu'à des fins d'actualisation des adresses et de facturation de l'impôt. Par ailleurs, ces restrictions doivent faire partie de la convention.

Protection des données et école

Conservation des données des écoliers

Dans le cadre de la révision du Règlement d'exécution de la Loi sur l'enseignement scolaire spécialisé (RES), l'Autorité a été consultée au sujet de la conservation de données d'écoliers suivant un tel enseignement. Ces données devraient être conservées pendant 10 ans après le départ des écoliers de l'institution/école, contrairement à d'autres données d'écoliers, qui sont détruites à la sortie de l'école. L'instruction de ce cas a montré que la conservation de ces données particulières, en raison des rapports accompagnant les feuilles de notes, est nécessaire à la compréhension des résultats scolaires. Il a donc été suggéré de régler de manière restrictive les droits d'accès, car ils portent sur des données très sensibles et ont de surcroît un caractère exceptionnel.

Demande de modèle d'autorisation par des parents d'élève pour la publication de photos de leurs enfants sur internet

En vue d'analyser sous l'angle de la protection des données, une commune a soumis à l'Autorité un projet de modèle d'autorisation parentale pour la publication de photographies d'enfants des écoles ou des crèches sur le site Internet de ces dernières. A titre préliminaire, l'Autorité déconseille vivement la publication de photos et de vidéos d'enfants sur Internet que ce soit à titre publicitaire ou informatif. La diffusion systématique de photographies et vidéos sur Internet doit être consentie par les parents ou le représentant légal avant d'être autorisée.

L'Autorité rappelle que chaque personne est titulaire du droit à son image. Ceci lui permet de s'opposer à sa diffusion ou de l'assortir de conditions. En outre, il est indispensable de recueillir le consentement exprès des parents ou du représentant légal pour diffuser des données personnelles d'enfants sur Internet. Il faut noter que les fichiers des enregistrements et des prises de vue doivent être accessibles uniquement à la personne responsable de la publication. De plus, il serait préférable de ne publier que des photos de groupe d'enfants et non des images individuelles et, de plus, sans identifiant. De manière proportionnelle aux circonstances du cas, un délai de destruction des enregistrements doit être communiqué. Le consentement peut être retiré à tout moment et doit être limité dans le temps. Par ailleurs, les photos et les vidéos doivent être prises par un appareil professionnel de l'institution. En effet, les collaborateurs ne peuvent pas prendre des images au moyen de leurs dispositifs privés. Enfin, l'Autorité souligne la responsabilité de l'institution dans la publication des images et relève en particulier l'absence d'intérêt public à publier des photos d'enfants.

Directives relatives à l'utilisation d'Internet et des technologies numériques dans les écoles
Suite à l'évolution des technologies, l'adoption de nouvelles directives élaborées par la Direction de l'instruction publique, de la culture et du sport (DICS) s'est révélée indispensable pour tenir compte des évolutions dans les écoles du canton, tant dans les usages (réseaux sociaux, cloud) que dans les équipements (smartphones, réseaux sans fil). L'Autorité a ainsi analysé le projet desdites directives ainsi que de sa notice explicative.

Projet d'une haute école impliquant que les étudiants soient filmés
L'Autorité a été approchée par une haute école dans le cadre d'un projet que celle-ci veut mener avec ses étudiants. Il s'agit de filmer ces derniers dans le but de traiter avec eux, au niveau pédagogique, les différentes phases d'apprentissage.

L'Autorité s'est prononcée sur le contenu de la déclaration de consentement des étudiants concernés. Elle devra notamment contenir le but des enregistrements, l'organe responsable des enregistrements et les personnes autorisées à consulter les données enregistrées. De plus, le document à faire signer devra définir la finalité du traitement, mentionner la durée de conservation des données enregistrées ainsi qu'énumérer les mesures de sécurité informatiques qui ont été prises pour protéger les données.

L'Autorité précise encore que des appareils d'enregistrement, appartenant à l'école, sont à privilégier. De plus, en cas d'utilisation de séquences à des fins de présentation externe, un consentement spécifique y relatif doit être transmis par les personnes concernées.

Divers
Demande d'un Office des poursuites d'ouvrir un compte Facebook
Un Office des poursuites souhaite savoir s'il peut ouvrir un compte Facebook dans le but de contacter certains débiteurs injoignables par les canaux usuels et de connaître notamment leur domicile, l'objectif étant d'obtenir des données personnelles que les débiteurs publient librement sur Facebook. L'Autorité a estimé que l'utilisation de Facebook, dans ce but, n'est pas conforme à la protection des données. En effet, la communication, respectivement la notification des actes de poursuites aux personnes poursuivies est réglée de manière précise par la Loi sur la poursuite pour dettes et la faillite (LP). Par ailleurs, le site Facebook n'est pas soumis aux normes techniques de sécurité appliquées aux sites officiels de l'Etat de Fribourg et l'hébergement de ses données n'est pas effectué dans un Etat dont le niveau de protection des données est adéquat. Dans l'hypothèse où l'Office des poursuites utiliserait la messagerie Facebook pour effectuer des communications liées aux poursuites, la confidentialité ne serait plus garantie. De plus, l'utilisation de Facebook peut être qualifiée comme une externalisation, dont les conditions légales ne sont ici pas remplies. L'Autorité rappelle que l'utilisation des médias sociaux ne doit pas remplacer l'activité administrative.

S'agissant de l'objectif d'obtenir des données personnelles par le biais des publications des débiteurs, l'Autorité a également estimé que l'utilisation d'un réseau social par une autorité dans ce but n'est pas appropriée, dans la mesure où d'autres moyens existent et sont plus efficaces, en particulier l'utilisation de la plateforme FRI-PERS. L'Autorité a également relevé la problématique de la preuve et d'une éventuelle violation du secret de fonction liée à l'utilisation de Facebook dans ce contexte, puisque l'entreprise elle-même a connaissance des consultations des profils et des notifications transmises.

Demande d'accès aux données des autres offices des poursuites du canton sur la plateforme THEMIS
Les offices des poursuites du canton de Fribourg utilisent l'application informatique THEMIS qui leur permet d'accéder aux données des débiteurs de leur district respectif. Dans le but de simplifier le travail des différents offices, l'Autorité a été consultée pour savoir si un accès à l'ensemble des données du canton disponibles sur THEMIS était possible.

En effet, une telle demande d'accès illimitée aux informations contenues sur la plateforme THEMIS pour chaque office du canton correspond à une procédure d'appel. Cette procédure répond à des conditions légales strictes. Notamment une base légale au sens formel est nécessaire, d'autant plus qu'il s'agit de données sensibles. S'agissant de l'article 91 de la Loi fédérale sur la poursuite pour dettes et la faillite, l'Autorité est d'avis qu'il permet uniquement un accès spécifique à des données du débiteur dans un cas d'espèce et ne permet pas un accès systématique.

Installation d'un sas de sécurité à l'entrée d'un tribunal d'arrondissement du canton de Fribourg
L'Autorité a été consultée dans le contexte d'un projet de renforcement de la sécurité d'un tribunal d'arrondissement. La question posée était de savoir s'il est admissible, du point de vue de la protection des données, de demander aux personnes venant assister aux audiences publiques de présenter une pièce d'identité, de relever leur identité et de les conserver dans un cahier. En principe, les débats publics sont censés rester accessibles à tous.

Selon l'avis de l'Autorité, il est cependant admissible de procéder à un contrôle d'identité du public à l'entrée du tribunal, soit par le dépôt des pièces d'identité à l'entrée, soit par la création et la gestion d'une liste des visiteurs. Toutefois, celle-ci doit être détruite à la fin de la séance, respectivement à la fin d'une courte période définie. En effet, celle-ci est admise uniquement pour assurer la police de l'audience (cf. art. 63 CPP). Enfin, l'Autorité recommande de faire déposer aux visiteurs leurs sacs et téléphones portables dans des casiers à l'entrée du bâtiment afin de prévenir le risque d'enregistrements durant les séances.

Travaux divers
Obligation de garder le secret de fonction
La Préposée a rédigé une déclaration d'engagement pour le personnel ayant accès à des données à caractère personnel. Cette déclaration peut être obtenue auprès de l'Autorité.

Révision de la Loi cantonale sur la protection des données
Au plan cantonal, il y a lieu également d'examiner si la Loi cantonale sur la protection des données et son ordonnance d'exécution doivent aussi faire l'objet d'une adaptation en raison de la révision du droit de l'UE sur la protection des données et de la révision du droit fédéral. La Préposée à la protection des données a été chargée de la direction des travaux en question. Un groupe de travail a commencé son travail.

Accès aux archives communales en lien avec les mesures de coercition à des fins d'assistance – enfants placés
Suite à l'entrée en vigueur en avril dernier de la législation fédérale permettant aux anciens enfants placés et aux internés administratifs avant 1981 de demander le versement de prestations financières à titre de réparation, l'Autorité a collaboré avec d'autres services cantonaux pour établir une brochure informative au sujet de l'accès aux archives communales en lien avec les mesures de coercition à des fins d'assistance.

La nouvelle loi crée un droit d'accès spécial en faveur des personnes concernées, de leurs proches, mais aussi des chercheurs, et réunit ainsi dans une seule et même institution différentes règles provenant des législations sur la protection des données, sur l'accès aux documents et sur l'archivage, afin de permettre un accès le plus large possible aux personnes autorisées. Le droit d'accès spécial existe en parallèle des autres droits d'accès prévus par la législation cantonale, il ne se substitue pas à eux.

Les responsables des archives ont le devoir d'aider les victimes et leurs proches à retrouver les documents en lien avec la mesure qui les concerne. L'accès aux dossiers doit être aisé et gratuit. De plus, l'intérêt de toute personne qui remplit les conditions d'accès au sens de la loi l'emporte toujours sur l'existence d'un éventuel intérêt public au maintien du secret des documents visés (p. ex. le secret des procès-verbaux du conseil communal ne peut pas être invoqué par les communes).

1.2 Contrôles

La Préposée à la protection des données a procédé, d'entente avec la Commission, à trois contrôles de grande envergure en matière de protection des données. Ont été contrôlées deux unités auprès de la Direction de la sécurité et de la justice DSJ ainsi qu'une commune. Ces contrôles ont duré plusieurs jours. Il a été fait appel à nouveau à une société externe pour effectuer les contrôles, étant précisé que la Préposée à la protection des données a été présente pendant tous les contrôles. Il convient de relever en particulier la bonne coopération des responsables et des collaborateurs.

L'un des contrôles qui a eu lieu auprès d'une unité de la DSJ a pu être achevé, l'autre a été effectué mais le rapport n'est pas encore disponible. Il est apparu que les collaborateurs sont, dans l'ensemble, sensibilisés aux questions du droit de la protection des données. Dans les limites fixées par l'étendue du contrôle, le rapport de la première unité a souligné notamment le besoin d'agir sur les points suivants: il manque des directives ou règlements internes pour l'utilisation d'outils privés à des fins professionnelles, les mots de passe pour l'accès au système d'exploitation comme à l'application propre au domaine concerné devraient pouvoir être impérativement modifiés par l'utilisateur, la gestion des autorisations d'accès est insuffisante. Les collaborateurs devraient avoir accès exclusivement aux données dont ils ont besoin pour effectuer leurs tâches. A plus d'une reprise, même dans d'autres domaines, il a été constaté que dans l'administration cantonale, la possibilité d'échanger des mails en toute sécurité avec des personnes de l'extérieur ne disposant pas d'une adresse mail de l'administration cantonale fait défaut (pas de moyens de cryptage). L'hébergement de données auprès de sociétés externes s'avère toujours aussi problématique (gestion des autorisations, clauses de confidentialité). Il n'a pas été possible d'achever avant la fin de l'année le contrôle de la deuxième unité. La mise en œuvre des propositions et recommandations sera vérifiée lors de contrôles subséquents.

Le contrôle d'une commune s'est effectué sur deux jours. Il convient de relever les points principaux du rapport: les mots de passe ainsi que leur gestion sont peu sûrs et par conséquent insuffisants, la gestion des autorisations d'accès est elle aussi insuffisante, par ailleurs des clauses de confidentialité font défaut jusqu'à présent dans des contrats passés avec des prestataires externes, l'accès au courrier entrant et sortant contenant souvent des données et documents confidentiels devrait être accordé selon les besoins et au moyen d'une matrice de contrôle d'accès.

De plus, les contrôles de l'année précédente ont été poursuivis; en particulier, une prise de position de l'institution contrôlée en 2016 a été requise à propos des mesures ordonnées et celles-ci ont été vérifiées.

Il n'a pas été possible d'achever les contrôles subséquents des années antérieures. D'autres contrôles de ce type sont prévus.

Contrôle SIS: pendant l'année sous rapport, aucun contrôle coordonné n'a eu lieu avec les autres cantons ni avec le Préposé fédéral à la protection des données et à la transparence. Par contre, les bases d'un contrôle coordonné ont été mises au point. La Préposée à la protection des données a activement participé à l'élaboration d'un guide des contrôles coordonnés dans le cadre du groupe de coordination Schengen des préposés suisses à la protection des données. D'autre part, il a été procédé à des premiers éclaircissements internes préalables à l'organisation des autorisations d'accès au SIS (cf. art. 55 de l'Ordonnance du 8 mars 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'Etat 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

Divers services et organes publics ont demandé une extension de leur accès à FRI-PERS. La raison invoquée à cet effet fut fréquemment l'introduction d'une nouvelle application prévoyant une interface avec FRI-PERS, afin de mettre à jour le plus rapidement possible les données personnelles. L'Autorité est bien consciente du besoin des organes de pouvoir disposer de données personnelles actuelles et correctes dans les banques de données. Mais elle fait toujours remarquer qu'un tel accès via une interface ne peut que servir à la mise à jour des données et, sur la base de la finalité, ne peut en aucun cas être utilisé à d'autres mises en lien de données. Il faut en outre prendre en considération le fait que de telles procédures d'appel exigent toujours une autorisation d'accès individuelle; en d'autres termes, elles ne peuvent pas passer par un compte technique. Une procédure d'appel via un compte technique n'est pas autorisée par la loi, car l'enregistrement des divers appels (protocole) n'est pas garanti et, partant, aucun contrôle ne serait possible. Le protocole des appels doit permettre de détecter des abus. Le prestataire responsable doit de surcroît veiller à l'interne, au moyen de directives adéquates, à un traitement conforme aux règles.

Contrôles
Le Service de la population et des migrants SPoMi est responsable de la procédure d'appel de données sur la plateforme informatique cantonale (cf. art. 16a de la Loi sur le contrôle des habitants). Le SPoMi et l'Autorité se sont mis d'accord au cours de plusieurs rencontres sur une procédure commune de contrôle des droits d'accès à la plateforme, et sur des contrôles communs. Ils ont établi un guide à cet effet. Un premier contrôle commun est prévu pour 2018.

Interfaçage par webservices et avec réception d'événements
Pour accomplir ses tâches, l'Administration des finances (ci-après : AFin) a besoin de données actualisées et exactes et a obtenu, dans ce cadre, un accès aux données FRI-PERS nécessaires. Afin que les informations de sa base de données SAP R/3 réunissant les données relatives à la comptabilité, à l'encaissement des factures et au suivi du contentieux de l'Etat soient le plus à jour possible, l'AFin a requis un interfaçage par webservices et avec réception d'événements. Par interfaçage par webservices, il faut comprendre la consultation des données autorisées de l'application FRI-PERS par l'application SAP R/3. En effet, l'application SAP R/3 interroge l'application FRI-PERS concernant les données d'une personne déterminée, de sorte que le collaborateur peut consulter les données FRI-PERS à jour et corriger sa base de données. L'interfaçage avec réception d'événements est, quant à lui, l'envoi par l'application FRI-PERS à l'application SAP R/3 de toutes les mutations en relation avec les données autorisées. Un événement peut, par exemple, concerner les personnes décédées, de sorte que l'AFin recevra un message l'informant qu'une personne répondant aux critères d'accès autorisé est décédée. Après analyse de la demande, la Préposée à la protection des données a émis un préavis favorable temporaire, à savoir limité à une année, afin que l'AFin puisse pallier les lacunes. En effet, il ressort du dossier que différents services de l'Etat ont accès aux données de SAP R/3, par le biais d'une procédure d'appel qui est un mode de communication automatisé des données en ligne. Toute procédure d'appel ne peut être accordée que si une base légale le prévoit laquelle, dans le cas d'espèce, fait défaut. En outre, un tel accès à des données doit être documenté dans un règlement d'utilisation précisant notamment les fonctions des personnes autorisées, les données accessibles, la fréquence des interrogations, la procédure d'authentification et les mesures de sécurité et de contrôle. Enfin, il est relevé que l'AFin doit évaluer les autorisations d'accès, de sorte que chaque service doit avoir accès à ses propres débiteurs et créanciers.

Interfaçage par webservices
Dans le cadre de l'accomplissement des tâches du Service des curatelles d'adultes de la ville de Fribourg (ci-après: SCFR) en matière de protection de l'adulte, un accès aux données FRI-PERS nécessaires lui a été octroyé. Cet accès est limité aux données des habitants de la ville de Fribourg. Afin que les données soient actualisées et exactes, le SCFR a sollicité un interfaçage par webservices, par lequel son application KISS réunissant les données de ses clients interroge l'application FRI-PERS concernant les données d'un client déterminé. En l'espèce, la Préposée à la protection des données relève que les données traitées par le SCFR sont classées confidentielles, de sorte qu'elles doivent être protégées par cryptage lors de leur transmission et stockage, et une authentification et un contrôle des accès doivent être prévus. Dans la mesure où le responsable des données sensibles de KISS est le SCFR, la Préposée à la protection des données a préavisé favorablement la demande pour autant que les conditions strictes suivantes soient respectées. Seules les données des clients enregistrées dans la base de données KISS seront mises à jour par l'export des données FRI-PERS, de sorte que les habitants de la ville de

Fribourg qui ne sont pas sous curatelle ne seront pas ajoutés dans cette base de données. Seul, le chef du SCFR a accès aux données FRI-PERS et peut ainsi quotidiennement mettre à jour les données de KISS par les données FRI-PERS. Lors de l'attribution de nouveaux clients au SCFR, le chef aura la tâche de créer un nouveau dossier et, lorsque la mesure est levée, la personne est décédée ou pour tout autre motif permettant de clore un dossier, il est de sa responsabilité de fermer le dossier et de vérifier que les données du client ne soient plus mises à jour. Pour assurer la sécurité des données, le SCFR doit déterminer, en fonction des tâches de chaque collaborateur, les personnes autorisées à accéder aux fichiers ainsi que l'étendue de leur accès. En outre, la Préposée à la protection des données a rappelé que chaque collaborateur est soumis au secret de fonction. Enfin, le numéro AVS ne peut pas être utilisé pour procéder à la mise à jour des données entre les deux applications.

Extension de l'accès
Suite à l'introduction d'une taxe sur la plus-value dans la Loi fédérale sur l'aménagement du territoire et dans la loi cantonale y relative, le Service des constructions et de l'aménagement (ci-après: SeCA) est chargé, pour le compte de sa direction, du suivi des dossiers dans le cadre de la procédure de taxation et, en cas d'exigibilité de la taxe, de l'élaboration de l'avis de taxation et de son envoi au Service cantonal des contributions (ci-après: SCC) pour encaissement. Etant déjà bénéficiaire d'un accès aux données FRI-PERS, le SeCA sollicite une extension de son accès au numéro AVS afin d'élaborer l'avis de taxation et de permettre au SCC d'identifier le débiteur de la taxe. La Préposée à la protection des données rappelle que le SeCA ne fait pas partie des services et institutions habilités à utiliser systématiquement le numéro AVS selon la loi fédérale et qu'aucune base légale cantonale formelle ne le prévoit. Elle conclut que, dans le cadre de l'élaboration de la décision de taxation par le SeCA, l'utilisation de l'identificateur de bâtiment permettrait également au SCC d'identifier le débiteur dans la mesure où ce dernier a accès à cette information. Un préavis défavorable est émis concernant l'accès au numéro AVS mais favorable à l'identificateur du bâtiment.

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.

Dans le cadre des demandes d'installation de système de vidéosurveillance, l'Autorité constate que les requêtes sont souvent lacunaires. En effet, l'analyse des risques et des mesures de prévention possible au regard du but poursuivi font souvent défaut. Sans ces informations essentielles, à savoir le but de l'installation, la nature et la fréquence des atteintes ainsi que les moyens pris pour prévenir la réalisation de ces risques, il est difficile d'émettre un préavis. En outre, les images des prises de vue des caméras manquent aussi fréquemment au dossier de demande. Or, ces dernières sont nécessaires pour analyser si le système de vidéosurveillance filme le domaine privé ou public, s'il est dirigé contre des

immeubles ou maisons privés et si un système de floutage doit être employé. En effet, une autorisation d'installation d'un système de vidéosurveillance est obligatoire si des enregistrements du domaine public sont réalisés, le domaine privé n'étant pas soumis à la Loi cantonale sur la vidéosurveillance.

L'Autorité a pris position sur divers projets de vidéosurveillance pendant l'année objet du rapport. Toutes les prises de position de l'Autorité sont mises en ligne sur son site Internet.

Enregistrements vidéo dans un centre commercial
Une demande d'installation de vidéosurveillance recouvrait les zones intérieures et extérieures d'un commerce privé. Les caméras prévues pour filmer à l'extérieur, à propos desquelles l'Autorité s'est exprimée, filmaient le domaine public. L'Autorité a jugé disproportionnée l'installation d'une vidéosurveillance dans la zone de l'entrée du personnel et pour la surveillance des places de parc, car la sécurité et l'ordre public sont des tâches relevant de la compétence de la police. Le Tribunal cantonal a rejeté un recours déposé par le propriétaire du commerce en question contre la décision de la Préfecture refusant l'installation de caméras supplémentaires sur le domaine public. Le Tribunal cantonal est arrivé à la conclusion que la caméra qui était dirigée sur le parking du personnel ainsi que sur l'entrée de celui-ci n'était pas conforme au principe de la proportionnalité (surveillance du personnel, renseignement sur d'éventuels covoiturages et échange d'informations), ce d'autant moins qu'à l'intérieur du bâtiment, dix caméras étaient déjà installées qui recouvraient également cette sortie.

Vidéosurveillance en temps réel ou avec enregistrement
Une administration communale est au bénéfice d'une autorisation d'installation de vidéosurveillance comprenant 9 caméras réparties dans tous les étages et dont la visualisation est effectuée en direct par la réceptionniste de l'entrée principale. La condition requise pour son octroi était principalement de ne pas enregistrer les images pendant les heures d'ouverture soit de 8h00 à 17h00, sauf pour les deux caméras du premier étage filmant les portes de services sensibles. Par la suite, la Préposée à la protection des données a préavisé favorablement la demande de modification de l'installation de vidéosurveillance de la commune, dans le sens que les caméras du premier étage n'enregistrent plus les images durant les heures ouvrées, mais en contrepartie sont visionnées en temps réel par le personnel des secrétariats respectifs. En outre, il est précisé que le visionnement en temps réel des deux caméras du premier étage, par la réceptionniste de l'entrée principale, n'est plus nécessaire et que les enregistrements existants de ces deux caméras doivent être détruits.

Vidéosurveillance effectuée par une entreprise privée
Une entreprise exposée à des activistes souhaite installer des caméras extérieures filmant ses portails d'accès afin d'assurer la sécurité de son site de production et d'observer l'accès des véhicules dans son enceinte. Le cas d'une seule une caméra est analysé dans la mesure où le champ de vision des autres caméras n'a pas été transmis. L'entreprise désire alors filmer son portail d'accès ainsi qu'une partie de la route communale également empruntée par les entreprises voisines. Puisqu'elle projette d'enregistrer des images d'une partie du domaine public, une autorisation est nécessaire. Pour être installée et exploitée sur le domaine public, la vidéosurveillance doit respecter le but prévu par la loi à savoir de prévenir les atteintes aux personnes et aux biens, et de contribuer à la poursuite et à la répression des infractions. Or, il ressort du dossier que l'observation de l'accès des véhicules dans l'enceinte ne répond pas au but précité et ne peut être observé au moyen de la vidéosurveillance. Toutefois, la Préposé à la protection des données déduit de la requête que l'entreprise souhaite prévenir les atteintes aux biens et poursuivre les suspects potentiels en cas de dommage sur son site de production. Avec cette nouvelle formulation, le but devient conforme à la loi et il paraît dès lors envisageable que la vidéosurveillance permette de limiter les risques d'atteinte. Dans le cadre de l'analyse du respect du principe de la

proportionnalité, il appert que, pour atteindre le but précité, il n'est pas nécessaire de filmer la route communale puisque seule la surveillance du domaine privé de l'entreprise est suffisante. C'est d'ailleurs également l'avis du Conseil communal concerné, propriétaire de la route, qui préavise favorablement l'installation pour autant qu'elle n'empiète pas sur son domaine public. Ainsi, la caméra ne devra filmer que le domaine privé de l'entreprise de sorte que le champ de vision de la caméra devra être modifié. La Préposée à la protection des données émet un préavis défavorable à la demande d'installation qui ne passe pas l'examen de la proportionnalité. Elle renvoie le requérant à l'avis du Préposé fédéral à la protection des données qui est compétent en ce qui concerne la vidéosurveillance du domaine privé.

Surveillance par vidéo d'une pizzéria
Le système de vidéosurveillance en projet capture des images de la porte d'entrée principale de la pizzéria ainsi que de la vitrine donnant sur une route cantonale et sur un parking. Le dossier ne mentionne aucune atteinte aux biens ou aux personnes et précise que la pizzéria a été récemment ouverte. Il ressort des recommandations du Préposé fédéral à la protection des données que la surveillance de l'espace public par un privé est jugée disproportionnée et interdite. En effet, un système de vidéosurveillance filmant le domaine public, dans le but de protéger les intérêts de particuliers, enregistre des images d'un nombre indéterminé de personnes et porte ainsi atteinte à leurs droits de la personnalité. Ces personnes ne peuvent souvent pas éviter l'espace surveillé et sont obligées de tolérer cette atteinte à leurs droits, que des intérêts privés ne sauraient justifier. Il rappelle que la sécurité et l'ordre publics n'incombent pas aux particuliers mais à la police. Un particulier ne peut donc pas arguer de son intérêt en matière de sécurité pour surveiller l'espace public. Dans le cas d'espèce, il s'agit d'une surveillance de l'espace public par le propriétaire de la pizzéria, surveillance qui porte atteinte non seulement aux usagers de cette dernière mais également aux passants. Ainsi, l'installation de ce système de vidéosurveillance ne passe pas l'examen de la proportionnalité, de sorte que la Préposée à la protection des données a préavisé défavorablement la demande. Partant, il convient de retirer la caméra ou de changer son champ de vision de manière à ce qu'elle ne filme que le domaine privé, à savoir l'intérieur de la pizzéria.

Modification et extension d'une installation de vidéosurveillance
Un établissement de l'administration fribourgeoise, déjà au bénéfice de l'autorisation d'installer un système de vidéosurveillance, possède 33 caméras en fonction. Par courrier, il demande la modification et l'extension de son système de vidéosurveillance, principalement des extensions à la vision en temps réel par le service où la caméra est installée en sus de l'enregistrement des images, la modification de l'emplacement d'une caméra et des demandes d'installation de 8 nouvelles caméras mais sans visualisation en direct. Une partie des caméras installées ne subissant ni modification ni extension, seule une analyse individuelle des autres caméras est effectuée et un préavis est donné à chacune d'elle. S'agissant de données sensibles, le visionnement des enregistrements ne peut être effectué qu'en cas d'atteintes avérées et le système de stockage des données doit être protégé dans un lieu adéquat et non accessible aux personnes non-autorisées. La Préposée à la protection des données a précisé que les postes des services accueillant régulièrement des visiteurs doivent fonctionner selon un système de floutage des images et être gérées de manière à ce qu'aucune personne non-autorisées ne puissent les visionner en direct, alors que les postes des autres services doivent être installés dans un endroit fermé et difficile d'accès par des personnes non-autorisées. En outre, l'accès aux enregistrements doit être limité strictement aux personnes en ayant la nécessité et une liste nominative des personnes autorisées à visionner les images en temps réel de chaque service devrait, dans l'idéal, être annexée au Règlement d'utilisation du système de vidéosurveillance. Toutefois, au vu des changements réguliers de personnels des différents services, seule la liste des vigiles est exigée. Enfin, chaque personne ayant accès à la visualisation en temps réel doit signer une clause de confidentialité.

Caméra de vidéosurveillance mobile sur les points de récolte des déchets
Une commune a demandé l'autorisation d'installer une caméra de vidéosurveillance mobile sur les différents points de récolte de déchets. Suite au préavis défavorable de l'Autorité, des tests ont été organisés, en accord entre les parties, sur deux points de récoltes prédéterminés. Une fois, le résultat de ces tests connu, l'Autorité relève dans son préavis que l'installation prévoit de poursuivre plusieurs buts, à savoir le contrôle de la salubrité et le contrôle du respect des Règlements communaux. Par ailleurs, l'installation permettrait le contrôle des horaires d'ouverture et des dépôts interdits. Or, au sens de la loi cantonale et de la jurisprudence fribourgeoise, le but visé n'est pas conforme dans la mesure où le système ne doit pas être utilisé comme moyen de dénonciation des incivilités, des dépôts sauvages ou interdits et d'éventuelles atteintes à l'ordre public. Seul le but de prévenir les atteintes aux personnes et aux biens, à savoir aux déprédations et aux dommages à la propriété, serait conforme. Afin de respecter le principe de la proportionnalité, il est indispensable d'établir une liste mentionnant l'angle et la position de la caméra mobile sur chaque zone autorisée afin que la capture d'images soit à chaque fois identique et de veiller, au besoin par des moyens techniques de blocage, à ce que la caméra ne puisse être dirigée vers des immeubles ou des maisons privées sis à proximité des points de récolte. En outre, un système de floutage des images devra être employé. Afin que le système de surveillance soit toujours conforme aux besoins et aux conditions légales, il est nécessaire que le conseil communal le réévalue tous les 5 ans, notamment au vu des progrès technologiques. S'agissant du délai de conservation des images d'une durée de 100 jours, celui-ci est trop long, les images devront être effacées le plus rapidement possible. Enfin, l'hébergement et le stockage des données doivent être effectués en Suisse.

Réévaluation de l'installation de vidéosurveillance d'un café
Dans le cadre d'une autorisation de vidéosurveillance avec enregistrement demandée par un café, l'Autorité avait rendu un préavis favorable mais soumis à des conditions strictes. Par décision, le Préfet avait octroyé l'autorisation et limité le système à une année. À l'échéance de ce délai et pour vérifier la conformité de l'installation de vidéosurveillance aux besoins et aux conditions légales, l'Autorité a demandé au Préfet de lui transmettre un rapport comparatif des atteintes et des interventions de police entre la situation avant et après l'installation du système de vidéosurveillance permettant ainsi de déterminer la situation réelle. Après analyse du rapport, l'Autorité a estimé qu'actuellement la vidéosurveillance est conforme aux besoins.

Externalisation des enregistrements de vidéosurveillance et contenu du contrat d'outsourcing
Avec les avancées technologiques et le développement du marché, la vidéosurveillance et ses modalités d'application se complexifient. La question du stockage et de l'hébergement des enregistrements vidéo par une entreprise externe à l'organe public, en Suisse ou à l'étranger, se pose d'autant plus que l'externalisation/outsourcing se multiplie. Dans ce contexte, l'Autorité communique une liste non exhaustive des conditions à respecter et qui doivent figurer non seulement dans le contrat de sous-traitance, mais aussi en cas de vidéosurveillance du domaine public, dans le règlement d'utilisation y relatif.

Pose d'une caméra de vidéosurveillance dans un champ
Dans le but de surveiller son cheval, un particulier souhaite installer une caméra de vidéosurveillance sur sa propriété. Dans la mesure où il ne capture pas d'image du domaine public, le système de vidéosurveillance n'est pas soumis à la Loi sur la vidéosurveillance (LVid) et ne nécessite aucune autorisation. Toutefois, l'installation doit respecter les principes de la Loi fédérale sur la protection des données (LPD), qui règle notamment le traitement des données personnelles entre personnes privées et qui est de la compétence du Préposé fédéral à la protection des données et à la transparence (PFPDT).

A titre indicatif, l'Autorité a tout de même relevé que, pour respecter le principe de la proportionnalité, la caméra ne doit pas filmer les domaines privés voisins, sauf consentement de leurs propriétaires. En outre, un signalement visible doit informer les personnes susceptibles d'entrer dans le champ de vision de la caméra et leur indiquer également auprès de quelle personne elles peuvent faire valoir leur droit d'accès à leurs données.

Pose d'un appareil photo sur une parcelle en construction
Un particulier souhaite installer sur sa parcelle un appareil photo prenant des clichés, automatiquement et à intervalle régulier, de l'évolution des travaux de construction de sa villa. Dans le cas où le champ de vision de l'appareil capture des images du domaine public, même partiellement, ce dispositif est alors interdit puisqu'il ne remplit pas les exigences légales. En revanche, s'il prend exclusivement des images de sa propriété privée et non du domaine public, le cas relève alors de la compétence du Préposé fédéral à la protection des données et à la transparence (PFPDT). A titre indicatif, l'Autorité a néanmoins relevé que ce dispositif photographique implique la prise de photos des ouvriers travaillant sur le chantier. Or, toute personne est, de manière générale, titulaire du droit à l'image qui lui permet de s'opposer à la prise d'images d'elle-même et à leur diffusion ou du droit de soumettre leur utilisation à conditions. Si lesdites photos sont destinées à être communiquées, le consentement des personnes concernées doit être obtenu avant tout partage. En revanche, dans le cas où les photos demeurent dans un usage exclusivement personnel, la Loi sur la protection des données (LPD) ne s'applique pas. Toutefois, il est recommandé d'avertir au préalable les personnes qui entreront dans le champ de vision de l'appareil. Pour limiter l'atteinte, l'Autorité conseille de prendre des photos à une fréquence moindre, comme par exemple une le matin avant l'arrivée des ouvriers et une le soir après leur départ.

1.4 ReFi – registre des fichiers[13]

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'Autorité[14].

Après la mise à jour de l'application informatique, intervenue en 2015 et 2016, il s'agissait essentiellement, durant l'année sous examen, de vérifier la saisie des déclarations de fichiers. 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 d'établir quels sont les collectes de données existant dans une commune et de mettre au point des annonces-types. Il n'a pas encore été possible d'achever ces travaux.

[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).

Sur invitation des Hautes Ecoles spécialisées HESSO/FR, la Préposée à la protection des données a présenté, au cours de sessions de formation continue spécifiques, le droit cantonal de la protection des données et a sensibilisé des professeurs ainsi que des collaboratrices et collaborateurs administratifs aux exigences du droit de la protection des données. La session s'est tenue pendant quatre jours.

La Préposée à la protection des données a participé pendant l'année sous rapport à plusieurs séances avec des représentants du Centre fri-tic: elle a conseillé le Centre dans le cadre de la mise au point de directives sur l'utilisation d'Internet et des réseaux sociaux dans les écoles. L'Autorité a jugé favorablement l'initiative qu'a prise la Direction de l'instruction publique, de la culture et du sport. Par ailleurs, la Préposée a présenté un exposé à la Journée Réseau sur le sujet «Big Data et protection des données» ainsi que sur la sécurité des données à l'école.

2. Statistiques

Protection des données en général

Durant la période considérée, 300 dossiers en matière de protection des données (sans les demandes FRI-PERS et vidéosurveillance, voir ci-dessous) ont été introduits, dont 62 sont pendants au 1er janvier 2018. Ces dossiers comprennent 108 conseils et renseignements, 62 avis, 28 examens de dispositions législatives, 13 communications de décisions (art. 27 al. 2 LPrD), 8 contrôles et inspection ou suivis de contrôle, 9 présentations, 36 participations à des séances et autres manifestations et 36 demandes diverses. 139 dossiers concernent des organes cantonaux ou des institutions chargées de tâches publiques, 51 des communes et paroisses, 66 d'autres organismes publics (cantons, autorités de protection des données), 39 des particuliers ou des institutions privées et 5 des médias (cf. statistiques annexées). Pour les dossiers pendants des années précédentes, 54 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 2017, 6 demandes ont été soumises à la Préposée à la protection des données pour préavis: 2 demandes d'accès, 2 demandes d'extension de l'accès, 1 demande d'interfaçage par webservices et 1 demande d'interfaçage par webservices et avec réception d'événements. De ces requêtes, 3 demandes sont toujours en traitement et 3 ont obtenu un préavis positif. 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 2017, la Préposée à la protection des données a reçu 14 demandes d'installation de vidéosurveillance avec enregistrement pour préavis, 1 annonce d'installation de vidéosurveillance sans enregistrement et a dû se déterminer à 2 reprises dans des cas de modification et extension d'une installation et d'installation sans autorisation. De ces requêtes, 2 préavis positifs ont été émis, 2 préavis mixtes, 3 préavis défavorables alors que les 10 restantes sont encore en cours de traitement. Certains préavis positifs étaient assortis de conditions, notamment de satisfaire à l'exigence de signalisation des systèmes de vidéosurveillance. Par ailleurs, 10 demandes émanaient des services de l'Etat ou de communes et 7 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 préfectures 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 2017. 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

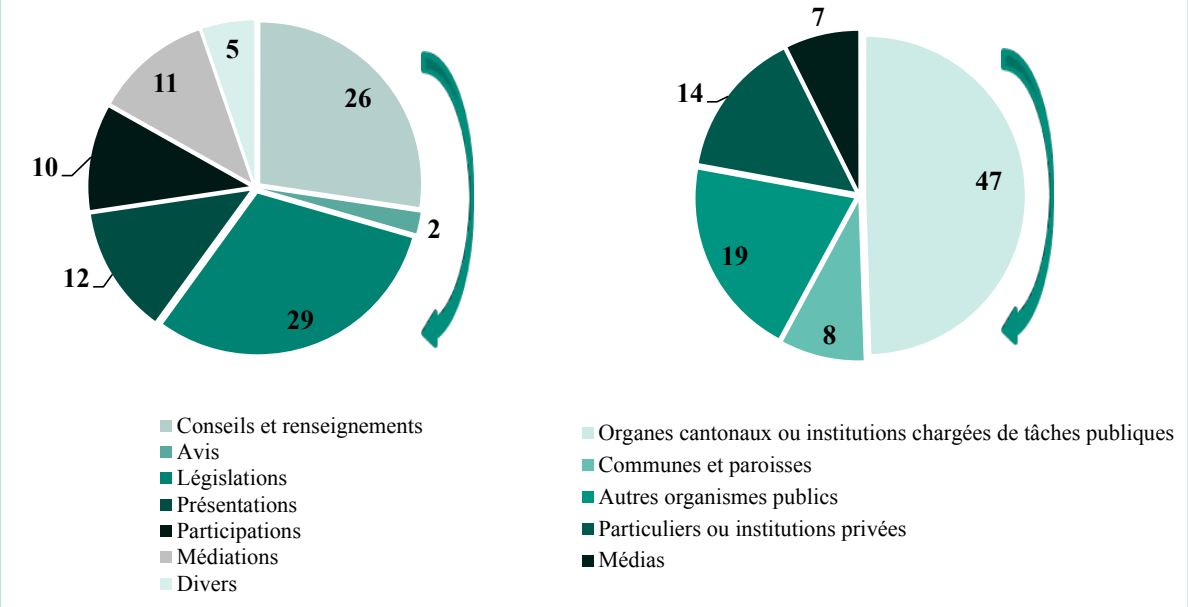
La bonne collaboration entre les deux Préposées s'est poursuivie en 2017. Plusieurs mesures avaient été prises dès le début pour la préservation de cette coopération. Les séances de la Commission, auxquelles les deux Préposées participent, traitent régulièrement les dossiers portant sur les deux domaines. 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.

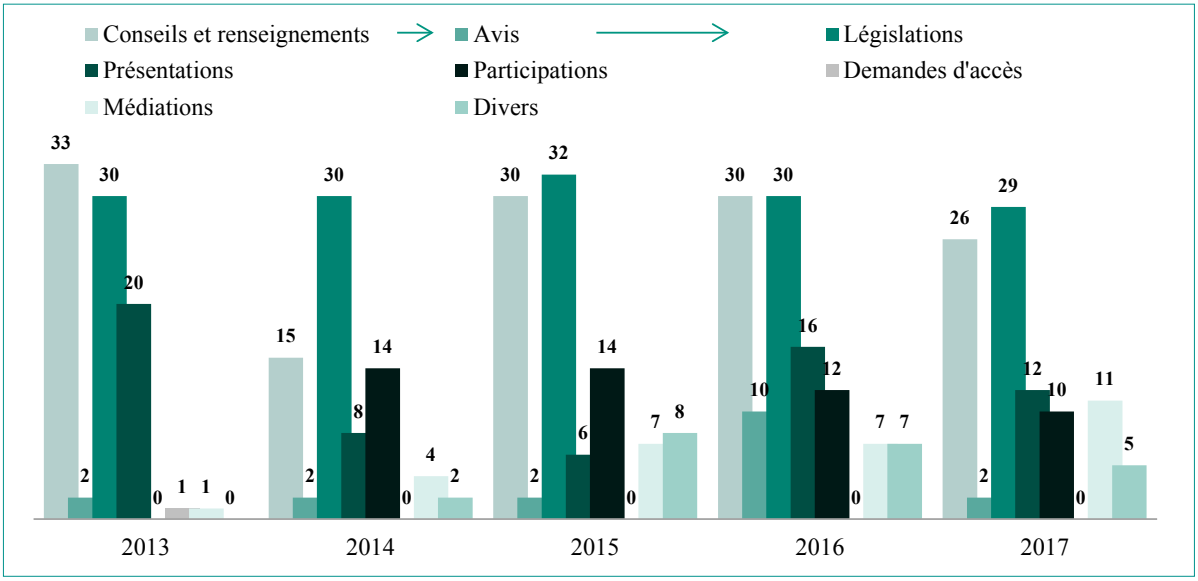
Statistiques de la transparence

Demandes / interventions en 2017

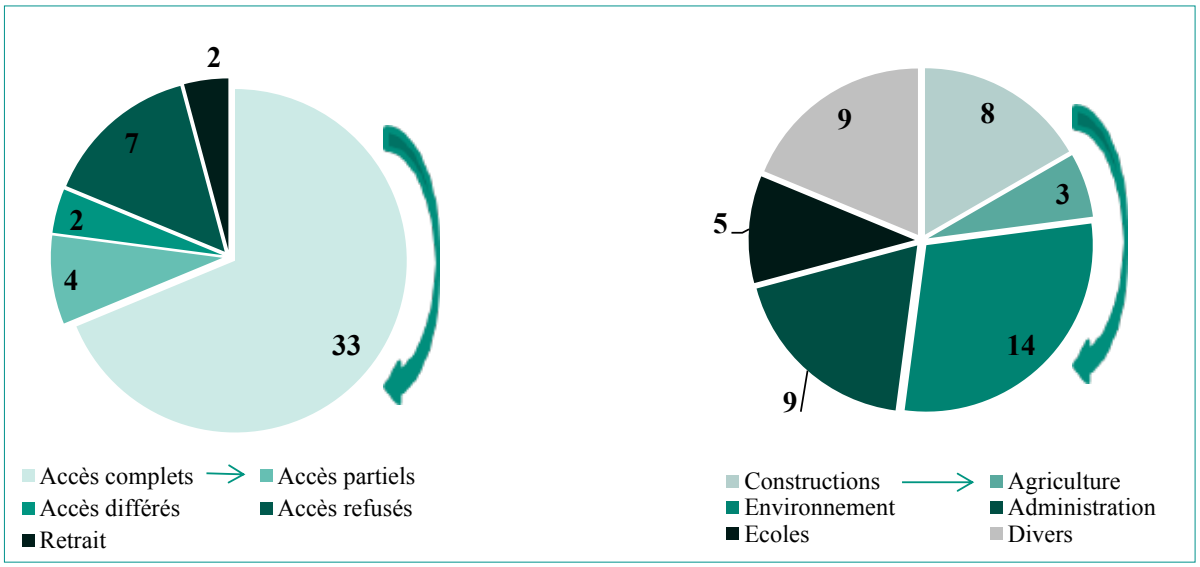


- Les «conseils et renseignements» sont donnés par la Préposée à la transparence.
- Le terme «législations» comprend les travaux de réflexion sur des dispositions législatives et les réponses aux consultations.
- La notion de «présentations» recouvre par ex. les exposés dans le cadre de la présentation 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 95 dossiers ouverts en 2017, 42 dossiers sont communs avec ceux de la protection des données, dont 28 consultations.

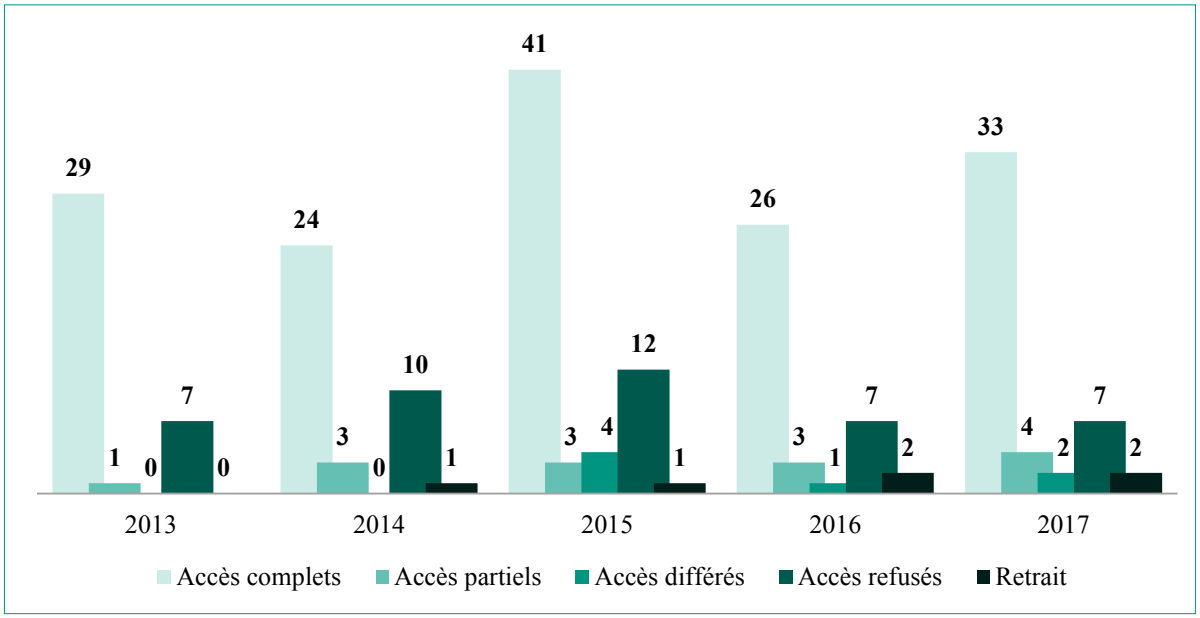
Comparatif



Evaluation du droit d'accès en 2017

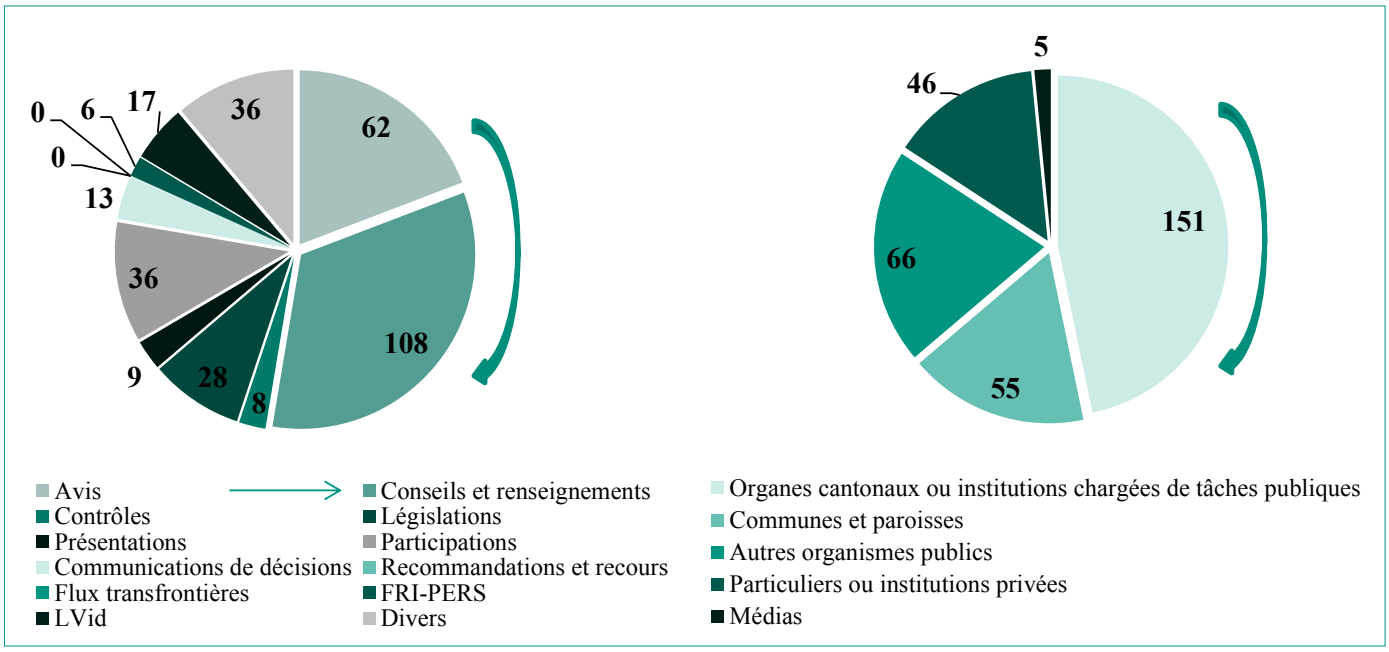


Comparatif



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

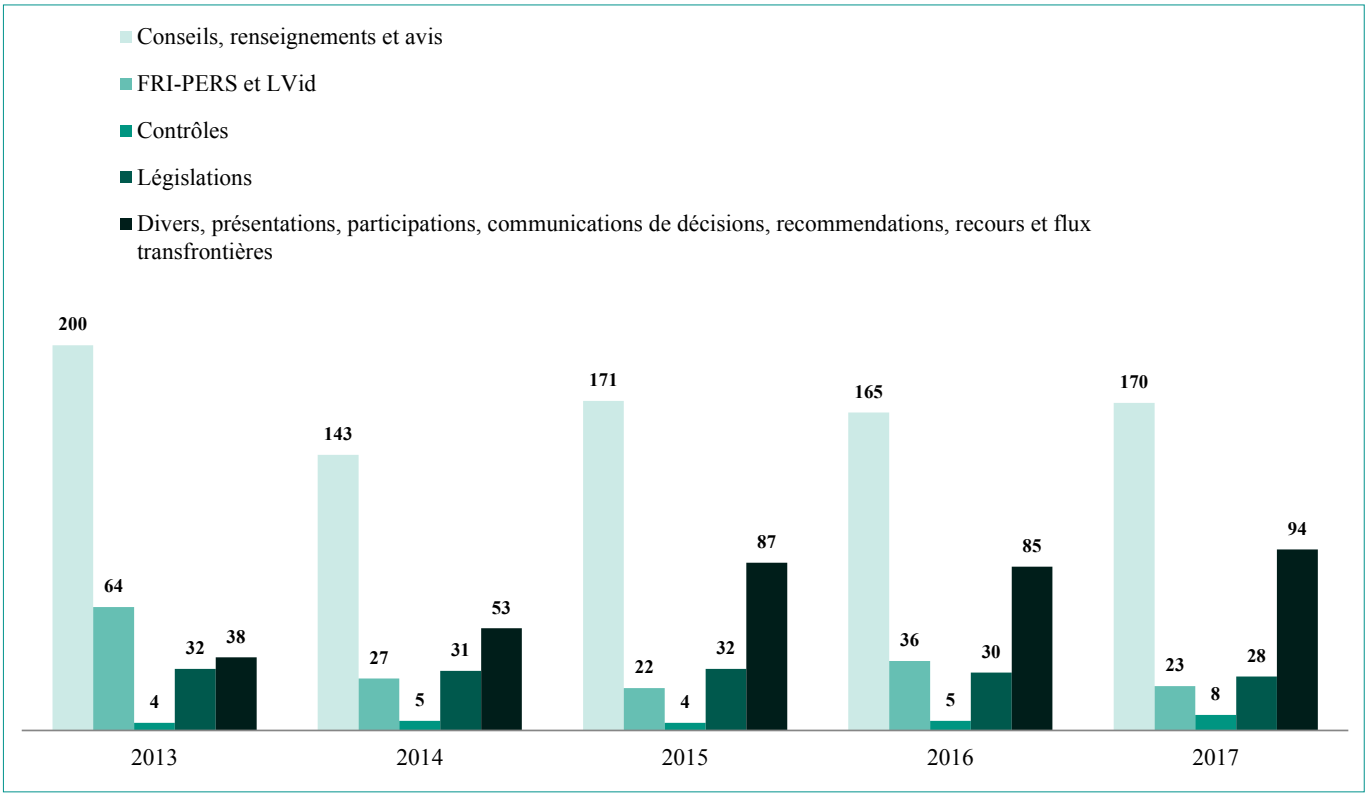
Demandes / interventions en 2017



- 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 323 dossiers ouverts en 2017, 42 dossiers sont communs avec ceux de la transparence, dont 28 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
2017	62	108	8	28	9	36	13	0	0	6	17	36	323
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