# Rapport d'activité 2018

—

pour la période du 1er janvier
au 31 décembre 2018

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

Avril 2019

—

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 2018 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 2019

| Le Président<br>de la Commission | La Préposée<br>à la transparence | La Préposée<br>à la protection des données |
|---|---|---|
| L. Schneuwly | A. Zunzer Raemy (jusqu'au 30.06)<br>M. Stoffel (dès le 01.09) | A. Reichmuth Pfammatter |

# Table des matières

# Table des abréviations et termes utilisés

| | |
|---|---|
| AFOCI | Association fribourgeoise pour l'organisation des cours interentreprises |
| AP | Avant-projet |
| AP-LPREX | Avant-projet de la loi fédérale sur les précurseurs de substances explosibles |
| ATPrD | Autorité cantonale de la transparence et de la protection des données |
| AVS | Assurance-vieillesse et survivants |
| CPJA | Code de procédure et de juridiction administrative du 23 mai 1991 |
| DAEC | Direction de l'aménagement, de l'environnement et des constructions |
| DICS | Direction de l'instruction publique, de la culture et du sport |
| DSAS | Direction de la santé et des affaires sociales |
| DSJ | Direction de la sécurité et de la justice |
| ECAB | Etablissement cantonal d'assurance des bâtiments |
| ECALEX | Nouvelle loi sur l'assurance immobilière, la prévention, les secours en matière de feu et d'éléments naturels |
| Fedpol | Office fédéral de la police Fedpol |
| FRI-PERS | Plateforme informatique cantonale du contrôle des habitants |
| Fritic | Centre de compétences de la DICS, responsable de tous les aspects en lien avec les médias et technologies de l'information et de la communication (MITIC) dans le domaine de l'enseignement du canton de Fribourg |
| HESSO//FR | Haute Ecole spécialisée de Suisse occidentale//Fribourg |
| LArch | Loi du 10 septembre 2015 sur l'archivage et les Archives de l'Etat |
| LASoc | Loi du 14 novembre 1991 sur l'aide sociale |
| LCH | Loi du 23 mai 1986 sur le contrôle des habitants |
| LGCyb | Loi du 2 novembre 2016 sur le guichet de cyberadministration de l'Etat |
| LInf | Loi du 9 septembre 2009 sur l'information et l'accès aux documents |
| LMéd | Loi du 25 juin 2015 sur la médiation administrative |
| LPD | Loi fédérale du 19 juin 1992 sur la protection des données |
| 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 |
| OSAV | Office fédéral de la sécurité alimentaire et des affaires vétérinaires |
| OVid | Ordonnance du 23 août 2011 sur la vidéosurveillance |
| PFPDT | Préposé fédéral à la protection des données et à la transparence |
| PLASTA | Ordonnance sur le système d'information en matière de placement et de statistique du marché du travail |
| Privatim | Conférence des Préposé(e)es suisses à la protection des données |
| ReFi | Registre des fichiers |
| RGPD | Règlement général sur la protection des données |
| SESPP | Service de l'exécution des sanctions pénales et de la probation |
| SAP | Logiciel (Systems, Applications and Products for data processing) |
| SAgri | Service de l'agriculture |
| SASPP | Service de l'application des sanctions pénales et des prisons |
| SCC | Service cantonal des contributions |
| SEJ | Service de l'enfance et de la jeunesse |
| SIS | Système d'information Schengen |
| SITel | Service de l'informatique et des télécommunications |
| SPO | Service du personnel et de l'organisation |
| SPoMi | Service de la population et des migrants |
| SProb | Service de probation |
| THEMIS | Application métiers pour les Offices des poursuites |

# 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 diplômé-e-s 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 extrêmement difficiles à remplir de manière satisfaisante avec les moyens dont elle dispose. En effet, la Préposée à la protection des données est amenée à travailler dans de nombreux projets de grande envergure traitant des données sensibles ainsi que la digitalisation. 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;
- préaviser les dérogations en matière de protection des données pour des phases d'essai comme prévu dans l'article 21 LGCyb.

En 2018, la Commission était présidée par *M. Laurent Schneuwly,* Président du Tribunal civil de la Sarine. Les autres membres de la Commission étaient: *M. Philippe Gehring (Vice-président),* ingénieur

[1] https://bdlf.fr.ch/app/fr/texts_of_law/17.5/versions/4692
[2] https://bdlf.fr.ch/app/fr/texts_of_law/17.1/versions/4691

en informatique EPFL, *M^me^ Anne-Sophie Brady,* conseillère communale, *M. André Marmy,* médecin, *M. Jean-Jacques Robert,* ancien journaliste, *M. Luis-Roberto Samaniego,* spécialiste en sécurité informatique, et *M. Gerhard Fiolka,* Professeur à l'Université.

La Commission a tenu neuf séances en 2018. 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 149 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/app/fr/texts_of_law/114.21.12/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).

La collaboration entre l'Autorité et le Médiateur cantonal s'est poursuivie, comme le prévoit la Loi sur la médiation administrative (LMéd).

## 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, s'est réuni deux fois durant l'année 2018 à l'invitation du PFPDT[6]. Les séances ont traité, entre autres objets, de l'évaluation Schengen 2018 de la Suisse, qui s'est déroulée du 26 février 2018 au 2 mars 2018 auprès de la Confédération et du canton de Lucerne. Les experts de l'UE ont estimé que la Suisse met en œuvre et applique l'acquis de Schengen. L'utilisation du Système d'information Schengen (SIS), la coopération entre les services de police et le traitement des données personnelles ont notamment fait l'objet d'un examen. Cependant, le manque de ressources du Préposé lucernois à la protection des données a été critiqué.

[4] https://bdlf.fr.ch/app/fr/texts_of_law/17.3/versions/3089 et https://bdlf.fr.ch/app/fr/texts_of_law/17.31/versions/3090
[5] https://www.fr.ch/atprd/institutions-et-droits-politiques/transparence-et-protection-des-donnees/rapports-dactivite
[6] https://www.edoeb.admin.ch/edoeb/fr/home.html

Comme les autres autorités cantonales, la Préposée à la protection des données fait en outre partie de la Conférence des Préposé-e-s suisses à la protection des données **privatim**[7]. L'Autorité a pu profiter également en 2018 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 Genève. Elle a mis l'accent sur l'intelligence artificielle au sens large, avec des contributions sur «La cité intelligente» et «Quelle protection des données pour l'Homo numericus face à l'intelligence artificielle?». L'assemblée plénière d'automne s'est tenue à Glaris. La séance d'information était consacrée au «blockchain» (technologie, applications et aspects relevant de la protection des données). Par ailleurs, privatim a organisé pour ses membres et ses collaborateurs une séance d'introduction au droit de la protection des données, proposé un atelier sur l'informatique en nuage et publié une fiche d'information sur les portails en ligne des administrations publiques.

Le Président de privatim est, depuis mi-mai 2016, 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 de l'Etat de Fribourg (cours interentreprises AFOCI). La Préposée à la protection des données a présenté quant à elle deux cours (un en français et un en allemand) à l'HEG à l'occasion des formations continues proposées par l'Etat de Fribourg. De surcroît, sur invitation de Fritic, elle a présenté un exposé de deux demi-journées sur le sujet de la protection des données dans le contexte de l'école.

## 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[8]. En mai 2018, l'Autorité cantonale de la transparence et de la protection des données a tenu sa traditionnelle **conférence de presse.** La mise en place du nouveau site Internet du canton a entraîné des travaux importants pour l'Autorité eu égard à la refonte de son offre et à la migration des contenus. Le soutien d'une main-d'œuvre supplémentaire a permis de rendre le nouveau site de l'Autorité plus attractif et informatif.

Dans ses **newsletters** semestrielles[9], l'Autorité a fait connaître son travail à un public plus large et a abordé des thèmes d'actualité en lien avec la transparence et la protection des données. De plus, l'Autorité publie chaque année un guide actualisé **à l'attention spécifique des communes.** Ce guide vise à leur fournir des informations et des conseils s'appliquant à des cas concrets.[10]

[7] https://www.privatim.ch/fr/
[8] https://www.fr.ch/atprd/institutions-et-droits-politiques/transparence-et-protection-des-donnees/publications-0
[9] https://www.fr.ch/atprd/institutions-et-droits-politiques/transparence-et-protection-des-donnees/newsletter-0
[10] https://www.fr.ch/sites/default/files/contens/atprd/_www/files/pdf97/atprd_guide-pratique-a-latt.-des-communes-f---actualisation1.pdf

# 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 2018 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 réglementation d'application de la Loi sur la Haute Ecole pédagogique Fribourg**
L'avant-projet prévoit une évaluation périodique du personnel, de l'enseignement, de la recherche et des prestations des tiers. La Commission relève qu'il s'agit de clarifier le règlement quant aux modalités de transmission et de communication des résultats.
Sous l'angle de la protection des données, la Commission considère que l'anonymat des personnes qui remplissent les questionnaires d'évaluation doit être garanti et des règles de transmission des résultats doivent être instaurées. Elle suggère d'introduire à cet effet une norme qui précise les instruments utilisés pour réaliser les évaluations et clarifier ainsi quelles données personnelles sont utilisées. Par ailleurs, la durée de conservation et le délai de destruction des résultats et des données personnelles doivent être établis. Enfin, l'utilisation du NAVS13 doit être prévue dans une loi au sens formel (en l'occurrence la Loi sur la Haute Ecole pédagogique) et limitée à des situations spécifiques et exceptionnelles.

[11] https://www.fr.ch/atprd/institutions-et-droits-politiques/transparence-et-protection-des-donnees/consultations

Parallèlement, la Commission remarque que la durée de conservation des données relatives à l'identité et au parcours de formation fixée à 45 ans est contraire à la protection des données. Une telle durée de conservation est admissible uniquement en ce qui concerne les diplômes et les titres, car elle sert l'intérêt des anciens élèves.
Sous l'angle de la transparence, selon la Commission, la HEP devrait clarifier à qui elle communique les résultats des évaluations et sous quelle forme.

**Loi fédérale sur les précurseurs de substances explosibles**
L'Autorité a été amenée à s'exprimer sur l'avant-projet de la Loi fédérale sur les précurseurs de substances explosibles (AP-LPREX). Dans ce cadre, la Commission a émis des remarques relatives à la protection des données.
Premièrement, elle a relevé qu'il est important de préciser au moyen d'une liste exhaustive ce qui est entendu par «données personnelles» au sens de la loi. En effet, une telle définition est indispensable notamment pour justifier la collecte de données sensibles (par exemple pour les données qui doivent être fournies lors d'une demande d'accès à des précurseurs chimiques).
Ensuite, l'AP-LPREX prévoit que lors de la vente de précurseurs, un examen de l'autorisation d'acquisition via le système informatique de fedpol doit être effectué préalablement par le vendeur. Pour être licite, ce point doit être expressément prévu dans la loi et les données consultables doivent être limitées au strict nécessaire (principe de la proportionnalité).
Enfin, la Commission a déjà fait remarquer à plusieurs reprises qu'il est contraire à la protection des données d'utiliser le numéro AVS à 13 chiffres (NAVS 13) comme identificateur universel en dehors des assurances sociales.

**Règlement du personnel de l'ECAB et règlement sur le traitement du personnel de l'ECAB**
La Commission a été consultée sur un projet de règlement relatif au traitement du personnel et au personnel de l'Etablissement cantonal d'assurance des bâtiments. Dans ses remarques, elle a rappelé que la collecte de données médicales nécessite une base légale formelle puisqu'elles constituent des données sensibles. Par ailleurs, seules les données nécessaires sont collectées. Lorsqu'un examen médical est nécessaire pour un poste de travail, il y a lieu de préciser comment est fait cet examen médical et quelles sont les modalités s'y afférant. Si l'examen médical est fait sur la base d'un questionnaire, celui-ci doit être adressé par le collaborateur au médecin-conseil. Aucune personne autre que le médecin-conseil ne doit avoir accès au dossier médical du collaborateur. De plus, la communication d'informations contenues dans le dossier médical par le médecin-conseil doit se limiter au fait de dire si le collaborateur est apte à l'exercice de la fonction (oui/non) et de préciser s'il y a nécessité d'effectuer un éventuel examen médical complémentaire. La Commission a rappelé que l'employeur doit prévoir les mesures organisationnelles et techniques pour assurer la sécurité informatique. Il veille à sensibiliser les collaborateurs lors de formations régulières. Enfin, la Commission estime qu'il manque des normes relatives à la constitution du dossier personnel, sa durée de conservation, respectivement des différentes catégories de documents, et au droit d'accès de la personne concernée à son dossier. La Commission a été d'avis que seules les Ressources humaines de l'ECAB devraient avoir accès au dossier personnel.

**Avant-projet de loi modifiant la Loi sur les impôts cantonaux directs et la loi sur l'impôt sur les successions et les donations**
La Commission a été consultée concernant un avant-projet de loi modifiant la Loi sur les impôts cantonaux directs et la loi sur l'impôt sur les successions et les donations. La Commission a salué l'effort de clarifier le traitement électronique des données dans la loi. Toutefois, elle a regretté que cette consultation se fasse apparemment par voie de consultation restreinte. En outre, la Commission

a soulevé qu'aucune référence à la LPrD n'est faite alors que le traitement des données personnelles est évoqué. Concernant les systèmes d'informations pouvant contenir des données sensibles, la Commission a suggéré de définir quelles données sensibles sont concernées et notamment par quels organes elles sont transmises. S'agissant de la procédure d'appel prévue, la Commission a rappelé que chaque procédure d'appel doit être prévue dans une base légale spécifique. La proposition de disposition légale en question étant trop large et vague, la Commission a précisé que, lorsque des données sensibles sont concernées, une base légale au sens formel et suffisamment détaillée est nécessaire, d'autant plus que le risque d'abus dans le cadre des procédures d'appel est plus élevé. Par ailleurs, cette loi autorise le Conseil d'Etat d'édicter les dispositions d'exécution concernant l'accès aux données et aux autorisations. Dans ce cadre, la Commission préconise de prévoir une procédure analogue à celle de l'accès aux données de la plateforme Fri-Pers et de nommer l'Autorité comme autorité de préavis. Pour rappel, il est mentionné que le contribuable a le droit de consulter à tout moment les pièces du dossier qu'il a produites ou signées. Enfin, la Commission a estimé qu'il était prématuré de prévoir une destruction des documents sur support papier, n'étant pas certaine qu'il existe à l'heure actuelle un système garantissant l'équivalence des deux supports.

**Projet d'Ordonnance relative à l'Espace santé-social**

L'Etat de Fribourg souhaite mettre à disposition de son personnel une consultation spécialisée nommée «Espace santé-social» intervenant notamment dans les domaines tels que l'atteinte à l'intégrité, les risques psychosociaux au travail ou encore les problèmes financiers et personnels. C'est dans ce cadre que la Commission a été consultée par la Direction des finances au sujet de ce projet d'ordonnance. Elle a relevé que les données traitées dans le contexte de l'espace santé-social sont des données sensibles exigeant un devoir de diligence accru lors de leur traitement pour prévenir le risque accru d'atteinte y relatif (cf. art. 3 let. c et art. 8 LPrD). La Commission a rappelé que la garantie de la confidentialité de la démarche ainsi que celle de son contenu sont primordiales. Dès lors, une communication peut avoir lieu seulement si une base légale formelle la prévoit (cf. art. 10 al. 1 let. a LPrD), notamment dans le Code pénal, ou s'il y a un danger pour le collaborateur. Il est rappelé que les données personnelles doivent être recueillies en principe auprès de la personne concernée (cf. art. 9 al. 1 LPrD). Aucune collecte de données par l'intermédiaire d'une base de données ne peut se faire sans l'accord explicite du collaborateur concerné. Enfin, la Commission a souligné que des mesures techniques et organisationnelles doivent être mises en place afin que le SPO ne puisse pas avoir connaissance des accès effectués par l'Espace santé-social via HR-Access.

**Modification de l'Ordonnance sur la partie générale du droit des assurances sociales – dispositions d'exécution relatives à l'observation des assurés**

Dans le cadre du projet d'Ordonnance sur la partie générale du droit des assurances sociales introduisant des dispositions d'exécution relatives à l'observation des assurés, la Commission a soulevé que, sous l'angle de la protection des données, les dispositions relatives à la gestion et à la conservation des dossiers ne s'adressent qu'aux assureurs. Elle propose donc que l'Ordonnance règle également les modalités de gestion et de conservation des dossiers établis par les spécialistes, ceux qui effectuent les observations, et qu'elle définisse clairement les règles auxquelles ils sont soumis concernant la protection et la sécurité des données. Dans ce domaine sensible des observations dans le cadre des assurances sociales, la Commission juge nécessaire que le Conseil fédéral détermine clairement les obligations des spécialistes en matière de protection des données et que ces obligations figurent explicitement dans l'Ordonnance.

### 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, comme le démontrent les exemples suivants. Notamment, les projets informatiques sont régulièrement à l'ordre du jour de la Commission.

Durant l'année sous rapport, 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.

La Commission a également traité divers dossiers en lien avec la digitalisation de l'administration cantonale (cf. Plan directeur de la digitalisation et de ses systèmes d'information). Elle s'est notamment penchée sur divers projets pilotes qui ont pu être mis en œuvre grâce à la base légale de la Loi sur la cyberadministration et le préavis positif de la Commission. Un autre projet qu'accompagne la Commission est celui de la mise en œuvre d'un système de référentiels cantonal, prévu comme base de données pour toute l'administration.

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, 71 demandes d'accès ont été déposées auprès des organes publics fribourgeois en 2018. Dans 50 cas, les organes publics ont accordé un accès complet et dans 9 cas un accès restreint. Dans 4 cas, l'accès a été différé. Dans 7 cas, l'accès aux documents a été refusé. Dans 1 cas, la demande d'accès est en cours. Les domaines les plus concernés étaient les domaines de l'administration, de l'agriculture, des constructions et des écoles.

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 2018 tandis que d'autres ont investi jusqu'à 30 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'article 22a LPrD 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 2018, la Commission a reçu une copie de 26 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 2018, 15 demandes en médiation ont été introduites auprès de la Préposée à la transparence. Dans 7 cas, un accord a été trouvé, dans 4 cas, la Préposée a émis une recommandation. Les 2 cas de médiation qui étaient encore pendants à la fin de l'année 2017 ont pu être clos en 2018 avec une recommandation. 4 cas de médiation sont encore pendants.

Dans le premier cas qui était encore pendant fin 2017, il s'agissait d'une demande d'accéder à des documents en rapport avec des **subventions accordées à des organisateurs d'évènements culturels.** Une association culturelle a demandé à l'Agglomération de Fribourg l'accès à la liste de tous les bénéficiaires de subventions entre les années 2010 et 2017 ainsi qu'aux montants qui leur ont été accordés, aux dossiers qu'ils ont introduits, et à toutes les décisions de refus total ou partiel pour la même période. Etant donné qu'elle n'a obtenu qu'une partie des documents demandés, l'association a déposé une demande en médiation auprès de l'Autorité par le biais d'un avocat, et elle en a par la suite limité la demande d'accès à deux dossiers. Dans sa recommandation, la Préposée a relevé que certains passages des documents demandés risquaient de tomber sous une exception de la LInf et qu'ils devaient par conséquent être caviardés. Elle a cependant estimé qu'un refus d'accès total ne serait pas opportun et qu'un accès partiel aux documents souhaités devrait être accordé.

Dans le deuxième cas qui était encore pendant fin 2017, il s'agissait d'une demande d'accès à une série de **documents relevant du domaine de l'environnement** déposée auprès de plusieurs organes de l'administration cantonale par une personne privée. Après l'écoulement du délai de réponse prévu par la loi, et sans réponse de la part de l'organe public, la personne privée a pris contact avec l'Autorité. Elle a manifesté son mécontentement face à la transmission ultérieure de certains documents demandés. D'autres documents ont été envoyés après la séance de médiation, mais sans contenir les données scientifiques souhaitées. La Préposée à la transparence a, par conséquent, rédigé une recommandation. Dans sa recommandation, elle relève que les organes de l'administration cantonale concernés devraient donner l'accès, selon les règles de la LInf, à tous les documents qui sont encore en leur possession. En ce qui concerne les documents contenant des données scientifiques, la Préposée a conseillé à la requérante de déposer une demande d'accès auprès de l'association où, selon les organes de l'administration cantonale, se trouvent les informations demandées et qui, selon l'analyse effectuée par la Préposée, est directement soumise à la LInf.

La première demande en médiation de l'année 2018 a été introduite par un journaliste qui, après avoir demandé l'accès à un **rapport du Service du médecin cantonal** concernant un établissement médico-social auprès de la Direction de la santé et des affaires sociales, a reçu une réponse négative. Pendant la procédure de médiation, il s'est avéré que le rapport demandé faisait partie d'une procédure administrative en cours devant la Préfecture et, par conséquent, la LInf n'était pas applicable. Le journaliste a demandé à la Préposée de clore le dossier.

La deuxième demande en médiation a été soumise par le même journaliste suite au dépôt d'une demande auprès de la ville de Bulle pour l'accès à plusieurs **documents relatifs au réaménagement du centre-ville.** L'accès aux documents demandés a été refusé. Après la séance préparatoire organisée par la Préposée à la transparence avec les autorités de la ville, le journaliste a décidé de renoncer à sa demande et le dossier a été classé.

Un troisième cas portait sur l'accès à toutes les **décisions exécutoires** rendues entre 2015 et 2017 concernant des interdictions de détention d'animaux ainsi que des interventions des autorités et des recours selon la **loi suisse sur la protection des animaux.** Un avocat avait envoyé une demande d'accès à l'administration cantonale et reçu une réponse négative de la Direction des institutions, de l'agriculture et des forêts en raison d'un intérêt privé prépondérant. La Préposée à la transparence a reconnu dans sa recommandation que cette exception pouvait effectivement s'appliquer à certains passages des documents concernés, mais qu'un refus total d'accès n'était pas proportionné. Elle a estimé qu'un accès partiel devrait être accordé selon les règles de la LInf. Dans sa décision suite à la recommandation, l'organe public a refusé d'octroyer l'accès aux documents.

Deux autres demandes en médiation ont été déposées par un particulier. Il s'agissait dans le premier cas du **discours de Saint-Nicolas** qui avait eu lieu dans une commune en 2017. La Conseillère communale contactée, ne considérant pas la requête du citoyen comme une demande d'accès, a refusé de fournir les documents en question. Après plusieurs contacts entre la Préposée à la transparence et celle-ci, le Conseil communal a donné accès au document demandé. Dans le deuxième cas, le même citoyen cherchait à avoir accès à un **échange de correspondance entre une commune et la Direction de l'instruction publique, de la culture et du sport.** N'ayant pas reçu de réponse à sa demande d'accès dans le délai prévu par la LInf, il a déposé une demande de médiation. La Préposée a contacté la direction concernée et le citoyen a obtenu les documents demandés.

Les sixième et septième demandes de médiation portaient sur un **rapport d'audit** mandaté par le conseil d'administration de l'Hôpital de Fribourg (HFR) en août 2017 afin d'analyser la gouvernance de l'HFR. Plusieurs personnes ont demandé l'accès au document suite à la publication d'un résumé du rapport d'audit et d'un communiqué de presse y relatif en février 2018. L'HFR a ensuite voulu accorder l'accès à une version caviardée, mais deux tiers concernés se sont opposés et ont déposé une demande de médiation. La Préposée à la transparence a ensuite opté pour un caviardage légèrement plus large du rapport et a recommandé d'accorder un accès partiel à l'HFR sous cette forme. Suite à la décision de l'HFR d'accorder l'accès au rapport selon la recommandation de la Préposée, un des tiers a déposé un recours auprès du Tribunal cantonal. Le Tribunal cantonal a rejeté le recours du tiers en constatant qu'un refus complet de l'accès au rapport irait à l'encontre du but de la LInf, le caviardage permettant de préserver suffisamment l'intérêt privé du tiers.

La huitième demande en médiation traitait de l'opposition d'un tiers à une demande d'**accès à une décision d'une préfecture** concernant l'entretien des canalisations d'eaux usées dans un secteur d'une commune du canton. Cette décision tranchait des recours déposés par différents propriétaires du secteur contre une décision de la commune. Après consultation des tiers concernés et malgré l'opposition d'un de ceux-ci, la préfecture s'est déterminée en faveur de l'accès intégral à la décision. Le tiers qui s'y est opposé a alors demandé une médiation auprès de la Préposée en faisant valoir des intérêts privés prépondérants. La Préposée a considéré que les éléments invoqués ne concernaient pas la sphère privée protégée de la personne et ne constituaient dès lors pas des intérêts privés prépondérants pour s'opposer à une demande d'accès. Elle a recommandé d'accorder l'accès à la décision; la préfecture a suivi cette recommandation.

La neuvième demande en médiation portait sur des demandes d'accès à **des documents et informations en lien avec un projet de réglementation d'exécution ECALEX et les directives ECAB** auprès de la Direction de la sécurité et de la justice. Suite à l'intervention de la Préposée, la DSJ a accordé l'accès aux documents en trois étapes, le requérant ayant déclaré que les documents n'étaient pas complets suite aux deux premiers envois, ayant précisé et ajouté certaines demandes. Le recourant a ensuite demandé à l'Autorité de constater que la DSJ avait violé les principes de la célérité et de la bonne foi dans le cadre de ses demandes. L'Autorité a un pouvoir de surveillance de la mise en œuvre du droit d'accès en matière de demandes d'accès, mais la LInf ne se prononce pas sur la question de savoir si c'est la Préposée ou la Commission qui est en charge de cette surveillance. Puisque la Préposée a une tâche de médiation qu'elle a exercée dans cette affaire, la Commission cantonale de la transparence et de la protection des données a exercé ce pouvoir de surveillance. Elle a décidé que la DSJ a traité les requêtes avec la diligence et la célérité requises par la LInf (art. 9 al. 1 LInf) et conformément au principe de la bonne foi (art. 8 al. 2 LInf). Le requérant a fait recours contre cette décision au Tribunal cantonal. Le recours était encore pendant à la fin de l'année.

La dixième demande en médiation concernait une demande d'accès à **un rapport d'un conseil communal ad interim sur son mandat** dans une commune fribourgeoise, demandé par le Préfet de la Sarine. Durant la séance de médiation convoquée par la Préposée, la personne qui a demandé l'accès au rapport et le Préfet sont tombés d'accord sur le fait de prévoir un échange sur le contenu de ce rapport. Le requérant a demandé à la Préposée de suspendre sa requête en médiation. La requête était toujours suspendue à la fin de l'année.

La onzième demande en médiation émanait d'une personne qui a demandé à avoir accès à des **procès-verbaux d'une commission parlementaire du Grand Conseil.** Les procès-verbaux de séances non-publiques sont des cas particuliers pour lesquels la LInf prévoit que l'accès est exclu. Durant la séance de médiation convoquée par la Préposée, l'organe public a informé le requérant que les procès-verbaux demandés ne contenaient pas les informations recherchées par le requérant. Le requérant a invité la Préposée à procéder au classement du dossier.

La douzième demande en médiation concernait une demande d'accès auprès de la Direction de l'aménagement, de l'environnement et des constructions à des **documents en lien avec le subventionnement fédéral du projet Poya, ainsi que la correspondance** entre la DAEC et l'Office fédéral des routes depuis le 30 septembre 2016. Après l'intervention de la Préposée, la DAEC a fourni les documents requis avant la séance de médiation. Durant la séance, le requérant a convenu avec la DAEC que celle-ci allait s'assurer d'avoir bien transmis toute la correspondance demandée, et il a invité la Préposée à clore le dossier.

La treizième demande en médiation portait sur **divers documents et informations détenus par l'ECAB.** Malgré le fait que le requérant a refusé de participer à la séance de médiation convoquée par la Préposée, l'ECAB a fourni des informations et des documents au requérant. Ce cas était encore pendant à la fin de l'année sous rapport.

La quatorzième demande en médiation concernait des **mesures contre le bruit** effectuées par la DAEC sur les routes cantonales fribourgeoises. La Préposée a convoqué une séance de médiation, mais qui n'a plus pu avoir lieu pendant l'année sous rapport. Ce cas était encore pendant à la fin de l'année sous rapport.

La quinzième demande en médiation émanait d'une journaliste et portait sur un **rapport d'enquête administrative d'une commune fribourgeoise.** La Préposée a convoqué une séance de médiation, mais qui n'a plus pu avoir lieu pendant l'année sous rapport. 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 lorsque celui-ci se récuse, la Préposée à la transparence n'a traité aucun dossier en 2018.

### 1.3. Demandes

Durant l'année sous rapport, des 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 décisions relatives à des procédures administratives, d'archives, de documents en lien avec l'aménagement du territoire, la construction, le trafic routier, ou encore de documents d'assemblées générales d'une association intercommunale.

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 2018 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.

## 2. Statistiques

Durant la période considérée, 112 dossiers ont été introduits, dont 25 sont pendants au 1er janvier 2019, 31 conseils et renseignements, 7 avis, 28 examens de dispositions législatives, 9 présentations, 18 participations à des séances et autres manifestations, 15 demandes en médiation et 4 demandes diverses. 53 dossiers concernent des organes cantonaux ou des institutions chargées de tâches publiques, 9 des communes, 19 d'autres organismes publics (cantons, autorités de transparence et protection des données), 22 des particuliers ou institutions privées et 9 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.

En 2018, la Préposée à la protection des données a traité divers dossiers concernant des projets préliminaires du SITel traitant des données personnelles. De plus, elle a participé à plusieurs groupes de travail (système de référentiel cantonal, projets pilotes pour des solutions Cloud). Enfin, la Préposée gère le groupe de travail, au sein duquel sont représentés de nombreux services et directions de l'Etat, groupe de travail relatif à la révision de la loi sur la protection des données et son adaptation à la législation européenne, activité possible grâce au soutien d'un collaborateur du SLeg. Pour ce faire, un groupe restreint de travail est amené à faire des propositions quant au contenu de chaque disposition légale et à effectuer des recherches légales, jurisprudentielles et doctrinales relatives à la révision.

La Préposée à la protection des données est membre du groupe d'accompagnement du projet Cybersanté et a participé à plusieurs séances en 2018. Sous le terme «Cybersanté», il faut entendre le projet de mise en œuvre, par exemple, du dossier électronique du patient selon la loi fédérale y relative et ses projets. Le canton apporte sa contribution à la création des conditions cadres nécessaires à cet effet.

La Préposée a, en outre, traité plusieurs dossiers communs avec la Préposée à la transparence, à savoir lorsque la demande touche les domaines de la transparence et de la protection des données.

La Préposée à la protection des données a tiré parti des possibilités d'échange bilatéral et de sensibilisation dès qu'elle en a eu l'occasion, par exemple dans le cadre des discussions avec la HESSO/FR, le centre de compétences Fritic concernant les directives relatives à l'utilisation d'Internet ou des questions d'organisations privées chargées de tâches publiques.
La Préposée et ses collaboratrices ont pris part à plusieurs formations continues, notamment de sensibilisations internes.

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

**Communication de données par un service à un autre**
*Vérification légale d'une solution informatique pour un échange sécurisé de données personnelles et confidentielles entre une autorité judiciaire et un établissement*
Lors de la mise en place d'un échange de données personnelles et confidentielles, l'autorité judiciaire a souhaité que le SITel certifie que le procédé technique choisi satisfasse aux exigences de la protection des données. Il ressort des discussions que les données doivent être enregistrées sur des serveurs du SITel, qu'une convention entre les deux entités et le SITel doit être conclue afin de régler la procédure et les droits d'accès de chaque service, qu'un effacement des données dans les 24 heures suite à l'envoi soit paramétré et que le site soit exclu de la recherche pour éviter que les informations soient retrouvées.

**Protection des données et contrôle des habitants**

*Communication au contrôle des habitants de données personnelles des gérances immobilières*

L'Autorité a été contactée au sujet de la communication systématique de données personnelles des gérances immobilières au contrôle des habitants. En effet, les données personnelles d'une habitante ont été transmises directement par sa gérance au contrôle des habitants et ce avant qu'elle n'ait pu s'acquitter de son obligation légale de s'annoncer. L'Autorité a rappelé que le législateur fribourgeois n'a autorisé la recherche de renseignements auprès des bailleurs et gérants d'immeubles qu'à titre subsidiaire, lorsque la personne n'a pas transmis ou transmis de manière incomplète ces informations. Ainsi, une pratique d'échange systématique de données n'est pas prévue par la législation cantonale (cf. art. 8a LCH et art. 10 LPrD).

**Protection des données et travail**

*Contrôle des courriers électroniques des collaborateurs de l'Etat*

L'Autorité a été sollicitée dans le cadre d'une enquête au sujet de la transmission d'un courriel confidentiel envoyé à plusieurs collaborateurs ainsi qu'à d'autres personnes au sein ou en dehors de l'administration cantonale. L'Autorité a rappelé que, selon l'Ordonnance relative à la surveillance de l'utilisation d'Internet par le personnel de l'Etat, des contrôles personnalisés peuvent être effectués si les contrôles globaux (relatifs au volume du courrier électronique) ou d'autres constatations mettent en évidence des indices d'abus. Si des indices d'abus concernant certains collaborateurs venaient à être mis en exergue, tout en tenant compte du principe de la proportionnalité, le contrôle se limite alors au nombre de messages envoyés et reçus, aux éléments d'adressage, aux types et volumes de fichiers attachés. En aucun cas, il ne porte sur le contenu du message (cf. art. 8 de l'Ordonnance). Ainsi, en cas d'abus relevé, le SITel est habilité à vérifier si le collaborateur visé a transmis le courriel confidentiel à d'autres personnes ainsi que la liste des destinataires. En revanche, si aucun abus n'est observé, le contrôle personnalisé ne pourra être réalisé.

*Production des attestations de rendez-vous médicaux*

L'Autorité a été consultée dans le but d'obtenir des informations relatives aux attestations de rendez-vous médicaux, demandées pour que le collaborateur puisse comptabiliser ses heures. Dans les Directives relatives à la gestion et à la saisie du temps de travail, le SPO a prévu qu'en cas de visite médicale un justificatif peut être demandé, donnant alors une certaine marge d'appréciation au Service. Une pièce justificative n'est pas obligatoirement un certificat médical, mais peut être une attestation de rendez-vous ou une autre confirmation. L'Autorité est d'avis que demander d'une manière systématique une attestation de rendez-vous médical faisant ainsi connaître le nom du médecin traitant, et notamment sa spécialisation par laquelle l'employeur peut déduire la nature de la maladie, n'est pas proportionnelle et contraire aux principes de la protection des données. L'Autorité estime qu'il est normal de demander une attestation lorsque surviennent des doutes d'abus ou en cas d'absences répétitives.

**Protection des données et école**

*Transmission de données et photos à l'école pour un travail*

L'Autorité a été contactée au sujet d'un projet scolaire visant la réalisation d'un arbre généalogique accompagné d'une rédaction. Pour cela, les élèves avaient comme devoir d'apporter en classe les noms, prénoms, photos ou encore dates de naissance et éventuellement de décès des membres de leur famille. Il semblerait qu'il n'ait pas été précisé aux élèves, ainsi qu'à leurs parents, quel allait être le sort du traitement des données personnelles, qui s'en chargerait et à quelles fins ces dernières seraient utilisées. Le traitement des données ayant trait aux enfants est toujours sensible, d'autant plus lorsque leur utilisation et le nom de son responsable ne sont pas expressément communiqués aux personnes

concernées. Dans ce contexte, l'Autorité a rappelé que différents projets pédagogiques peuvent être menés afin d'améliorer la qualité de l'école et de garantir son adaptation à l'évolution de la société (cf. art. 24 de la Loi sur la scolarité obligatoire), mais qu'il est toutefois interdit aux enseignants de divulguer à des tiers des informations relatives à la vie privée des élèves ou de leurs proches dont ils ont eu connaissance dans le cadre de leur travail (cf. art. 42 de la Loi sur la scolarité obligatoire).

*Communiqué de presse affichant des photographies d'enfants*
L'Autorité de la protection des données s'est assurée que le Service de la culture a pris toutes les mesures nécessaires relatives aux photographies affichant des enfants lors de la promotion d'un festival culturel. En effet, les annexes d'un communiqué de presse du festival culturel comprenaient des photographies affichant des visages d'enfants clairement identifiables. L'Autorité a tenu à saluer le fait que le Service de la culture ait pris les mesures nécessaires concernant la publication de ces images. L'Autorité a tenu à rappeler que lorsque des enfants sont concernés, la protection de leur sphère privée est primordiale et ne doit souffrir aucune exception. Ainsi, les images d'enfants ne doivent pas être publiées à moins que certaines conditions strictes soient respectées, par exemple les photos contiennent uniquement des vues générales, la prise de vue est suffisamment éloignée pour qu'aucun enfant ne puisse être reconnu, le consentement est obtenu des parents si l'enfant est mineur et de lui-même si l'élève est majeur.

*Formulaire de consentement relatif à la publication de photographies, de films ou d'enregistrements lors d'événements scolaires*
Durant l'année scolaire, il n'est pas rare que les élèves soient photographiés, filmés ou/et enregistrés dans le cadre d'activités ordinaires, telles que les journées sportives, courses d'école, cérémonies de promotion ou de remises des diplômes. Ces données peuvent être diffusées sur le site Internet ou Intranet de l'école, voire sur les réseaux sociaux et/ou publiées dans le journal interne de l'école, voire dans la presse, à certaines conditions. Afin de fournir une information la plus transparente possible aux représentants légaux et aux élèves majeurs et pour demander leur autorisation d'utiliser et de publier ces données prises lors d'événements scolaires, une école professionnelle du canton de Fribourg a soumis un formulaire de consentement à l'Autorité. La Préposée à la protection des données salue l'initiative et en particulier le fait que le consentement soit limité dans le temps, à savoir par année scolaire, et que le représentant légal ou l'élève majeur puisse choisir sur quels supports il autorise ou pas l'utilisation et la publication de ses données. Toutefois, il est rappelé que ce n'est pas dans les tâches de l'école de publier des images des élèves. Une publication ne peut être effectuée qu'avec le consentement explicite de la personne concernée, respectivement de son représentant légal, et ne doit contenir que le prénom de l'élève. En cas de refus, l'Autorité rappelle que l'école devrait alors prendre des mesures afin de ne pas publier de portrait de cet élève et de le flouter sur les photos de groupe.

**Protection des données et santé**
*Enregistrement électronique des dossiers patients et hébergement dans un Cloud*
Une société en charge de prestations médicales spécifiques dans une clinique a abordé l'Autorité afin de savoir s'il était possible d'héberger les dossiers patients dans un Cloud. L'Autorité a rappelé qu'une clinique externalisant certaines prestations médicales vers une société, sur approbation de la Direction de la santé et des affaires sociales, demeure responsable de la protection des données y relatives. De ce fait, elle doit prendre l'ensemble des dispositions nécessaires pour prévenir le risque accru d'atteinte que comporte le traitement de données sensibles. En l'espèce, la société chargée de ces prestations a délégué, à son tour, le traitement des données à un tiers, suite à l'aval de la clinique, en collaboration avec la DSAS. L'Autorité a précisé que l'hébergement et le stockage des données dans un Cloud sont soumis à des conditions strictes, telles que par exemple l'utilisation d'un nuage privé. N'ayant pas eu

à disposition les informations nécessaires, l'Autorité n'a pas pu analyser si la solution choisie par la société est conforme à la législation en matière de protection des données. Enfin, l'Autorité a constaté que la Convention entre la clinique et la société ainsi que le contrat entre la société et le tiers chargé du traitement des données sont lacunaires. Elles ne contiennent aucune instruction relative à la protection des données.

*Application de la loi fédérale et cantonale à la protection des données*
Une société anonyme à but non lucratif en charge de recherches et de développement dans le domaine de la santé a abordé l'Autorité dans la mesure où elle souhaite établir des directives relatives à la protection des données. A cette fin, elle souhaite savoir si c'est la législation fédérale ou cantonale sur la protection des données qui lui est applicable, puisqu'elle est une société privée dont l'actionnaire unique est l'Université de Fribourg. En tenant compte de son but non lucratif et principal, de ce qui ressort de ses statuts tels que le contrôle du transfert des actions, de l'indemnisation du Conseil d'administration et de la soumission du Rapport d'activité au Conseil d'Etat, l'Autorité est arrivée à la conclusion que la société est soumise tant à la loi fédérale (LPD) pour les activités purement privées, qu'à la loi cantonale (LPrD) pour les tâches publiques qui sont dévolues par l'Université et qui ressortent de la loi. Il en résulte que les données contenues dans les banques de données et les biobanques doivent être séparées: d'une part les données provenant d'organes publics (tels que les hôpitaux) qui sont soumises à la LPrD et d'autre part les données provenant d'entreprises privées qui sont soumises à la LPD. Si cette séparation s'avère techniquement impossible ou trop coûteuse, l'Autorité est d'avis que les règles les plus strictes seront appliquées, à savoir celles de la LPrD. De ce fait, les mandats externalisés par la société doivent être soumis pour approbation à la Direction concernée.

*Dossier médical informatisé du détenu*
Dans le cadre du projet du dossier médical informatisé du détenu, l'Autorité a été consultée afin de lui soumettre la solution informatique choisie pour héberger les dossiers de santé auprès d'une société privée. Après l'analyse de différents documents transmis tels que le contrat d'hébergement, le concept de la sûreté de l'information et de la protection des données et les spécifications des interfaces, l'Autorité a rappelé que les services concernés demeurent responsables des données lors d'une externalisation. Dans ce contexte, ils doivent donner les instructions nécessaires relatives à la sécurité informatique et des données à l'entreprise privée par le biais d'un contrat. En l'espèce, il y a non seulement une externalisation du traitement des données mais également une sous-traitance, à savoir que l'entreprise mandatée pour la solution informatique héberge les données médicales auprès d'un autre prestataire privé, de sorte qu'un contrat de sous-traitance doit également être conclu entre le mandataire et le sous-traitant. Par conséquent, il est nécessaire que les deux contrats contiennent les conditions strictes de l'Etat, en particulier celles concernant la confidentialité, le chiffrement, les droits d'accès, la durée de conservation des données et la disponibilité des données, qu'ils soient approuvés par la DSJ et soient conformes entre eux. Au niveau de l'authentification, l'Autorité a précisé que, dans la mesure où les données sensibles sont accessibles par des utilisateurs internes et externes à l'Etat, il s'agira de mettre en place une authentification forte pour les accès des externes.

*Analyse de formulaire de consentement général de collecte des données auprès de patients pour la création d'une biobanque élaboré par l'Académie suisse des sciences médicales*
L'Autorité a été abordée au sujet de la légalité d'un formulaire de consentement général relatif à la collecte de données et d'échantillons auprès de patients pour la création d'une biobanque. Ce formulaire vise à faciliter la recherche dans le domaine médical en Suisse et à l'étranger. Après renseignements auprès de l'HFR, ce dernier a confirmé ne pas faire usage de ce modèle de consentement.
L'Autorité a précisé que le dossier médical, faisant partie des données transmissibles selon le

formulaire, contient énormément de pièces difficiles à anonymiser. Par ailleurs, l'article 7 alinéa 2 de la Loi relative à la recherche sur l'être humain prévoit expressément que la personne concernée a le droit, à tout moment, de refuser de participer à un projet de recherche sans avoir à observer une procédure particulière. Cependant, l'Autorité a relevé que le formulaire ne prévoit pas de possibilité claire pour le patient de s'opposer totalement à ce que ses données soient collectées et utilisées pour la recherche. Pour ce faire, seule une démarche active supplémentaire de la part du patient est prévue. En outre, les explications relatives aux pratiques de codages et d'anonymisation des données manquent de clarté.

*Transmission de données d'une association au Service de l'enfance et de la jeunesse*
Une association à but non lucratif a contacté l'Autorité afin de savoir s'il était conforme à la protection des données, que celle-ci doive systématiquement transmettre au Service de l'enfance et de la jeunesse la copie du formulaire d'admission à un programme type, avant de commencer un accompagnement des jeunes. L'Autorité est d'avis qu'il n'existe pas une base légale suffisante pour justifier la transmission systématique au SEJ des données sensibles contenues dans le formulaire. La confidentialité des données semble essentielle à l'efficacité d'un tel programme de prévention, c'est pourquoi chaque mesure prise doit être dans l'intérêt unique des participants. Dès lors, l'Autorité estime que la transmission des données se justifierait uniquement dans certains cas, soit lorsque le programme n'est pas efficace, que le participant se trouve dans une situation de danger ou encore qu'il est dans son intérêt d'annoncer le cas au SEJ pour qu'il prenne les mesures de soutien appropriées (cf. art. 22 al. 1 let. a LEJ). En l'espèce, la communication au SEJ du nombre de participants est suffisante pour les données statistiques et l'octroi du subventionnement dû. Pour conclure, l'Autorité suggère de compléter le formulaire d'admission dans la mesure où, le but et la base légale du traitement des données ainsi que les destinataires devraient y figurer, ces données sont collectées de manière systématique (cf. art. 9 al. 3 LPrD).

*Accès au dossier médical d'un patient décédé*
Un particulier a approché l'Autorité car il souhaitait avoir accès au dossier médical de son père décédé. L'Autorité a rappelé que le dossier de santé du patient est protégé par le secret médical et ce même après le décès de la personne. Toutefois, les proches de la personne ou des tiers peuvent avoir accès à certaines informations pertinentes après que le médecin se soit fait délier du secret professionnel par une décision de la Direction de la santé et des affaires sociales (cf. art. 90 al. 1 LSan).

**Protection des données et aide sociale**
*Communication de données par un service social à une commune - Accès des communes à la liste des personnes bénéficiant de l'aide pour le paiement des primes d'assurance RC ménage*
L'Autorité a été approchée par un service social afin de savoir s'il était conforme à la protection des données de communiquer aux communes l'identité des personnes bénéficiant de l'aide communale pour le paiement de la prime incendie inclue dans l'assurance RC ménage. En effet, les communes doivent prendre en charge le paiement des primes des personnes nécessiteuses qui ne sont pas à même de s'en acquitter (cf. art. 5 al. 2 de la Loi sur l'assurance obligatoire du mobilier contre l'incendie). Dans ce contexte, l'Autorité a informé le Service social que le fait d'être bénéficiaire de l'aide sociale constitue une donnée sensible et qu'il est donc nécessaire qu'une base légale formelle existe pour communiquer ces données (cf. art. 3 et 8 LPrD). Cependant, l'Autorité a relevé que la loi ne prévoyait pas la communication de l'identité des bénéficiaires aux communes, de sorte que ces informations ne sont pas nécessaires à l'accomplissement de leur tâche. Enfin, elle a précisé que la raison pour laquelle

la tâche de l'aide sociale a été confiée à un organe séparé de la commune a précisément pour but de préserver la confidentialité quant à l'identité des bénéficiaires de l'aide sociale à l'égard des communes. Si l'identité de ces personnes était communiquée aux communes, cela dénuerait le principe de tout sens.

Dans un autre dossier, l'Autorité a retenu qu'il n'existait pas de base légale prévoyant la communication systématique d'informations concernant des dossiers d'aide sociale au Conseil communal et que le consentement tacite n'est pas prévu dans ce cas-là. Ainsi, l'Autorité a conclu que toute transmission d'informations par le service social est exclue, excepté la décision de la commission sociale. Or, la transmission de données sous forme anonymisée est par contre possible à des fins de statistiques.

*Questions relatives au secret de fonction et à la protection des données au sein du service social*
Un service social voulait savoir s'il était possible, dans le respect du secret de fonction, de demander l'adresse d'anciens bénéficiaires auprès de certaines communes afin de vérifier la possibilité de remboursement. L'Autorité a rappelé que, conformément à l'article 28 LASoc, les employés doivent respecter le secret de fonction et les bénéficiaires sont tenus de coopérer, de renseigner le service (art. 24 LASoc) également lors de la procédure de remboursement. Lorsqu'un service d'aide sociale souhaite obtenir des informations sur un bénéficiaire auprès d'un organe public, il s'agit d'une collecte de données et en même temps d'une divulgation de données relative au nom du bénéficiaire. Sous l'angle de la protection des données, le service d'aide sociale doit disposer d'une base légale qui permet, d'une part, de collecter et, d'autre part, de divulguer ces données. En même temps, l'organe d'entraide doit être autorisé à transmettre ces données. Dans le cas d'espèce, l'Autorité a suggéré de demander l'accès à la plateforme informatique cantonale Fri-Pers qui contient les données des habitants du canton. En cas de déménagement hors canton, une communication ne peut se faire que dans un cas d'espèce.

**Protection des données et données fiscales**
*Demande d'accès*
La Commission s'est prononcée sur une décision rendue par le SCC refusant l'accès d'un particulier à des informations relatives à l'une de ses procédures fiscales closes et à l'écriture comptable d'un transfert d'impôts d'un contribuable à un autre. Elle a rappelé que l'exercice du droit d'accès par une personne aux données la concernant n'est en principe soumis à aucune condition et n'est pas limité dans le temps, sauf s'il s'agit de consulter des données archivées. Le requérant n'est pas tenu de se référer à un fichier déterminé et peut demander à accéder à toutes les données contenues dans un fichier dont l'organe public abordé est le responsable. Le droit de la personne à être renseigné sur les données recueillies la concernant s'étend à la fois aux données de base, telles qu'elles sont enregistrées, et à celles qui résultent de leur traitement. Le responsable du fichier peut refuser, restreindre ou différer la communication des renseignements si et dans la mesure où un intérêt public le commande ou l'intérêt digne de protection d'un tiers l'exige. Il doit indiquer le motif de refus dans une décision (art. 25 LPrD). L'Autorité a souligné que les droits d'accès doivent être respectés même si la personne concernée est largement connue des institutions fribourgeoises.

*Transmission au SCC des états locatifs du parc immobilier d'une fondation*
L'Autorité a été contactée pour savoir s'il était conforme à la protection des données qu'une fondation en faveur du logement transmette au SCC les états locatifs complets de ses parcs immobiliers contenant notamment les nom, prénom et loyer payé par ses locataires. En effet, la fondation bénéficie d'une exonération fiscale à condition de remplir le critère d'exclusivité d'attribution des logements à des personnes nécessiteuses. L'Autorité a précisé que les données personnelles ne peuvent être

communiquées de manière systématique que si une base légale le prévoit (cf. art. 4 et 10 al. 1 LPrD) et ne doivent être traitées que dans le but pour lequel elles ont été collectées ou dans un but qui, selon les règles de la bonne foi, est compatible avec lui (cf. art. 5 LPrD). En l'espèce, l'Autorité a relevé que le SCC ne s'appuie sur aucune disposition légale qui pourrait justifier la transmission systématique de ces données et la communication des données relatives aux locataires constitue un changement de finalité du traitement qui nécessite le consentement préalable de la personne concernée, les données étant collectées afin de gérer les contrats de bail uniquement.

*Communication de données du SCC aux communes*
En leur qualité d'autorités de taxation, les communes bénéficient d'une collaboration privilégiée avec le SCC, en particulier concernant l'échange de données fiscales. Ces échanges se font par le biais d'une plateforme informatique sécurisée. Afin de rappeler l'importance du secret fiscal et de la protection des données au personnel communal, le SCC souhaite insérer un avertissement qui apparaitrait avant chaque téléchargement de données fiscales. A cette fin, le SCC a soumis le projet à l'Autorité dans la mesure où cela touche à la protection des données.

**Protection des données et construction**
*Délimitation entre les règles sur l'archivage, le droit d'accès selon la LInf et la protection des données*
Un archiviste a approché l'Autorité afin de connaître les articulations entre la Loi sur l'archivage, la LInf et la protection des données dans le cadre d'une demande d'accès à un permis de construire datant de 1930. En effet, la LInf s'applique à la consultation des archives historiques tant que le délai de protection de celles-ci n'a pas expiré (cf. art. 14 al. 1 LArch). Le délai passé, la consultation est libre. Selon l'Autorité, l'accès à des plans d'une construction privée datant de 1930 contenant le nom des propriétaires de l'époque comporte alors des données personnelles de l'époque. Toutefois, ces données devraient à première vue pouvoir être accessibles à la personne qui désire consulter les archives. S'il est constaté que le dossier contient des données sensibles (cf. l'art. 3 al. 1 let. c de la LPrD), un caviardage de ces données sensibles peut être dans ces cas nécessaire. L'Autorité a rappelé qu'il est par ailleurs possible de permettre la consultation du document demandé, en mettant de côté les éventuels autres documents du dossier.

*Publication de plans de constructions sur des sites Internet de communes*
Selon le Règlement d'exécution de la loi sur l'aménagement du territoire, dès l'acceptation du dossier complet, la commune publie les coordonnées cartographiques dans la Feuille officielle ou utilise pour ce faire tout autre moyen de communication dont elle dispose (cf. art. 92 al. 1). L'Autorité a estimé que la publication de l'intégralité des plans des constructions mis à l'enquête sur le site Internet des communes va trop loin et dépasse «les coordonnées cartographiques» et a donc proposé de publier uniquement l'avis, permettant ainsi aux personnes intéressées de consulter les plans sur place par exemple.

*Transmission d'informations relatives aux permis de construire par les communes à une revue médiatique*
L'Autorité a été consultée par une administration communale, laquelle est régulièrement contactée par une revue sollicitant les informations relatives à des demandes de permis de construire pendantes. L'Autorité a rédigé une note à l'attention des préfectures concernant la transmission de données relatives à des projets de construction. Il ressort de cette dernière qu'il y a lieu de distinguer différents cas de figure. 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 et c'est la LPrD qui s'applique. Si par contre l'autorité statue sur recours, ce sont les dispositions du CPJA qui s'appliquent. Lorsque la

procédure du permis de construire est close et le permis de construire entré en force, il n'existe alors plus aucun moyen de recours contre la décision et c'est la LInf qui s'applique. Encore convient-il de rappeler que les entreprises intéressées peuvent obtenir les informations durant la mise à l'enquête publique ou directement auprès des propriétaires concernés.

**Protection des données et sécurité d'information**

*Politique de confidentialité pour le nouveau site de l'Etat de Fribourg*

L'Autorité a été consultée dans le cadre du projet du futur site web de l'Etat de Fribourg, notamment concernant l'impressum et la Politique de confidentialité du website. L'Autorité salue les mesures mises en place pour informer l'utilisateur des données qui sont collectées lors de sa visite du site. Elle conseille d'installer un lien pour désactiver les cookies permettant de reconnaître l'utilisateur lors de sa prochaine visite, respectivement d'expliquer à l'utilisateur comment il peut faire pour révoquer son accord initial de les accepter. Pour l'analyse de l'utilisation du site par Google Analytics, les données doivent être anonymisées, notamment l'adresse IP. L'Autorité suggère de mentionner que le site web fr.ch ne collecte pas de données personnelles, excepté le numéro IP qui est anonymisé et les données personnelles que l'utilisateur transmet lors d'une prise de contact.

*Caviardage des données personnelles des documents classés dans PLASTA*

L'Autorité a été contactée par un service afin de savoir si leur pratique concernant la tenue des dossiers des assurés était conforme à la protection des données, notamment dans le cadre de l'utilisation de son système d'information en matière de placement et de statistique du marché du travail (PLASTA). Afin de garantir le droit des personnes à ce que leurs données ne soient pas accessibles à des personnes non-autorisées, l'Autorité a rappelé que le service ne doit traiter que des données personnelles absolument nécessaires et pertinentes pour l'accomplissement de ses tâches, ce qui s'exprime dans les droits d'accès différenciés. Il doit par ailleurs prendre toutes les mesures organisationnelles et techniques appropriées contre tout traitement non-autorisé des données.

*Fichiers des lecteurs d'une bibliothèque hébergés dans un Cloud d'une entreprise privée dont le siège se situe en Allemagne*

Dans le cadre d'une nouvelle plateforme d'échange entre les bibliothèques suisses, les bibliothèques du canton de Fribourg étudient la possibilité d'adhérer à ce projet. La nouvelle application va gérer l'accès aux documents et le prêt. Pour ce faire, elle se basera sur un fichier des lecteurs contenant des données personnelles. En l'espèce, un mandat va être conclu entre les bibliothèques du canton et une société privée, laquelle a pour actionnaires les différentes Universités et Hautes Ecoles de Suisse. Cette dernière souhaite sous-traiter l'hébergement des fichiers de lecteur auprès d'un prestataire privé qui met à disposition un Cloud. S'agissant d'une externalisation de données, l'Autorité rappelle que les contrats de mandat et de sous-traitance doivent être négociés et contenir les instructions nécessaires relatives à la protection et à la sécurité des données de l'Etat, en particulier concernant la confidentialité, les droits d'accès, le chiffrement, la journalisation ainsi que le lieu d'hébergement. Pour des tests de migration des données, l'Autorité demande d'informer tant les utilisateurs actifs que passifs. L'Autorité regrette toutefois que l'utilisateur n'ait pas le choix de refuser la transmission de ses données. Dans ce cas, il devra consulter les ouvrages directement sur place. Enfin, l'Autorité rappelle que le sous-traitant qui a son siège en Europe est soumis au RGPD. Toutefois, il est également possible qu'il soit soumis au Cloud Act et que, de ce fait, des données soient transmises aux autorités étrangères. Aux dernières nouvelles, l'Autorité est informée que les migrations test seront effectuées avec des données anonymes.

*Avertissement relatif à la sécurité de données publiques*
Par l'intermédiaire de privatim, une dénonciation relative à des failles de sécurité informatique concernant un registre a été transmise à l'Autorité. Afin d'y remédier dans les plus brefs délais et de prévenir les organes et services concernés, l'Autorité a informé les personnes responsables au sein de l'administration afin que ces dernières prennent les mesures utiles. A cette fin, l'Autorité recommande vivement aux organes et services concernés de demander des actions immédiates afin que les standards de sécurité soient respectés. Le SITel a été abordé dans ce sens pour transmettre la liste des mesures minimales à respecter pour une application de ce type. Il est relevé que cette dénonciation a été communiquée par privatim à tous les cantons.

**Protection des données et projets de digitalisation 4.0**
Les exemples suivants démontrent la complexité toujours grandissante des projets. En effet, d'une part, ils mélangent des données et partenaires privés et publics limitant la compétence de l'Autorité a une partie du projet uniquement. D'autre part, les projets sont toujours plus denses et s'étendent sur plusieurs années. Pour rappel, le Préposé fédéral à la protection des données est compétent en ce qui concerne le traitement de données par des privés et des organes publics fédéraux.

*Plateforme de gestion et d'information recensant des données relatives à un projet de recherche*
Une haute école du canton de Fribourg a obtenu un projet de recherche ayant pour buts d'établir une vue d'ensemble actuelle du marché immobilier du canton, de pouvoir anticiper les tendances et d'aider les différents partenaires fribourgeois concernés dans leurs prises de décisions importantes. L'Autorité a été consultée dans la mesure où une collecte de données personnelles provenant de différentes sources privées et publiques ainsi qu'une interconnexion de ces dernières seront effectuées. Elles vont être hébergées sur une plateforme informatique à laquelle différents partenaires auront accès. S'agissant d'un traitement systématique des données notamment publiques, l'Autorité informe qu'il manque une disposition légale formelle ainsi que des dispositions légales relatives à l'appariement de ces données. Enfin, une procédure d'appel devra être mise en place.

*Collecte des données par les hébergeurs*
L'Autorité a été approchée dans le cadre d'un projet ayant pour but principal de simplifier la collecte des données du client dans les hébergements du canton et de diffuser automatiquement ces informations aux organismes concernés (Office fédéral de la statistique, Police cantonale, Centrale d'encaissement de la taxe de séjour, etc.). Par rapport aux échanges nécessaires avec les organes et services cantonaux, elle a précisé que les hôtes doivent être clairement informés du traitement de leurs données afin d'être transparent notamment sur les données collectées et leurs communications aux organes et à d'autres organismes, leurs traitements, la finalité, les destinataires, ceci au moyen de la publication d'une politique de confidentialité sur son site Internet ainsi que ceux de leurs partenaires d'hébergement.

Concernant l'externalisation des données de l'Etat de Fribourg, à savoir l'utilisation des Clouds, l'Autorité a été confrontée à de nombreux dossiers qui engendraient une grande charge de travail. En voici un aperçu:

*Externalisation du traitement des données de l'Etat de Fribourg (Cloud)*
Le SITel a contacté l'Autorité concernant l'évolution du système de la messagerie «Microsoft Office 365» pour obtenir des informations relatives à la protection des données concernant l'externalisation de certaines données de l'Etat dans des Clouds. Suite à une réponse sommaire de la Préposée à la

protection des données, le SITel sollicite une prise de position de la Commission. Dans ce cadre, cette dernière a évalué l'externalisation du traitement des données des organes publics dans un Cloud suisse ou étranger de manière générale. A ce sujet, elle a établi une note qui est accessible sur le site Internet de l'Autorité.

Il ressort principalement de la réponse de la Commission que les organes publics cantonaux qui prévoient d'externaliser le traitement des données dans un Cloud doivent veiller à respecter la protection des données et demeurent responsable des données. Concernant la sécurité informatique, le SITel en demeure responsable, de sorte qu'il doit prendre les mesures d'organisation et techniques appropriées contre tout traitement non autorisé des données et doit notamment assurer la confidentialité, la disponibilité et l'intégrité des données. La Commission est d'avis qu'un Cloud étatique fribourgeois est la solution la plus à même à limiter les risques liés à la sous-traitance, à la localisation des données, à l'accès des autorités étrangères aux données et à la perte des données et permettrait de garder la maîtrise totale de toutes les données traitées par l'Etat. Elle précise que cette option doit être privilégiée étant donné l'obligation légale ou contractuelle de garder le secret. N'ayant pas connaissance du fait que d'autres cantons externalisent leurs données, elle suggère de le développer en partenariat avec d'autres cantons ou avec la Confédération. A défaut de privilégier un Cloud fribourgeois, romand ou national, elle rappelle que des mesures techniques et organisationnelles strictes doivent être appliquées dans la mesure où l'Etat traite des données sensibles et soumises au secret de fonction/professionnel. Une liste de conditions strictes à respecter est alors transmise (nuage privé, hébergement en Suisse ou dans un état sûr, pas d'externalisation des données soumise au secret de fonction/professionnel, chiffrement, établissement d'un contrat personnalisé et approuvé). L'Etat poursuit le travail sur l'axe législatif afin de permettre l'utilisation du Cloud à l'Etat de Fribourg.

Suite à divers échanges avec l'Autorité (Commission et Préposée) et les services concernés, un préavis de l'Autorité a été sollicité afin de proposer au Conseil d'Etat d'autoriser une phase exploratoire sur diverses solutions informatiques en Cloud, comme le prévoit l'article 21 de la Loi sur le guichet de cyberadministration (LGCyb). La Commission a exigé une analyse des risques et émis par la suite, sur la base de cette dernière, un préavis favorable assorti de conditions à différents projets pilotes.
Elle exige que l'hébergement soit effectué en Europe, l'applicabilité du droit suisse et du for en Suisse, le cryptage des données et la détention de la clé par l'Etat (SITel), la conclusion d'une clause de confidentialité, l'information à la Commission en cas de fuite/panne de données et la communication du résultat de l'évaluation. Enfin, si l'article 21 LGCyb ne précise pas la forme de l'autorisation du Conseil d'Etat, l'Autorité est d'avis qu'un essai pilote est un traitement de données comme un autre et nécessite dès lors une base légale au moins pour traiter les données sensibles.
Actuellement, l'Ordonnance est en vigueur et les projets précités sont en cours de traitement. L'Autorité est dans l'attente des résultats de l'évaluation.

*Référentiels EDU*
Dans l'année sous rubrique, l'Autorité a été à nouveau en contact avec le Centre de compétences Fritic dans le cadre des référentiels de l'éducation. Il s'agit de deux plateformes hébergeant les données de références concernant les élèves, enseignants et employés des écoles du canton de Fribourg, les établissements scolaires, le cursus scolaire des élèves ainsi que les données de références transversales à tous les degrés, telles que les statistiques. Par références, on entend des données contrôlées et validées par d'autres sources de données afin d'éviter toute erreur lors de la collecte des données et d'éliminer ou de fusionner les personnes à double. Les règles d'accès aux données des référentiels et les fonctions de recherches et d'ajouts des personnes ont été discutées. Le projet est en cours d'élaboration, notamment par la mise en production de certaines applications informatiques et la mise à jour des bases légales correspondantes.

*Processus de gestion de la photo d'identité lors d'une demande d'extrait des offices des poursuites depuis le guichet virtuel de cyberadministration*
L'Autorité a été sollicitée pour une analyse du processus de gestion de la photo d'identité lors d'une demande d'extraits des offices des poursuites depuis le guichet virtuel de cyberadministration. Pour s'identifier sur le guichet virtuel de cyberadministration, le citoyen pourra utiliser soit le numéro AVS soit fournir la photo d'une pièce d'identité lors de la commande de son extrait de l'office des poursuites. Les documents sont créés depuis l'application THEMIS et envoyés sous forme électronique au guichet virtuel. L'Autorité a pris note que la copie de la carte d'identité est uniquement stockée dans l'application THEMIS et, en aucun cas, dans le guichet de cyberadministration. L'Autorité a précisé que la carte d'identité pourrait être utilisée, et uniquement, à des fins d'identification dans le cas où l'accès à cette prestation se fait par le biais du site Internet de l'Office des poursuites et l'application THEMIS, mais ne peut être utilisée à d'autres fins.

**Divers**
*Registre cantonal des poursuites*
L'Autorité a été consultée au sujet de la mise en place d'un registre cantonal des poursuites. En effet, actuellement les extraits du registre des poursuites auraient une pertinence limitée en raison du fait que, suite à un déménagement, le citoyen qui fait l'objet de poursuite dans un district peut obtenir une attestation de non poursuite au lieu de son nouveau domicile, ce qui engendrait une sorte de «tourisme des débiteurs».

L'Autorité est d'avis que la création d'un registre cantonal des poursuites pose plusieurs problèmes. Premièrement, le droit des poursuites (y compris le droit de consultation des registres) est réglé au niveau fédéral, ce qui veut dire que pour harmoniser l'échange entre les offices des poursuites cantonaux il faudrait que la loi fédérale soit révisée. Deuxièmement, en vertu du principe d'exactitude des données et pour assurer une identification sûre du débiteur, chaque office devrait employer exactement le même système de collecte et d'organisation des données afin de pouvoir assurer une équivalence de contenu, ce qui n'est pas le cas actuellement. Enfin, la création d'un registre des poursuites cantonal engendrerait une charge de travail supplémentaire pour les offices de poursuites.

*Certificat de mœurs*
Suite à une question posée par un parlementaire, la Commission a pris position concernant l'utilisation du certificat de mœurs dans le canton et son traitement sous l'angle de la protection des données. Au terme de son analyse, la Commission a constaté, d'une part, qu'il n'existait pas de définition légale du certificat de mœurs et, d'autre part, que la pratique des communes à ce sujet et son contenu divergeaient grandement. En effet, certaines communes se limitaient à délivrer une

attestation de domicile alors que d'autres délivraient un certificat attestant que le citoyen jouissait d'une bonne réputation. Au niveau de la protection des données, ces pratiques étaient donc plus ou moins intrusives, ce qui conduisait à une inégalité de traitement des citoyens au niveau cantonal. La Commission a proposé de supprimer le certificat de mœurs de la législation fribourgeoise.

*Plateforme centrale suisse des données laitières*
Une exploitation agricole du canton de Fribourg a consulté l'Autorité au sujet du traitement de données effectué par une société privée qui enregistre et gère les données laitières pour le compte des pouvoirs publics et du secteur laitier, par le biais de son application web. En effet, cette société met à disposition des données détaillées pour la production laitière et les résultats du contrôle du lait en Suisse. Chaque producteur de lait a accès aux données de son exploitation. Or, il ressort de la requête que les résultats des analyses de lait sont accessibles par des fromageries non-concernées par le lait vendu ayant fait l'objet du contrôle. Dans la mesure où des organes fédéraux (dans le cas d'espèce l'OSAV) et une société privée sont responsables de ladite plateforme, l'Autorité a considéré que cette dernière est de la compétence du Préposé fédéral à la protection des données. Ainsi, la demande lui a été transmise en accord avec les exploitants. Suite à l'échange avec le Préposé fédéral et le rappel des particuliers, l'Autorité a incité les exploitants à s'adresser à l'Autorité de surveillance, qui est l'OSAV, et à la société concernée afin de faire valoir leurs droits, en particulier afin d'empêcher la communication de leurs données à des tiers. Le cas échéant, ils ont la possibilité d'agir au travers de démarches de droit civil pour limiter les atteintes à leur personnalité.

**Travaux divers**
*Feuilles informatives*
L'Autorité a travaillé à l'élaboration de feuilles informatives et de guides de bonnes pratiques. D'une part, elle a actualisé le guide pratique à l'attention des communes et, d'autre part, elle a entrepris de finaliser les travaux relatifs à un guide d'informations aux communes contenant les règles de bonne conduite en matière de sécurité de l'information, guide élaboré sur la base des contrôles effectués dans différentes communes.
De plus, il est à mentionner que privatim a réalisé un guide consacré aux exigences juridiques et techniques des portails web de l'administration publique. Ce guide soutient les organes publics dans la planification et l'exploitation de tels portails web, offre des repères quant à leur développement et sert à leur évaluation par les Préposés à la protection des données.

*Règlements communaux*
Durant l'année sous rubrique, la Préposée à la protection des données a été consultée, à sept reprises, par la DSJ au sujet des projets de règlements communaux de police. Dans ses préavis, elle relève que, dans le renvoi aux lois, la mention des bases légales concernant la protection des données et la vidéosurveillance fait défaut. Elle se prononce également sur les dispositions concernant les drones et la vidéosurveillance, en y ajoutant des précisions.

### 1.2 Contrôles
La Préposée a procédé, d'entente avec la Commission, à un contrôle de grande envergure en matière de protection des données auprès d'une préfecture et a pu achever le contrôle d'une institution en rendant son rapport final. 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 concernés.

Le contrôle de 2017 s'est conclu par la rédaction du rapport. 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 a notamment souligné 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, et 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. Les mots de passe manquent de complexité. 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 courriels en toute sécurité avec des personnes de l'extérieur ne disposant pas d'une adresse électronique 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).
Le contrôle de 2018 a incité l'Autorité à signaler la nécessité de protéger les dossiers contenant des données personnelles, surtout des données personnelles sensibles, et de les fermer à clé dans des armoires en cas de conservation sous une forme physique.

Par ailleurs, l'Autorité a effectué les travaux préparatoires en vue du contrôle d'une commune en 2019. Il n'a pas été possible d'achever les contrôles subséquents des années antérieures, faute de ressources. D'autres contrôles de ce type sont prévus.

Pendant l'année sous revue, aucun contrôle SIS coordonné n'a eu lieu avec les autres cantons ni avec le Préposé fédéral à la protection des données et à la transparence. En revanche, un contrôle commun des fichiers journaux a été réalisé pour la première fois avec le Service de la population et des migrants, en charge de la plateforme Fri-Pers. Le nombre de requêtes des dix principaux utilisateurs a fait l'objet d'un contrôle par sondage pendant deux semaines et les droits d'accès ont été soumis à un contrôle général. Ce fut l'occasion pour la Préposée de sensibiliser et d'attirer l'attention sur le fait que Fri-Pers ne peut pas être consulté pour satisfaire la curiosité. Du reste, ces contrôles ont révélé que l'utilisation de la plateforme est conforme à la protection des données. Il s'est avéré par ailleurs que Fri-Pers ne dispose pas d'une plateforme d'apprentissage dédiée.

### 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.

*Accès par un service social*

Dans le cadre de l'accomplissement de ses tâches, notamment en matière sociale, un service social du canton de Fribourg a obtenu un accès aux données de la plateforme informatique cantonale Fri-Pers, limité aux données des habitants des communes concernées. Cet accès est d'autant plus nécessaire dans la mesure où il permet au service d'avoir des données à jour et exactes. En outre, cela

évite que les collaborateurs du service contactent d'autres organes ou communes pour demander des renseignements, au risque de violer leur secret de fonction. La nécessité de l'accès à l'historique des données n'a pas été reconnue.

*Autorisation spéciale de transmission de données Fri-Pers*
Dans le cadre de l'élaboration du Rapport quadriennal sur l'agriculture, plusieurs services et directions de l'Etat mènent une étude afin d'analyser les risques psycho-sociaux des agriculteurs du canton de Fribourg. A cette fin, une demande d'extraction de certaines données Fri-Pers concernant les exploitants du canton a été soumise à l'Autorité. Il ressort du préavis que le Règlement d'utilisation doit clairement mentionner le but défini, la liste des données transmises, l'indication que le numéro AVS est utilisé uniquement pour l'interconnexion des données et qu'il ne sera pas transmis au SAgri, la durée de conservation - respectivement la destruction - des données par le SAgri, la confidentialité et l'approbation des Directeurs concernés. Une fois le Règlement d'utilisation signé par les parties, le SPoMi peut transmettre les données des personnes qui ressortent de la liste des numéros AVS du SAgri.

*Accès indirect par Serafe SA*
Depuis 2019, le nouvel organe de perception de la redevance de radio-télévision, désigné par l'Office fédéral de la communication sur mandat du Département fédéral de l'environnement, des transports, de l'énergie et de la communication, est Serafe SA. Conformément à la Loi sur la radio et la télévision, c'est auprès des registres des habitants et du système d'information Ordipro du Département fédéral des affaires étrangères que Serafe SA acquiert les données sur les ménages et leurs membres nécessaires à la perception de la redevance. Il ressort de la législation que Serafe SA peut utiliser systématiquement le numéro AVS pour remplir ses tâches en relation avec la perception de la redevance, en cas de demande de précision aux communes et aux cantons concernant les données fournies. En outre, il est relevé que l'organe de perception a accès à des données sensibles sur la santé d'une personne notamment ou sur les mesures d'aide sociale accordées à celle-ci afin d'établir l'exonération de la redevance. La transmission des données est faite par le biais de la plateforme informatique et de communication de la Confédération sous forme cryptée. La Préposée à la protection des données a préavisé favorablement la demande.

*Nouvel accès suite à une réorganisation du service*
Suite à l'adoption de la nouvelle Loi sur l'exécution des peines et des mesures, entrée en vigueur le 1er janvier 2018, une réorganisation pénitentiaire cantonale a eu lieu. Le Service de l'application des sanctions pénales et des prisons (ci-après: SASPP) a fusionné avec le Service de probation (ci-après: SProb) constituant ainsi le nouveau SESPP. Dans ce cadre, le SESPP souhaite continuer à bénéficier de l'accès aux données Fri-Pers, tel que cela a été octroyé au SASPP. Compte tenu de ses tâches particulièrement sensibles, il est indispensable au SESPP de pouvoir s'assurer de l'identité des personnes concernées et d'obtenir des données à jour et exactes. En l'espèce, la Préposée à la protection des données a préavisé de manière favorable l'accès aux données de la plateforme informatique Fri-Pers.

*Contrôles*
Le SPoMi, en tant que responsable des données Fri-Pers procède, à intervalles réguliers, au contrôle des autorisations délivrées, en collaboration avec l'Autorité. Afin d'éviter les doubles contrôles et d'unir leurs forces, le SPoMi et l'Autorité ont établi un procédé commun pour effectuer des contrôles. Durant l'année sous rubrique, les deux entités ont effectué le contrôle d'un service de l'Etat qui traite de grandes quantités de données sensibles. Le contrôle a notamment porté sur des questions d'ordre général et sur les logfiles concernant certains collaborateurs du service. Il résulte de ce contrôle que le service utilise la plateforme Fri-Pers de manière conforme aux règles régissant la protection des données. La direction est consciente du caractère sensible des données et rend régulièrement son personnel attentif au secret de fonction. Le SPoMi et l'Autorité suggèrent au service contrôlé de mettre en place des profils fictifs lors de la formation du personnel à l'utilisation de la plateforme Fri-Pers.

**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)). La collaboration avec les préfets est bonne. Ceux-ci suivent généralement les prises de position de l'Autorité.

Des différentes demandes d'installation de vidéosurveillance, il ressort de plus en plus que les particuliers, les entreprises et les organes cantonaux et communaux recourent à un mandataire privé chargé de gérer la maintenance de l'installation et parfois d'héberger et stocker les enregistrements. Cela peut, par exemple, être des entreprises de sécurité privée, mais également des prestataires d'hébergement Cloud et des Data center. Dans ce contexte, il s'agit alors d'analyser si nous sommes en présence d'une externalisation du traitement des données. Le cas échéant, des conditions plus strictes doivent être prises concernant la sécurité et la protection des données. L'Autorité conseille vivement aux personnes concernées de s'informer avant la commande du système de vidéosurveillance et la conclusion du mandat avec le prestataire privé. En effet, il est déjà arrivé que des personnes se retrouvent avec une installation prête à l'emploi, mais sans autorisation valable d'installation de vidéosurveillance.

*Dénonciations*
Durant l'année sous rubrique, l'Autorité a été informée de plusieurs dénonciations concernant des installations de vidéosurveillance filmant le domaine public, sans autorisation. Il peut notamment s'agir de caméra installée à l'intérieur de magasins ou de restaurants privés et dont le champ de vision peut être dirigé vers le domaine public, notamment à travers des fenêtres ou des portes vitrées. 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.

*Vidéosurveillance dans une déchetterie communale*
Dans le cadre d'une demande de vidéosurveillance d'une déchetterie communale, l'Autorité a émis un préavis défavorable dans la mesure où le système d'installation de vidéosurveillance ne passe pas l'examen de la proportionnalité. En effet, la déchetterie étant située au centre du village, à côté d'habitations privées, elle n'est pas isolée. Ainsi, le risque que la caméra capture des images de simples passants et d'habitants du village est grand, en particulier puisque son champ de vision est dirigé

vers la route communale et les habitations privées. En conclusion, l'Autorité est d'avis qu'il n'est pas admissible de donner un poids plus important à l'intérêt public pour la prévention et la répression des atteintes aux biens matériels qu'à  l'atteinte aux libertés des usagers. D'autant plus qu'il ne ressort pas du dossier que l'infrastructure communale ait subi des déprédations.

*Caméras installées dans les centres d'hébergement des requérants d'asile*
Dans le cadre de son mandat pour le canton, une entreprise privée est en charge de l'hébergement et l'encadrement des requérants d'asile. Afin de prévenir les risques de violence entre les habitants du foyer, les atteintes au personnel encadrant ainsi que les dégâts aux biens, elle souhaite installer des caméras de vidéosurveillance dans les foyers destinés à leur accueil. L'Autorité a déjà préavisé plusieurs demandes de cette entreprise. A chaque fois, une analyse du cas d'espèce est faite, en particulier chaque prise de vue. L'Autorité est d'avis que les enregistrements doivent être stockés et hébergés au sein de l'entreprise en Suisse et qu'aucun accès à distance aux images ne doit être octroyé. En cas d'externalisation, des conditions plus strictes doivent être appliquées, telles que le chiffrement lors du transfert et du stockage et le fait que la clé doit être aux mains de l'entreprise mandatée. Les instructions nécessaires à la sécurité et protection des données doivent ressortir clairement du contrat de sous-traitance.

*Vidéosurveillance du bâtiment hébergeant les vestiaires d'un club de foot*
Un organe public rattaché à la DICS a déposé une demande d'installation de caméras. Il souhaite filmer l'intérieur du bâtiment des vestiaires afin d'empêcher des actes de vandalisme ainsi que des vols. S'agissant d'immeubles ouverts au public qui sont affectés à l'administration publique, la LVid est applicable. Dans le cas d'espèce, il faut tenir compte de la présence de mineurs et de l'intimité des personnes concernées. La Préposée à la protection des données émet un préavis favorable, pour autant que l'utilisation des caméras soit limitée de 16h à 22h la semaine et le week-end et que leur champ de vision soit limité au couloir menant aux vestiaires. En effet, il ne doit pas être dirigé vers la cage d'escaliers, le hall et l'entrée des toilettes, et en aucun cas filmer l'intérieur des vestiaires. Le système est limité à une année et doit être réévalué afin d'être conforme aux besoins. Enfin, au vu de la présence de mineurs dans le bâtiment, l'Autorité relève que cela implique d'informer personnellement les représentants légaux et les mineurs concernés.

*Surveillance vidéo d'une école communale*
Faisant suite à diverses incivilités et actes de vandalisme depuis de nombreuses années, une commune souhaite installer un système de vidéosurveillance sur le site regroupant ses différentes écoles. En effet, l'administration communale a constaté que, durant les heures creuses de l'activité scolaire, en soirée, la nuit et le week-end, les bâtiments et infrastructures extérieurs de ce complexe scolaire sont régulièrement victimes d'actes de vandalisme et que, malgré les plaintes transmises au Ministère public et les contrôles préventifs effectués par la Police et la société en charge de la surveillance des bâtiments communaux, aucun auteur n'a pu être appréhendé pour ces faits. Il ressort de la requête que l'installation fonctionnera aux heures dites «hors cadre scolaire», du lundi au vendredi, de 22h30 à 7h00 et les week-ends et jours fériés. Les champs de vision des caméras couvriront l'ensemble des cours extérieures des bâtiments scolaires. Dans ce cadre, la Préposée à la protection des données a préavisé favorablement la demande pour autant que le propriétaire privé voisin ait donné son consentement pour la partie filmée de sa propriété, que le système soit réévalué dans cinq ans et que les collaborateurs de l'entreprise de sécurité aient signé une clause de confidentialité.

*Installation d'un système de vidéosurveillance suite à des déprédations contre un bâtiment de l'Etat*
Un bâtiment de l'Etat a subi des dommages à la propriété par des activistes. A cette fin, le service souhaite installer des caméras de vidéosurveillance aux entrées de l'immeuble. Afin de limiter l'atteinte aux droits de la personnalité des collaborateurs des services hébergés, l'Autorité est d'avis que l'utilisation des caméras doit être limitée de 18h00 à 7h00 la semaine et 24h sur 24h le week-end ainsi que les jours fériés. Il est rappelé que les enregistrements ne peuvent être consultés qu'en cas d'atteinte avérée et par les personnes autorisées définies dans le Règlement d'utilisation. Enfin, l'Autorité précise que les collaborateurs et collaboratrices doivent être informés des endroits sous vidéosurveillance et des horaires où le système fonctionne. Ainsi, la Préposée à la protection des données a préavisé favorablement la demande.

### 1.4. ReFi – registre des fichiers[12]

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[13].

Après la mise à jour de l'application informatique intervenue les années précédentes, il s'agissait essentiellement 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 a entrepris d'établir quelles sont les collectes de données existant dans une commune et de mettre au point des annonces-types. Les travaux sont en cours. En effet, une grande commune du canton de Fribourg s'est proposée d'établir des exemples de chaque déclaration de fichier pour faciliter la saisie des autres communes.

### 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).

[12] https://www.fr.ch/atprd/institutions-et-droits-politiques/transparence-et-protection-des-donnees/registre-des-fichiers-refi
[13] http://appl.fr.ch/refi/etat/client/index.aspx

## 2. Statistiques

**Protection des données en général**

Durant la période considérée, 375 dossiers en matière de protection des données (sans les demandes Fri-Pers et vidéosurveillance, voir ci-dessous) ont été introduits, dont 68 sont pendants au 1er janvier 2019. Ces dossiers comprennent 115 conseils et renseignements, 88 avis, 28 examens de dispositions législatives, 26 communications de décisions (art. 27 al. 2 LPrD), 8 contrôles et inspection ou suivis de contrôle, 7 présentations, 42 participations à des séances et autres manifestations et 61 demandes diverses. 175 dossiers concernent des organes cantonaux ou des institutions chargées de tâches publiques, 82 des communes et paroisses, 70 d'autres organismes publics (cantons, autorités de protection des données), 47 des particuliers ou des institutions privées et 1 des médias (cf. statistiques annexées). Pour les dossiers pendants des années précédentes, 78 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 2018, 8 demandes ont été soumises à la Préposée à la protection des données pour préavis: 5 demandes d'accès, 2 demandes d'extension de l'accès et 1 demande d'autorisation spéciale. De ces requêtes, 4 demandes sont toujours en traitement et 4 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 2018, la Préposée à la protection des données a reçu 8 demandes d'installation de vidéosurveillance avec enregistrement pour préavis, 6 annonces d'installation de vidéosurveillance sans enregistrement et a dû se déterminer à 6 reprises dans des cas de dénonciations d'installations sans autorisation. De ces requêtes, 13 préavis positifs ont été émis, 1 préavis défavorable, alors que les 6 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, 9 demandes émanaient des services de l'Etat ou de communes et 11 de privés. Conformément à ce que prévoit l'article 9 OVid, la liste des installations de vidéosurveillance est disponible sur les sites Internet des préfectures.

# IV. Coordination entre la transparence et la protection des données

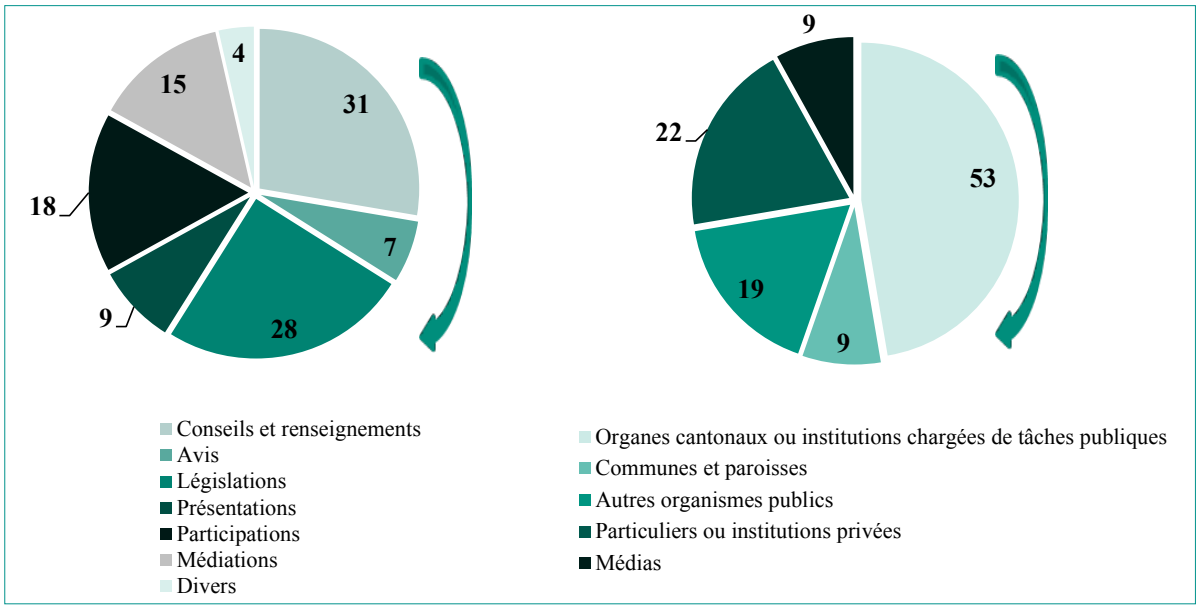
La bonne collaboration entre les deux Préposées s'est poursuivie en 2018. Plusieurs mesures avaient été prises dès le début pour la préservation de cette coopération. Les séances de la Commission, auxquelles les deux Préposées participent, traitent régulièrement les dossiers portant sur les deux domaines. 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.

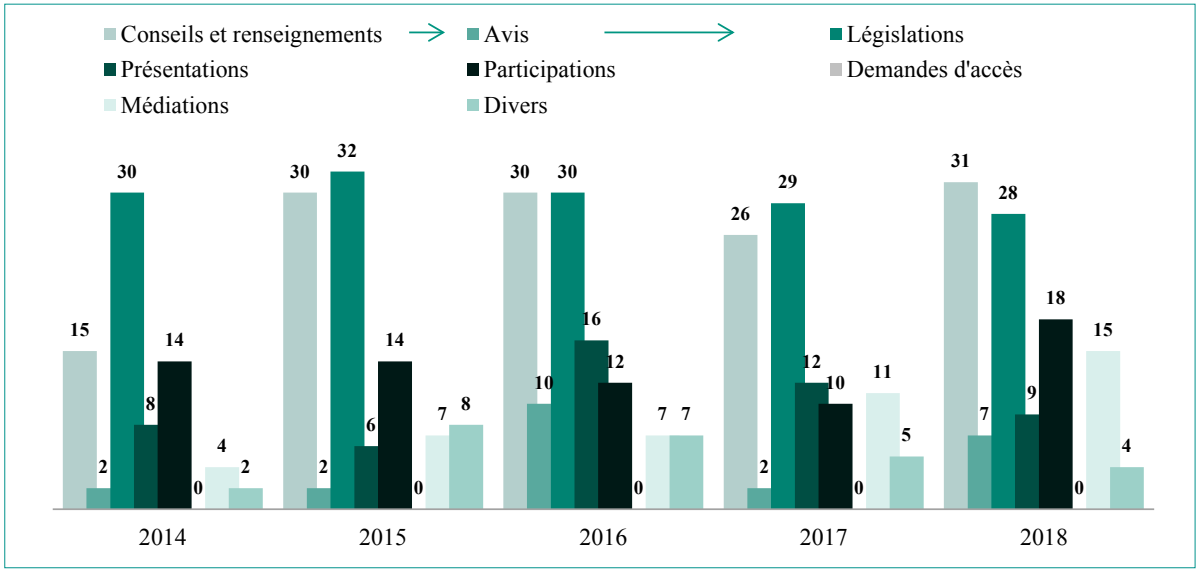
# Statistiques de la transparence

## Demandes / interventions en 2018

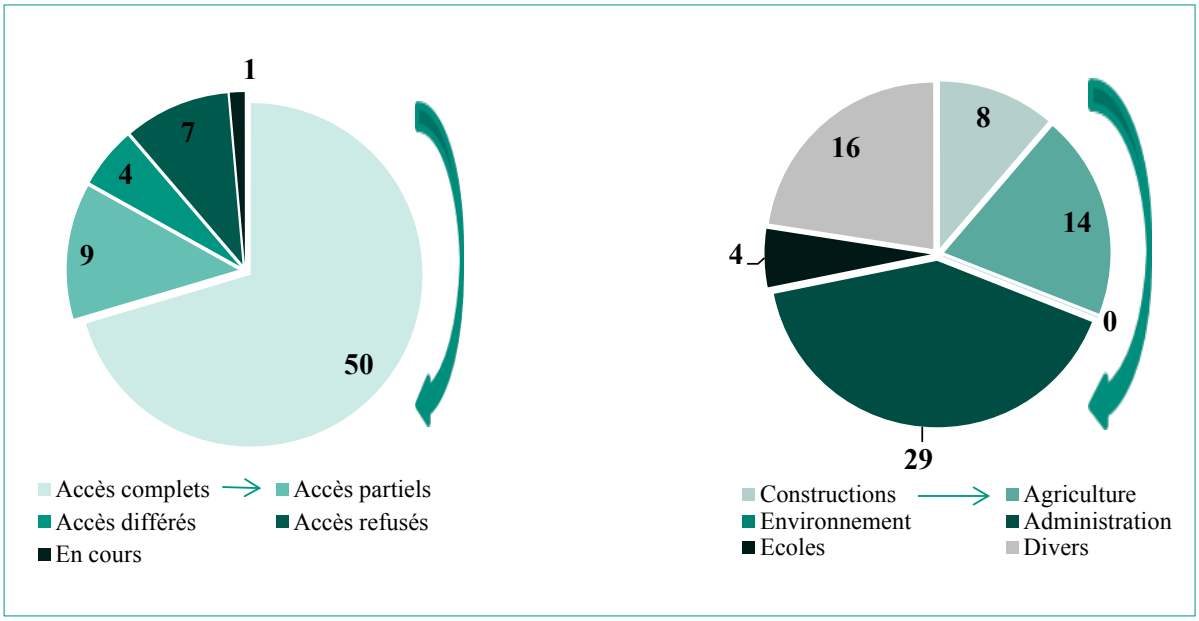



- Les «conseils et renseignements» sont donnés par la Préposée à la transparence.
- Le terme «législations» comprend les travaux de réflexion sur des dispositions législatives et les réponses aux consultations.
- La notion de «présentations» recouvre par ex. les exposés dans le cadre de la présentation du droit d'accès, les formations continues organisées par l'Etat de Fribourg et celles pour les apprenti-es et les stagiaires 3+1.
- La notion de «participations» recouvre par ex. les séances (groupes de travail), les conférences et les colloques.
- Parmi les 112 dossiers ouverts en 2018, 44 dossiers sont communs avec ceux de la protection des données, dont 28 consultations.

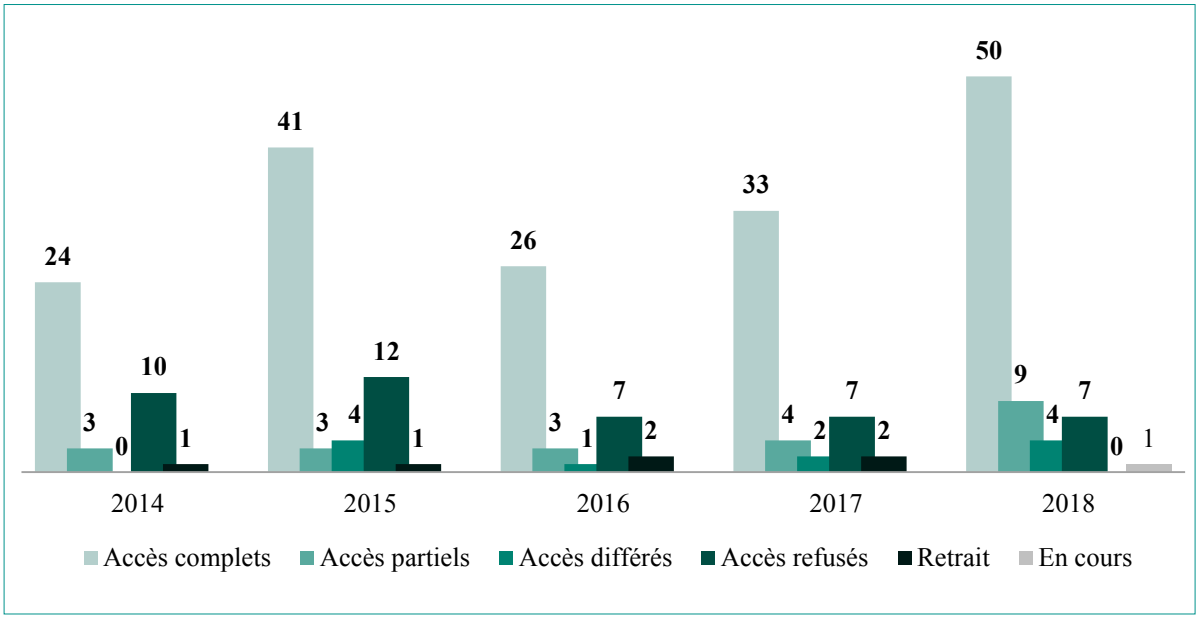
## Comparatif



## Evaluation du droit d'accès en 2018

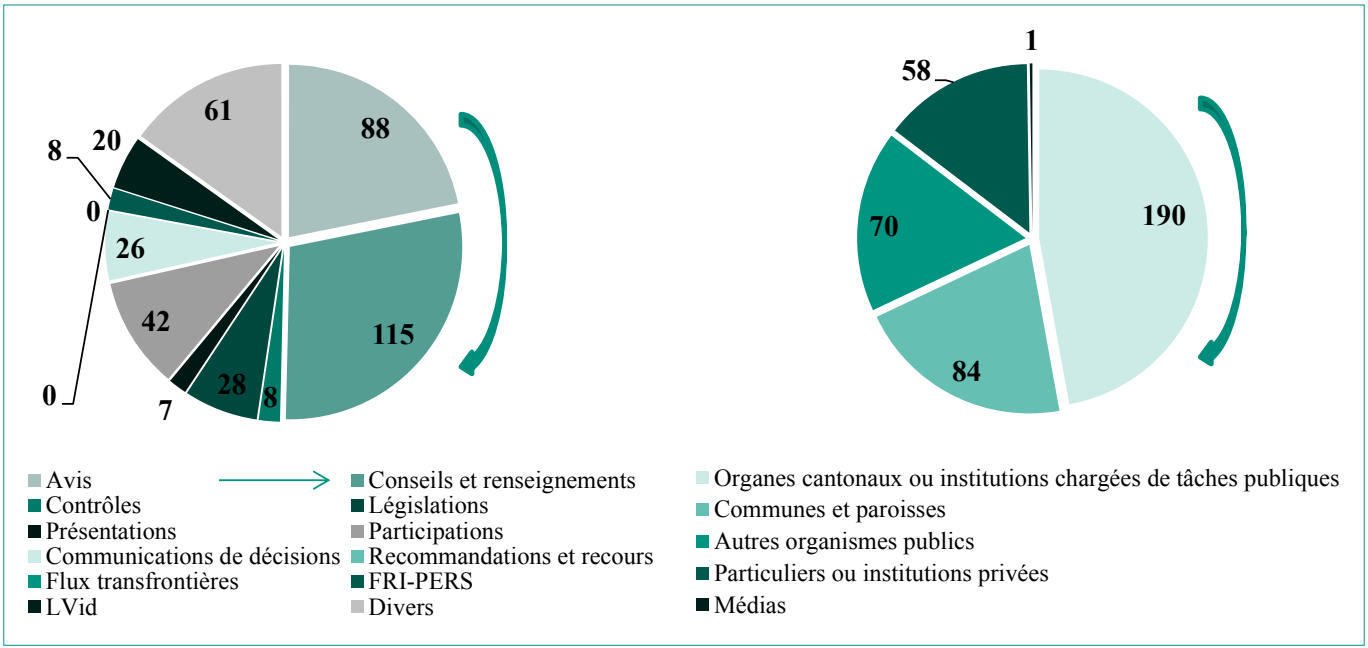



## Comparatif



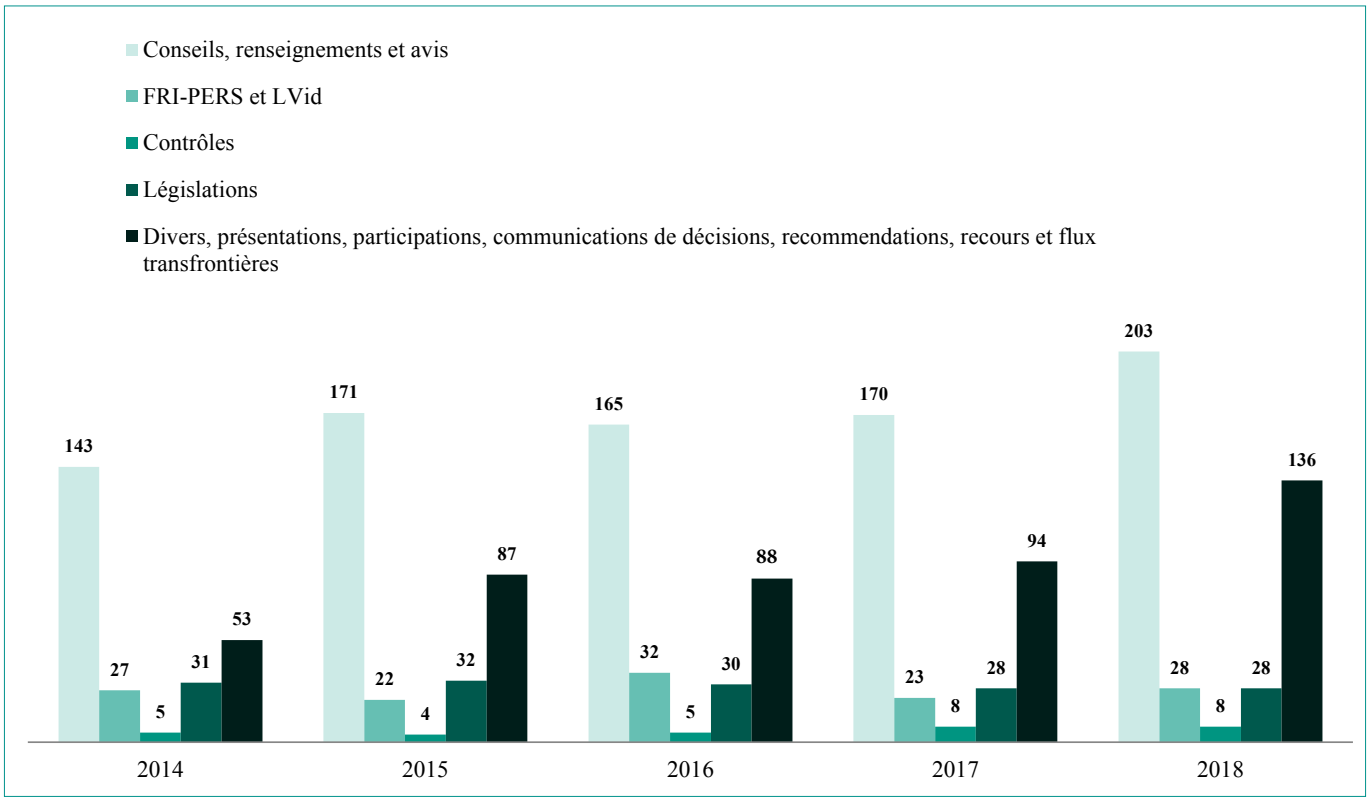
# Statistiques de la protection des données, FRI-PERS et LViD

## Demandes / interventions en 2018




- 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 403 dossiers ouverts en 2018, 44 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2018 | 88 | 115 | 8 | 28 | 7 | 42 | 26 | 0 | 0 | 8 | 20 | 61 | 403 |
| 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 |