

Rapport d'activité 2020

—
pour la période du 1^{er} janvier
au 31 décembre 2020



ETAT DE FRIBOURG
STAAT FREIBURG

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

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

Avril 2021

—
Imprimé sur papier 100% recyclé

AU GRAND CONSEIL
DU CANTON DE FRIBOURG

Madame la Présidente,
Mesdames et Messieurs les Député-e-s,

Nous avons l'honneur de vous adresser le rapport 2020 de l'Autorité cantonale de la transparence et de la protection des données. Après une mise en lumière des points forts de l'année et 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 poursuivrons avec quelques remarques au sujet de la coordination des deux champs d'activité (IV) pour aboutir à des considérations finales (V).

Nous avons décidé de nous concentrer, dans le rapport, sur les thématiques les plus importantes. Un résumé qui figure aux premières pages du rapport vous permet de vous faire rapidement une image générale des points forts dans le domaine de nos activités.

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

Fribourg, avril 2021

Le Président
de la Commission

L. Schneuwly

La Préposée
à la transparence

M. Stoffel

La Préposée
à la protection des données

F. Henguely

Table des matières

Points forts	6
<hr/>	
I. Tâches et organisation de l'Autorité	7
<hr/>	
A. Focus	7
1. Tâches de la Préposée à la transparence	8
2. Tâches de la Préposée à la protection des données	8
B. Collaboration supracantonale et cantonale	9
C. Engagement dans la formation	9
D. Information et communication	9
<hr/>	
II. Activités principales de la Commission	10
<hr/>	
A. Sujets communs à la transparence et la protection des données	10
1. Prises de position	10
1.1 Focus	10
1.2 Quelques exemples de prises de position	10
2. Dossiers spécifiques	13
B. Domaine de la transparence	16
1. Evaluation du droit d'accès	16
C. Domaine de la protection des données	16
1. Recommandation et recours en cas de non-respect des prescriptions (art. 22a et 30a al. 1 let. c LPrD)	16
2. Recours (art. 27 et 30a al. 1 let. d LPrD)	16
<hr/>	
III. Activités principales des Préposées	17
<hr/>	
A. Transparence	17
1. Points forts	17
1.1 Médiations dans le domaine du droit d'accès	17
1.2 Médiation dans le cadre de la Loi sur la médiation administrative	19
1.3 Demandes	19
2. Statistiques	20
B. Protection des données	21
1. Points forts	21
1.1 Coronavirus	21
1.2 CoPil, CoPro et groupes de travail	22
1.3 Dossiers complexes	24
1.4 Demandes	25
1.5 Violations de la sécurité des données	26
2. Contrôles	26
3. FriPers et vidéosurveillance	27
3.1 FriPers	27
3.2 Vidéosurveillance	28
4. ReFi - registre des fichiers	30

5. Echanges	30
5.1 Collaborations	30
5.2 Formations et sensibilisations	31
5.3 Travaux divers	32
6. Statistiques	32
<hr/>	
IV. Coordination entre la transparence et la protection des données	33
<hr/>	
V. Remarques finales	33
<hr/>	
Table des abréviations et termes utilisés	34
Annexe: statistiques	35
Statistiques de la transparence	35
Statistiques de la protection des données, Fri-Pers et LVid	37

Points forts

En 2020 en transparence, le nombre de demandes en médiation ainsi que de demandes de renseignement s'est stabilisé à un niveau comparable à 2019. 20 demandes en médiation ont été soumises à la préposée à la transparence, et toutes concernaient des documents différents. Dans 10 cas, un accord a été trouvé. La préposée a rendu 9 recommandations (dont 2 demandes en médiation qui dataient de 2019 et pour 1 médiation, les parties ont accepté que 2 recommandations soient rendues). Dans 1 cas et après échange avec les parties, la préposée à la transparence n'a pas pu entrer en matière. 2 requêtes en médiation ont été retirées par la personne requérante. 2 requêtes en médiation étaient encore pendantes à la fin de l'année.

Les chiffres portés à la connaissance de la préposée indiquent que 67 demandes d'accès ont été déposées auprès des organes publics fribourgeois en 2020. Dans 59 cas, lesdits organes ont accordé un accès total, restreint ou différé. A l'instar de l'administration fédérale, l'ATPrD part du principe que le nombre de demandes d'accès est en fait bien plus important, mais que celles-ci ne sont pas toujours identifiées comme telles, de sorte qu'elles ne sont pas systématiquement traitées sous l'angle de la loi sur l'information et l'accès aux documents (LInf) ni annoncées dans le cadre de l'évaluation. Une sensibilisation constante des organes publics semble dès lors très importante.

Le Tribunal fédéral et le Tribunal cantonal ont rendu différents arrêts dans le domaine de la transparence. Dans son arrêt, le Tribunal fédéral a maintenu l'arrêt du Tribunal cantonal: la préposée à la transparence avait considéré comme retirée la demande en médiation d'un requérant qui refusait de participer à la séance de médiation. Le Tribunal cantonal avait rejeté le recours du requérant contre cette décision. Dans un arrêt, le Tribunal cantonal a décidé que l'accès partiel au rapport d'une enquête administrative dans une commune doit être accordé, moyennant consultation des tiers. Dans un autre cas, le Tribunal cantonal a déclaré irrecevable

deux procédures qui visaient à contester un accord suite à une médiation concernant l'accès à des documents; il a renvoyé le dossier à la préposée.

La digitalisation de l'administration cantonale a poursuivi son développement et n'a cessé d'amener de nouveaux projets complexes mais a également nécessité une coordination à l'interne de l'administration concernant les responsabilités du traitement des données ainsi qu'une sensibilisation. En parallèle, la pandémie a donné un coup d'accélérateur à la digitalisation, entraînant une utilisation étendue des solutions informatiques et des outils de communication et modifiant le mode de travail de l'administration. Elle a également amené des changements importants et des restrictions drastiques de la sphère privée et de l'autodétermination, puisque des collectes systématiques de données personnelles effectuées par l'Etat, mais aussi par des acteurs privés, sont susceptibles de modifier à long terme la question de l'autodétermination. Durant cette période, la préposée à la protection des données a travaillé de manière pragmatique et étroite avec les autres autorités de protection des données de la Confédération et des cantons.

Les révisions législatives ont également nécessité une attention particulière, dans la mesure où la digitalisation de l'administration entraîne naturellement une adaptation des bases légales. De nombreux échanges ont eu lieu dans le cadre de l'adaptation de la législation cantonale à certains aspects de la digitalisation. Enfin, l'adoption de la nouvelle loi fédérale sur la protection des données va permettre de poursuivre la révision du droit cantonal de la protection des données.

Le domaine de la protection des données a, à nouveau, fait face à une forte augmentation de la charge de travail (+15%). Toutefois, ce n'est pas uniquement le nombre de dossiers qui a augmenté, mais plus encore leur complexité qui nécessite des connaissances spécifiques et touche à différents acteurs (privé et public, intercantonaux, etc.).

I. Tâches et organisation de l'Autorité

A. Focus

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 (80%). Le taux de travail de la préposée à la protection des données a été augmenté de 50% à 80% en avril 2020. 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. Dès la deuxième partie de l'année 2020, elle a en plus bénéficié d'un soutien administratif (100%) pour une durée de 12 mois, ainsi que d'un deuxième stagiaire juriste (100%) pour une durée de 12 mois également. Les moyens tiers de l'ATPrD ont passé de Fr. 70'000.- à Fr. 150'000 pour l'année 2020.

Les tâches de la **Commission cantonale de la transparence et de la protection des données** sont définies dans l'article 40b de la loi fribourgeoise du 9 septembre 2009 sur l'information et l'accès aux documents (LInf)¹ et dans les articles 12f et 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'article 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 12f LPrD;

En 2020, la Commission était présidée par *M. Laurent Schneuwly*, juge cantonal. Les autres membres de la Commission étaient: *M. Philippe Gehring* (Vice-président), ingénieur en informatique EPFL, *Mme Anne-Sophie Brady*, ancienne 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 9 séances en 2020. 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 168 heures sur l'ensemble de l'année. Enfin, tant le Président que le Vice-président ou des membres de la Commission ont pris part sporadiquement à des entretiens.

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

1. Tâches de la Préposée à la transparence

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).

2. Tâches de la Préposée à la protection des données

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

- contrôler l'application de la législation relative à la protection des données, notamment en procédant systématiquement à des vérifications auprès des organes concernés;
- conseiller les organes concernés, notamment lors de l'étude de projets de traitement;
- renseigner les personnes concernées sur leurs droits;
- collaborer avec le préposé fédéral à la protection des données et à la transparence (PF PDT) ainsi qu'avec les autorités de surveillance de la protection des données des autres cantons et avec celles de l'étranger;
- examiner l'adéquation du niveau de protection assuré à l'étranger, au sens de l'article 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 exemple:

- les tâches de préavis Fri-Pers en matière d'accès à la plateforme informatique contenant les données des registres des habitants et de contrôle des autorisations en collaboration avec le Service de la population et des migrants (ordonnance du 14 juin 2010 relative à la plateforme informatique contenant les données des registres des habitants)³;
- les tâches de préavis LVID en matière d'autorisation d'installation de systèmes de vidéosurveillance avec enregistrement (loi du 7 décembre 2010 sur la vidéosurveillance; ordonnance du 23 août 2011 y relative)⁴;
- les tâches de préavis lors de la diffusion sur un site Internet de données personnelles sensibles (ordonnance du 14 décembre 2010 relative à l'information sur les activités du Conseil d'Etat et de l'administration)⁵;
- la participation à des groupes de travail dans le cadre de la mise en œuvre du Référentiel cantonal de données de personnes, organisations et nomenclatures (ordonnance du 24 juin 2019 y relative)⁶.

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 précédents⁷), 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).

³ https://bdlf.fr.ch/app/fr/texts_of_law/114.21.12/versions/4597

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://bdlf.fr.ch/app/fr/texts_of_law/122.0.51

⁶ https://bdlf.fr.ch/app/fr/texts_of_law/184.16

⁷ <https://www.fr.ch/atprd/institutions-et-droits-politiques/transparence-et-protection-des-donnees/rapports-dactivite>

B. Collaboration supracantonale et cantonale

La préposée à la transparence et la préposée à la protection des données s'attachent à collaborer avec le préposé fédéral à la protection des données et à la transparence (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. En 2020, la réunion printanière a eu lieu en Valais, alors que celle d'automne prévue à Fribourg s'est déroulée par visioconférence (cf. infra III. B. 5.1 «collaborations et échanges»).

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 à la transparence qui réalisent des médiations, se réunit environ deux fois par an et aborde principalement les questions de la médiation et les thèmes relatifs au principe de la transparence.

Comme les autres autorités cantonales, la préposée à la protection des données fait partie de la *Conférence des commissaires suisses à la protection des données, privatim*⁸ (cf. infra III. B. 5.1 «collaborations et échanges»). Depuis 2020, l'ATPrD est membre de la Conférence internationale des commissaires à l'information (CICI).⁹ Ceci lui permet d'avoir un meilleur accès aux connaissances globales en matière de transparence et d'accès aux documents officiels.

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

C. Engagement dans la formation

La préposée à la transparence et la préposée à la protection des données ont donné un cours en français à la HEG à l'occasion des formations continues proposées par l'Etat de Fribourg.

En 2020, les cours interentreprises AFOCI des stagiaires 3+1 et des apprentis de l'Etat de Fribourg ont été uniquement dispensés en français dans le cadre de la formation administration publique «Protection des données, droit de l'information et archivage».

D. Information et communication

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 actualités¹⁰. La rubrique Actualités de l'Autorité est régulièrement mise à jour. En mai 2020, l'Autorité a tenu sa traditionnelle conférence de presse.

Dans ses **newsletters** semestrielles¹¹, 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. Le guide **à l'attention spécifique des communes** a également été actualisé cette année. Ce guide vise à leur fournir des informations et des conseils s'appliquant à des cas concrets¹².

⁸ <https://www.privatim.ch/fr/>

⁹ <https://www.informationcommissioners.org/goals-and-objectives>

¹⁰ <https://www.fr.ch/atprd/institutions-et-droits-politiques/transparence-et-protection-des-donnees/publications-0>

¹¹ <https://www.fr.ch/atprd/institutions-et-droits-politiques/transparence-et-protection-des-donnees/newsletter-0>

¹² https://www.fr.ch/sites/default/files/2020-10/2020.10.16_Guide%20pratique%20à%20l%27attention%20des%20communes%20version%202020%20F%20-%20dernière%20version%20-%20sans%20schémas%20sauf%20page%2064.pdf

II. Activités principales de la Commission

A. Sujets communs à la transparence et la protection des données

1. Prises de position

1.1 Focus

La Commission s'est prononcée sur les différents projets législatifs du **canton** et sur certains de la **Confédération**. Les projets de loi lui sont normalement communiqués, cependant elle remarque que les projets d'ordonnances ne lui parviennent pas dans tous les cas. En outre, l'Autorité a constaté que les projets législatifs ne prennent pas souvent en compte la digitalisation et ne proposent que rarement des bases légales concernant le traitement électronique des données, les systèmes d'information ainsi que les accès en ligne.

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 Internet¹³.

1.2 Quelques exemples de prises de position

Projet d'Ordonnance concernant l'organisation de la digitalisation et des systèmes d'information (abroge et remplace l'Ordonnance du 3 novembre 2015 sur la gestion de l'informatique et des télécommunications dans l'administration cantonale)

La digitalisation de l'administration engendre de nombreux traitements de données personnelles au sein de l'État. Au vu des modifications législatives en lien avec la protection des données, des mesures techniques et organisationnelles mais également du principe de sécurité des données inscrit dans la législation sur la protection des données et des tâches qui en découlent, les liens avec la protection des données doivent impérativement ressortir du projet d'Ordonnance. L'abrogation de l'Ordonnance du 3 novembre 2015 sur la gestion de l'informatique et des télécommunications dans l'administration cantonale, s'inscrivant dans l'ère numérique, ne doit pas affaiblir l'administration en particulier la gouvernance de l'Etat. Pourtant, celle-ci voit la disparition des règles relatives à la sécurité de l'information.

La Commission a dès lors rappelé la portée de la sécurité de l'information. Premièrement, cette dernière comprend la sécurité informatique; deuxièmement, elle implique l'élaboration de règles claires pour la pratique, notamment en matière de gestion des accès aux systèmes d'information, d'accès aux locaux, d'utilisation des appareils privés à des fins professionnelles, de failles de sécurité, etc.; et troisièmement, un responsable de la sécurité de l'information doit être mentionné (est-ce le Conseil d'État, la Chancellerie, chaque direction?) pour garantir une ligne de conduite claire.

S'agissant des tâches supplémentaires attribuées à l'Autorité (mise à disposition de ressources métiers afin de garantir la bonne réalisation des projets, correspondant informatique, rôle de mandant, support métier, etc.), la Commission a souligné que des ressources supplémentaires en personnel sont indispensables au sein de l'Autorité. Elle a rappelé qu'actuellement elle est en manque d'effectif pour répondre à ses tâches, de sorte que ces attributions supplémentaires ne pourront être

¹³ <https://www.fr.ch/atprd/institutions-et-droits-politiques/transparence-et-protection-des-donnees/consultations>

exécutées en l'état actuel La Commission a également relevé que l'intégration de l'Autorité dans le processus et les discussions des projets de digitalisation et d'informatique est nécessaire pour une réalisation conforme à la protection des données.

La Commission a conclu que la suppression de la Commission informatique de l'État est malheureuse puisqu'elle comptait au moins un informaticien indépendant. En pratique, les discussions avec des spécialistes informatiques externes à l'administration, proches des réalités de sociétés privées et du canton, permettent d'avoir une vision plus large de la digitalisation au sein de l'Etat et une meilleure compréhension des différents enjeux.

Collaborant régulièrement avec des informaticiens indépendants, notamment deux membres au sein de la Commission, l'Autorité apprécie les échanges et la plus-value de ces derniers.

Pré-consultation/avant-projet de Loi intégrant administrativement l'organe de médiation à l'Autorité cantonale de la transparence et de la protection des données

Le Conseil d'Etat a estimé opportun d'intégrer la médiation administrative à l'Autorité, à l'image de ce qui existe à l'heure actuelle pour les préposées à la transparence et à la protection des données. Cette configuration octroierait à la médiatrice cantonale la capacité de requérir le soutien de la Commission et d'accéder aux ressources, notamment en personnel et en locaux de l'Autorité.

Dans sa détermination, l'Autorité a expliqué qu'elle se trouve actuellement elle-même en sous-dotation au niveau du personnel. Dans la mesure où l'intégration administrative de la médiation administrative aura une influence sur le personnel, elle a relevé qu'elle souhaite que le personnel dédié à la médiation administrative lui soit attribué séparément, afin de garantir le bon fonctionnement de l'Autorité. Il importe de mentionner que

l'indépendance et le fonctionnement de la transparence et de la protection des données doivent être garantis. Le même raisonnement s'applique, par ailleurs, à la médiation administrative. Dans cette idée, une emphase est mise sur l'importance de prévoir des budgets séparés. Enfin, elle a précisé que les locaux actuels ne permettent pas en l'état l'intégration administrative de la médiation administrative dans l'Autorité. L'importance d'un bureau propre à la médiation administrative, comme cela est fait pour les préposées à la transparence et à la protection des données est nécessaire, demeurant réservée l'utilisation commune de la salle de conférence.

Avant-projet de loi modifiant l'organisation de la médiation administrative

Début septembre 2020, le Conseil d'État a autorisé la mise en consultation de l'avant-projet de Loi modifiant l'organisation de la médiation administrative. L'Autorité a répondu, d'une part, par le biais d'une détermination commune de la Commission et des préposées au sujet des nouveaux articles 31 al. 4 LPrD et 41 al. 4 LInf, et d'autre part, la Commission a précisé les points concernant les coûts de l'intégration administrative de la médiation administrative dans l'Autorité. L'Autorité a rappelé que l'avant-projet concerne la modification de l'organisation de la médiation administrative et que, lors des nombreux échanges, il n'a jamais été question de toucher les domaines de la protection des données et de la transparence. Il est relevé que ces ajouts d'articles auraient pour conséquence que dans chacune de leurs communications (rapport d'activité, newsletter, site Internet, etc.), les préposées devraient tout d'abord donner la possibilité à l'organe public concerné de réagir, puis d'intégrer sa prise de position dans leur communication. Premièrement, cette modification est contraire à l'indépendance de l'ATPrD, essentielle à son bon fonctionnement. En effet, l'Autorité doit pouvoir gérer elle-même sa communication vers l'extérieur, sans être mise sous pression par les organes publics soumis à sa surveillance.

Deuxièmement, aucune législation suisse ou européenne en matière de transparence et de protection des données ne prévoit pareille disposition. Troisièmement, un avis de droit rendu par l'Institut du Fédéralisme sur mandat de la Direction de la sécurité et de la justice du canton de Fribourg en 2010¹⁴ rappelle que le pouvoir exécutif ne peut imposer des prescriptions quant au choix et à la manière dont l'autorité de surveillance s'adresse au public. Il résulterait également de ces modifications un surplus de travail administratif et contraire au principe d'une administration efficace pour une Autorité déjà fortement sollicitée.

S'agissant des coûts de l'intégration, la mention dans le Message selon laquelle le projet d'intégration n'aura pas d'incidence en matière de ressources, par exemple financière, a interpellé la Commission. Elle a relevé que cette indication inexacte peut mettre à mal l'indépendance des domaines concernés. En effet, cette indépendance nécessite une séparation des ressources, des espaces de travail et du stockage des dossiers. Les préposées et la médiatrice administrative doivent pouvoir occuper trois bureaux séparés. En outre, cette intégration aura pour conséquence des tâches supplémentaires pour la Commission et le secrétariat de la Commission. Ces dernières doivent être prévues dans le budget de la médiation administrative.

Avant-projet de Loi modifiant la Loi sur le personnel de l'État et avant-projet d'Ordonnance modifiant le Règlement du personnel de l'État

La Commission a rappelé que la digitalisation souhaitée de l'ensemble de la pratique de l'administration cantonale requiert une sensibilisation du personnel à la protection des données ainsi qu'une réglementation plus détaillée sur cette thématique. Elle a constaté qu'aucune disposition légale nouvelle en matière de traitement des données du personnel, notamment traitement électronique, n'était proposée. Selon les exigences légales et jurisprudentielles ainsi qu'au vu de la digitalisation, les dispositions légales actuelles

sont insuffisantes. L'État traite de nombreuses données personnelles, telles que les données des collaborateurs-trices, de leur famille et leurs proches, leurs données de santé, les informations tirées du dossier de candidature et les données relatives aux compétences des collaborateurs-trices, etc. Il gère de nombreuses bases de données, qui sont souvent interconnectées entre elles, de sorte que des données personnelles sont communiquées systématiquement.

L'utilisation du numérique est aujourd'hui légion. L'État doit pouvoir, pour chaque traitement de données, s'appuyer sur une base légale. A noter qu'une grande partie des données peut être qualifiée de sensibles, qui nécessite l'existence d'une base légale formelle. La crise de la COVID-19 a montré la nécessité d'une réglementation adéquate pour l'administration publique. Au vu de l'évolution des technologies et des réalités actuelles du monde du travail, une réglementation circonstanciée en matière de protection des données est attendue s'agissant notamment de l'utilisation d'appareils privés à des fins professionnelles, de la formation et la sensibilisation du personnel eu égard au secret de fonction et à la protection des données, de la sécurité de l'information au sein de l'État, des mesures concernant le télétravail, du co-working, des systèmes d'information utilisés par l'État, etc. Les détails pourront faire l'objet d'ordonnance(s). Le sujet étant complexe, la Commission a donné pour exemple la législation étoffée en matière de traitement des données du personnel de la Confédération.

Projet d'ordonnance concernant la mise en place d'un projet d'annonce électronique des déménagements (Projet-pilote eDéménagement)

Cette consultation fait suite à l'analyse du projet global par la Commission et au préavis défavorable à l'accès FriPers qui relevaient notamment une absence de base légale pour le traitement des données envisagées (cf. *infra* III. B. 1.3).

¹⁴ WALDMANN Bernhard, SPIELMANN André, *L'indépendance de l'autorité cantonale de surveillance en matière de protection des données, avis de droit réalisé sur mandat de la Direction de la Sécurité et de la Justice du Canton de Fribourg*, 2010, p. 52 https://www.fr.ch/sites/default/files/contens/atprd/_www/files/pdf38/Avis_de_droit_F.pdf

Dans la mesure où il n'y a eu aucune communication concernant les contrats en cours de négociation, ni information complète quant à l'état de situation actuelle du projet dans le canton de Fribourg, une analyse détaillée de ce projet peut difficilement être menée. La Commission a toutefois relevé que comme le législateur a souhaité un essai pilote temporaire, les contrats à conclure ne doivent pas excéder la durée maximale de 2 ans prescrite pour la remise du rapport d'évaluation au Conseil d'Etat. En outre, l'échantillon de communes pilotes sélectionnées est trop large. Concernant l'utilisation systématique du numéro AVS, en dehors du domaine des assurances sociales, la Commission a relevé le défaut de base légale pour son utilisation systématique. Celui-ci ne peut être compensé par le consentement de l'administré-e. S'agissant des délais de conservation des différentes données personnelles traitées, les délais proposés par le canton de Berne dans le cadre de ce projet doivent être observés.

Enfin, les mesures de sécurité et de responsabilité n'étant pas clairement définies et en l'absence des garanties demandées en matière de protection des données, la Commission n'a pas pu se prononcer de manière favorable.

2. Dossiers spécifiques

La Commission a également traité de nombreux dossiers en lien avec la digitalisation de l'administration cantonale (cf. Plan directeur de la digitalisation et de ses systèmes d'information). La Commission, respectivement l'un ou l'autre de ses membres à titre individuel ou son Président, a eu en outre de nombreuses activités ponctuelles, comme le démontrent les exemples suivants.

Adaptation de la législation cantonale à certains aspects de la digitalisation

Conjointement à la révision totale de la loi sur la protection des données, l'avant-projet de loi visant à adapter la législation cantonale à certains aspects de la digitalisation a été mis en consultation fin 2019, après une collaboration urgente entre la préposée à la protection des données et différents services et directions de l'Etat. Ce dernier a pour but de modifier la loi actuelle sur la

protection des données en anticipant l'entrée en vigueur de certains articles prévus dans le projet de révision totale de la loi sur la protection des données, tels que l'externalisation, et la loi sur le guichet de cyberadministration de l'Etat (LGCyb) en intégrant notamment l'utilisation systématique du numéro AVS dans le cadre du référentiel cantonal.

Lors des travaux préparatoires, la Commission a communiqué sa prise de position, à savoir qu'elle est contre l'idée de faire entrer de manière anticipée les dispositions concernant l'externalisation de données personnelles, estimant inopportun de «saucissonner» l'avant-projet de révision totale de la LPrD qui regroupe toutes les dispositions traitant des standards de protection adaptés et nécessaires à une externalisation et qui est prêt à partir en consultation. S'agissant de la modification de la loi sur le guichet de cyberadministration de l'Etat, la Commission a maintenu, comme déjà manifesté à maintes reprises, son rejet quant à l'extension de l'utilisation systématique du numéro AVS même si son utilisation peut être élargie lors de la révision de la LAVS.

Courant 2020, la Commission a pris fortuitement connaissance du Message du Conseil d'Etat du 21 avril 2020 accompagnant le projet de Loi adressé au Grand Conseil. Ce projet contenait de profondes modifications par rapport à celui soumis préalablement à l'Autorité. La Commission a alors fait part de sa surprise au Conseil d'Etat, en précisant qu'une prise de contact aurait été adéquate, d'autant plus que les modifications apportées portent sur les définitions et principes cadre du droit de la protection des données. En tant qu'autorité indépendante, son bon fonctionnement doit pouvoir être garanti et une collaboration, voire un échange, lors de l'élaboration et modification de législations dont dépend l'activité de l'Autorité est espéré. De l'avis de la Commission, le projet modifié aurait dû inclure les principes généraux en matière de protection des données dans la LPrD, notamment l'externalisation, et non dans la LCyb comme prévu.

Faisant suite au courrier de la Commission, le Conseil d'Etat a exprimé son regret quant au manque de transparence exercé à l'encontre de l'Autorité. Néanmoins, il

a relevé que l'avis de la Commission a le plus souvent été sollicité dans le cadre de consultations d'avant-projets de textes touchant à la protection des données et a expliqué que la législation en vigueur ne prévoit pas expressément des droits étendus de participation aux travaux d'élaboration de lois connexes. Il a cependant précisé qu'une participation plus active de l'Autorité est projetée dans le cadre de la révision de la LPrD. Concernant le droit de siège légal des dispositions relatives à l'externalisation, le Conseil d'État ainsi que le Service de la législation (SLeg) sont d'un avis contraire et estiment qu'un seul renvoi doit être opéré de la LPrD vers la LCyb. Les divergences étant maintenues, l'Autorité a demandé au Secrétariat du Grand Conseil qu'une délégation de la Commission accompagnée de la préposée à la protection des données puisse être reçue par la Commission parlementaire chargée de traiter dudit projet de Loi. Après avoir été entendue par celle-ci, en présence notamment d'une délégation du SLeg, la Commission parlementaire a sollicité un commentaire écrit succinct de l'Autorité relatif aux articles litigieux. Le souhait de la Commission parlementaire étant, toutefois, de tendre vers un compromis; dans cette idée, des discussions ont eu lieu entre l'Autorité et le Conseil d'État. Après différents échanges, les positions finales de chaque partie ont été communiquées par écrit au Grand Conseil.

Tout en concédant le «sauçonnage» de la LPrD en vue d'une administration 4.0, la Commission a maintenu sa position concernant la non-extension de l'utilisation systématique du numéro AVS. Consciente des débats au niveau fédéral et si le Grand Conseil acceptait cette utilisation, l'Autorité a toutefois souhaité que le projet de Loi adaptant la législation cantonale à certains aspects de la digitalisation prévoit expressément sa consultation préalable quant aux mesures de sécurité. Elle a précisé qu'un accord a été trouvé en matière de traitements de données personnelles qui ont désormais leur siège dans la LPrD. Finalement, eu égard à l'externalisation de traitement de données sensibles ou sous secret particulier, la Commission a privilégié un hébergement en Suisse pour garantir la gouvernance des données soumises au secret de fonction. Le Conseil d'État a finalement proposé un message complémentaire modifié contenant les compromis sur l'ensemble du projet. Toutefois, deux points de divergence ont demeuré, à savoir l'extension

de l'utilisation systématique du numéro AVS dans le référentiel cantonal et l'hébergement privilégié en Suisse.

Lors de sa session ordinaire du 18 décembre 2020, le Grand Conseil a accepté le projet de Loi adaptant la législation cantonale à certains aspects de la digitalisation et suivi, concernant les deux dernières divergences, l'avis du Conseil d'État. Toutefois, un amendement a été accepté, durant la deuxième lecture, demandant au Conseil d'État de présenter tous les deux ans à la Commission des finances et de gestion un rapport sur l'externalisation.

Intégration de la médiation administrative au sein de l'Autorité cantonale de la transparence et de la protection des données

Le Conseil d'État a estimé opportun d'intégrer la médiation administrative au sein de l'Autorité afin qu'elle puisse bénéficier de la Commission cantonale pour l'aider à porter ses projets mais également d'accéder aux ressources en personnel et en locaux de l'Autorité. Après plusieurs discussions réunissant le Président de la Commission et certains de ses membres, la préposée à la transparence, la préposée à la protection des données, des représentants de la Chancellerie, du Service de la législation et de la Direction des institutions, de l'agriculture et des forêts (DIAF), l'Autorité a accueilli favorablement l'intégration de manière administrative à condition que l'indépendance des trois domaines soit garantie. Dans ce cadre, l'Autorité a été amenée à se prononcer à plusieurs reprises sur les projets de loi. Dans un premier temps, une détermination a été faite lors de la pré-consultation (cf. 1.2 ci-dessus), puis lors de la consultation (cf. 1.2 ci-dessus).

Rapport de fin de projet – Projet pilote «outils bureautiques collaboratifs - Microsoft Office 365» daté du 27 novembre 2019

Selon la législation cantonale, le Conseil d'État peut autoriser – après consultation de l'Autorité - le traitement automatisé de données sensibles non justifié par les bases légales en vigueur. Dans ce cadre, l'organe responsable transmet, au plus tard deux ans après la mise en œuvre de la phase d'essai, un rapport d'évaluation au Conseil d'État, lui proposant la poursuite

ou l'interruption du traitement. Si le Conseil d'Etat autorise la poursuite du traitement, il engage immédiatement la procédure législative pour donner une base légale formelle au traitement de ces données. Lors de la mise en consultation de l'avant-projet de loi adaptant la législation cantonale à certains aspects de la digitalisation, l'Autorité a pris fortuitement connaissance qu'un rapport de fin de projet avait été élaboré et transmis au Conseil d'Etat, lequel avait pris acte de son contenu.

En juin 2020, après réception et analyse succincte dudit rapport, la Commission a fait part de ses observations au Conseil d'Etat en les détaillant de manière non-exhaustive. Elle a relevé avoir été surprise du contenu du rapport qui n'est pas suffisamment circonstancié et ne comporte que peu d'analyse technique. De nombreux éléments font défaut et il regorge de plusieurs projets sous-jacents qui nécessitent une analyse non seulement technique mais aussi juridique. Elle a ajouté que ce rapport ne contient pas d'analyse complète des risques du point de vue organisationnel, juridique et technique. De plus, les éléments suivants manquent: le concept SIPD, la liste des données traitées, la classification des données, le flux détaillé des données, l'architecture, les appareils utilisés (professionnels et privés), l'analyse des risques et les mesures permettant de diminuer ces risques, les règlements et directives d'utilisation, les conditions générales d'utilisation et processus de travail, la procédure de «faille de sécurité» (data breach), les instructions données au prestataire de service, la question des responsabilités, etc. Le rapport décrit uniquement les objectifs atteints et les avantages de la solution, sans toutefois prendre en compte les risques du traitement des données dans le Cloud.

En conclusion, la Commission a relevé de grandes lacunes. Les mesures de réduction des risques devraient, à tout le moins, figurer dans le document. D'autant que le rapport fait principalement référence à l'infrastructure. Elle a précisé qu'il serait souhaitable que les flux de données et les processus qui doivent être soutenus par cette infrastructure soient également indiqués, ce qui permettrait d'identifier les risques et de décrire les exigences d'un fonctionnement conforme à la protection des données.

Conscient de la transformation profonde entreprise, le Conseil d'Etat a tenu à répondre aux remarques soulevées par la Commission. Il s'agit pour lui essentiellement de points d'ordre technologique et d'ordre organisationnel, pour lesquels une analyse plus approfondie serait requise en vue d'identifier les mesures adéquates. Certaines mesures pourraient être prises à court terme; mais d'autres nécessiteront indubitablement des réformes organisationnelles demandant plus de temps. Ainsi, le Conseil d'Etat est d'avis que la correction des éventuelles lacunes concernant Office 365 doit se faire en cours d'emploi, sous forme d'apprentissage et non, ex cathedra, avant même de commencer les travaux. Ce nonobstant, il a déclaré qu'il n'est pas prévu à ce stade de stocker l'ensemble des données dans le Cloud et que les données sensibles continueront à être conservées sur les serveurs de l'Etat.

Interview sur le dossier électronique du patient

Un membre de la Commission accompagné de la préposée à la protection des données a participé à une discussion sur le thème du dossier électronique du patient, afin de faire le point de la situation dans la région, notamment d'évoquer les enjeux liés à la protection des données.

Echanges individuels ou par voie de circulation

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 qui soulèvent des questions (par ex. dans le cas des recommandations rédigées par la préposée à la transparence).

B. Domaine de la transparence

1. Evaluation du droit d'accès

Selon les chiffres communiqués à l'Autorité, 67 demandes d'accès ont été déposées auprès des organes publics fribourgeois en 2020. Dans 45 cas, les organes publics ont accordé un accès complet et dans 11 cas un accès restreint. Dans 3 cas, l'accès a été différé. Dans 6 cas, l'accès aux documents a été refusé. 2 cas étaient encore ouverts à la fin 2020. Les domaines les plus concernés étaient les domaines de l'administration, de l'environnement, de l'agriculture et de la justice.

L'évaluation reflète le nombre de demandes d'accès annoncées par les organes publics auprès de l'Autorité. Comme au niveau fédéral, l'Autorité part de l'idée que 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. En moyenne, les organes publics ont annoncé 88 minutes consacrées au droit d'accès en 2020 tandis que d'autres ont investi jusqu'à 11 heures.

C. Domaine de la protection des données

1. Recommandation et recours en cas de non-respect des prescriptions (art. 22a et 30a al. 1 let. c LPrD)

Une tâche légale de la Commission concerne la mise en œuvre de la procédure prévue à l'article 22a en cas de violation ou de risque de violation des prescriptions sur la protection des données. Elle consiste à inviter l'autorité compétente à prendre les mesures nécessaires et, le cas échéant, à interjeter recours auprès du Tribunal cantonal contre une décision de rejet de la part d'un organe public. Durant l'année sous rapport, la Commission n'a fait aucune recommandation. Au vu de la situation sanitaire, l'Autorité a travaillé de manière pragmatique en accompagnant et conseillant les différents services.

2. Recours (art. 27 et 30a al. 1 let. d LPrD)

Dans le cadre des décisions prises conformément aux articles 23 à 26 LPrD, les organes publics doivent communiquer ces dernières à l'Autorité, qui a qualité pour recourir. Durant l'année 2020, la Commission a reçu une copie de 41 décisions, toutes émanant de la Police cantonale (principalement d'accès à ses propres données et de destruction de ses données) sauf 1 adressée par le Tribunal d'arrondissement de la Sarine. La Commission n'a pas interjeté de recours parce que ces décisions lui ont paru conformes à la législation en vigueur. L'Autorité salue notamment la Police cantonale qui lui transmet régulièrement ses décisions.

III. Activités principales des Préposées

A. Transparence

1. Points forts

1.1 Médiations dans le domaine du droit d'accès

Comme la Confédération et de nombreux cantons, celui de Fribourg dispose d'une procédure de médiation dans le domaine de la transparence. La LInf prévoit que celle-ci peut être mise en œuvre entre la personne qui a demandé l'accès et l'autorité concernée, respectivement entre les tiers qui se sont opposés à l'accès au document et l'autorité concernée. Il est possible de déposer une demande de médiation lorsque l'organe public ne prend pas position dans un délai de 30 jours, qu'il diffère, restreint ou refuse l'accès au document souhaité, ou qu'un tiers concerné s'oppose à ce que l'accès soit accordé.

La médiation se déroule, sous la direction de la préposée à la transparence, entre la personne requérante ou celle qui s'est opposée à l'accès au document et l'autorité concernée. La préposée entend les deux parties, qui s'expriment soit par écrit, soit dans le cadre d'une séance de médiation. La préposée a alors accès aux documents officiels pour réaliser la médiation et rendre sa recommandation. La procédure de médiation a pour objectif la conclusion d'un accord entre les parties. Si la médiation aboutit, l'accord est consigné par écrit et devient immédiatement exécutoire. Si elle échoue, la préposée à la transparence établit une recommandation à l'intention des parties. L'organe public rend ensuite une décision.

En 2020, le nombre de demandes en médiation et de demandes de renseignement est resté très élevé. 20 demandes en médiation ont été déposées auprès de la préposée à la transparence. Contrairement à 2019, où 12 demandes en médiation concernaient le même document et la préposée à la transparence avait dans ce cas rendu une recommandation, en 2020, chaque médiation a concerné un autre document. Dans 10 cas, un accord a été trouvé. La préposée a rendu 9 recommandations (dont 2 demandes en médiation dataient de 2019 et pour 1 médiation, les parties ont accepté que 2 recommandations soient rendues). Dans 1 cas et après échange avec les parties, la préposée à la transparence n'a pas pu entrer en matière. 2 requêtes en

médiation ont été retirées par la personne requérante. 2 requêtes en médiation étaient encore pendantes à la fin de l'année. Cette stabilisation du nombre de requêtes en médiation à un niveau élevé a eu pour conséquence que la préposée à la transparence n'a pas toujours pu accomplir ses tâches dans les délais prévus par la LInf.

Les accords de médiation peuvent revêtir différentes formes. Durant l'année sous rapport, des accords ont été conclus. Certains accords ont permis d'identifier les documents qui contenaient les informations recherchées par les personnes requérantes. Dans d'autres médiations, les personnes ayant demandé l'accès aux documents ont finalement renoncé à y obtenir l'accès et se sont contentées d'informations sur ceux-ci. Dans d'autres cas encore, les parties à la médiation se sont mises d'accord sur l'accès au document, éventuellement de manière différée ou caviardée.

Les demandes de médiation concernaient des documents très divers. Voici quelques exemples qui ont abouti à une recommandation.

Dans l'une d'elle, la demande d'accès portait sur des **courriers échangés** entre la Préfecture de la Sarine et la commune de Villars-sur-Glâne concernant des dénonciations faites en matière de police des constructions. Dans sa recommandation, en partant de l'hypothèse où le dénonciateur n'a pas la qualité de partie, la préposée a relevé que la LInf s'applique et recommandé en raison d'un intérêt public prépondérant (art. 26 al. 1 let. c LInf) d'octroyer un accès différé aux courriers une fois les procédures en lien avec les dénonciations terminées. Elle a estimé qu'un accès immédiat risquerait d'entraver notablement le processus décisionnel de l'organe public. Dans l'hypothèse où le requérant a la qualité de partie, la préposée a remarqué que seule la législation spéciale s'applique (art. 21 al. 1 let. b LInf) et que, ce faisant, l'accès ne peut pas être accordé selon la LInf.

Dans un autre cas, le requérant a demandé à la commune de Villars-sur-Glâne l'accès à **la copie de la note d'honoraires de l'avocat avec la feuille de détail des heures facturées**. Dans sa recommandation,

la préposée à la transparence a recommandé à la commune de maintenir son refus d'octroyer l'accès à ces documents. Elle a estimé que l'accès pouvait entraver notamment le processus décisionnel de l'organe public (art. 26 al. 1 let. c LInf) et compromettre sa position de négociation (art. 26 al. 1 let. e LInf). Si l'organe public devait ouvrir sa correspondance avec son avocat à la partie avec laquelle elle a un différend, les deux parties ne seraient plus sur un pied d'égalité quant aux informations dont elles peuvent disposer.

Une autre demande d'accès concernait les **coûts** assumés par la Bibliothèque cantonale et universitaire (BCU) dans le cadre d'abonnements à des revues scientifiques. Dans sa recommandation, la préposée a estimé que la BCU disposait d'une marge de manœuvre pour traiter cette demande d'accès, en raison de l'arrêt du Tribunal fédéral 1C_40/2017 du 5 juillet 2017 qui concernait une affaire similaire. A l'instar de la recommandation de 2016 dans un cas semblable, elle a recommandé d'octroyer l'accès au document demandé estimant que les motifs en faveur de l'accès l'emportaient.

Dans un cas qui concernait le domaine de l'environnement, la préposée à la transparence a recommandé à la Direction de l'aménagement, de l'environnement et des constructions (DAEC) d'octroyer l'accès à **deux rapports historiques de 2009 sur la décharge de la Pila**. Elle a estimé que l'article 21 al. 1 let. a LInf, qui prévoit que la consultation des documents relatifs à des procédures de juridiction administrative pendantes est régie exclusivement par la législation spéciale, n'était pas applicable. En effet, les deux rapports avaient été établis indépendamment de la procédure actuellement en cours une dizaine d'années avant que celle-ci ne débute. Un lien temporel étroit avec la procédure en cours n'était pas donné. Par ailleurs, la préposée à la transparence était d'avis que l'accès ne pouvait pas être différé en raison d'une entrave notable au processus décisionnel (art. 26 al. 1 let. c LInf), car les documents en question n'avaient pas été établis en vue d'une prise de décision sur la question de la répartition des responsabilités. Ainsi, l'utilisation d'un document dans un processus décisionnel ultérieur ne suffit pas à le retirer du droit d'accès garanti par la

LInf, et ce, d'autant plus lorsque les documents touchent à l'environnement (art. 4 de la Convention d'Aarhus).

L'année 2020 a débouché sur **4 arrêts** en matière de droit d'accès.

Le **Tribunal fédéral** a confirmé la décision de 2019 du Tribunal cantonal (601 2019 19) dans son arrêt 1C_353/2019 du 18 mars 2020. Dans cette affaire, le requérant ne s'était pas présenté à la séance de médiation sans motif valable et la préposée avait considéré la requête en médiation comme retirée. Le requérant avait fait recours contre ce classement, tout d'abord au Tribunal cantonal qui avait rejeté le recours, puis au Tribunal fédéral contre l'arrêt du Tribunal cantonal. D'après le Tribunal fédéral, la préposée à la transparence est libre de mener la procédure de médiation comme elle l'entend (art. 14 al. 2 OAD) dans le cadre de son pouvoir d'appréciation et les parties doivent suivre ses injonctions. La médiation constitue une étape obligatoire de la procédure d'accès et le requérant ne peut s'en dispenser de sa propre initiative.

Le **Tribunal cantonal** a rendu trois arrêts en matière de droit d'accès.

Dans le **premier arrêt** 601 2020 52 du 20 avril 2020 (non publié), le Tribunal cantonal a rayé du rôle un recours devenu sans objet. Une personne avait fait recours contre une ordonnance du Ministère public rendue suite à une demande d'accès. Dans son ordonnance, le Ministère public avait décidé d'octroyer l'accès aux documents sollicités et la personne concernée par ceux-ci avait fait recours contre cette ordonnance. Dans sa décision, le Tribunal cantonal a indiqué que le Ministère public aurait dû suivre la procédure prévue par la LInf et rendre une détermination au sens de la LInf, et non pas une ordonnance. Etant donné que la personne qui avait fait la demande d'accès a indiqué y renoncer, l'affaire est devenue sans objet.

Dans le **deuxième arrêt** (601 2019 207 et 601 2019 219) du 14 mai 2020, le Tribunal cantonal s'est prononcé sur la contestation d'un accord de médiation par la requérante. Celle-ci avait fait recours et ouvert action, car elle était d'avis que la Préfecture de la Sarine n'avait

pas exécuté correctement l'accord de médiation. Le Tribunal cantonal a déclaré irrecevables les deux requêtes et renvoyé le dossier à la préposée «*comme objet de sa compétence*». Il a jugé que l'accord de médiation selon la LInf «*a été formulé en des termes très généraux et qu'il s'apparente à une déclaration d'intention et s'avère difficilement justiciable, vu son caractère imprécis. Dans ces conditions, on doit considérer que le recours dont est saisi le Tribunal cantonal constitue au mieux une demande de reconsidération, respectivement d'interprétation, de la décision constatatoire qui a mis fin à la procédure d'accès. Il convient dès lors de transmettre cet acte à la Préposée à la transparence, comme objet de sa compétence*».

Dans le **troisième arrêt** 601 2019 96 du 9 novembre 2020, le Tribunal cantonal a décidé que l'accès partiel à un rapport d'une enquête administrative menée par la Préfecture de la Broye devait être accordé après consultation des tiers, qui pouvaient faire valoir un intérêt privé prépondérant pour s'y opposer et saisir la préposée d'une demande en médiation, à l'instar de la recommandation du 18 février 2019 de la préposée à la transparence.

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

En tant que suppléante de la médiatrice administrative cantonale, la préposée n'a traité aucun dossier en 2020.

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 s'est révélé très large, comme les années précédentes.

En 2020, 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 pas prendre position dans des cas concrets, sous réserve de la formulation d'une recommandation au sens de l'article 33 LInf. La

préposée à la transparence doit demeurer aussi neutre que possible avant cette étape. Les exemples suivants illustrent des questions posées et les réponses données:

Lorsqu'une demande d'accès concerne un document qui était public lors d'une procédure passée, peut-on accorder directement l'accès?

Situation initiale:

Un organe public a demandé si un document accessible au public pendant la mise à l'enquête d'un permis de construire, qui fait l'objet d'une demande d'accès ultérieurement, doit être traité selon la procédure prévue par la LInf.

Réponse:

La préposée à la transparence a relevé que ce n'est pas parce que le document a été accessible au public pendant une procédure spécifique qu'il faut renoncer à traiter une demande ultérieure conformément à la LInf. Il faut en particulier consulter les tiers lorsque l'accès risque de porter atteinte à un intérêt privé.

Une clause de confidentialité entre une commune et une entreprise privée dans un document concernant un projet dans le domaine de l'environnement est-elle valable?

Situation initiale:

Un requérant voulait savoir si une clause de confidentialité passée entre une commune et une entreprise privée dans un document concernant un projet dans le domaine de l'environnement est compatible avec les exigences de transparence de la LInf.

Réponse:

La jurisprudence reconnaît trois conditions cumulatives pour qu'une clause de confidentialité soit valable. Les informations doivent avoir été fournies à l'organe public par une personne privée. Elles l'ont été librement et non pas dans le cadre d'une obligation légale ou contractuelle. Enfin, l'organe public doit s'être engagé à la confidentialité sur demande expresse du privé. Les documents qui touchent à l'environnement ont

droit à un traitement particulier. La LInf prévoit que, lorsque la demande d'accès concerne des informations sur l'environnement, les exceptions normalement applicables doivent être interprétées de manière restrictive compte tenu de l'intérêt que la divulgation des informations demandées présenterait pour le public et selon que ces informations ont trait ou non à des émissions dans l'environnement. Cette particularité découle de la Convention d'Aarhus adoptée en 1998 au Danemark et ratifiée en 2014 par la Suisse. Cette convention européenne traite de l'accès à l'information, à la participation du public au processus décisionnel et à l'accès à la justice en matière d'environnement.

Comment traiter une demande d'accès aux registres de l'impôt ordinaire?

Situation initiale:

Une personne a demandé accès aux registres de l'impôt ordinaire dans une commune. Comment la commune doit-elle traiter cette demande?

Réponse:

La loi sur les impôts cantonaux directs (LICD; RSF 631.1) prévoit une disposition sur le secret fiscal (art. 139 LICD) ainsi qu'une disposition sur la publicité des registres de l'impôt (art. 140 LICD). Selon l'article 139 al. 1 LICD, les personnes chargées de l'application de la LICD doivent refuser aux tiers la consultation des dossiers fiscaux. L'article 139 al. 2 let. a-d LICD prévoit des conditions pour la communication de renseignements à des tiers.

Selon l'article 140 al. 1 LICD, les registres de l'impôt ordinaire contenant la mention de la cote d'impôt sur le revenu et la fortune sont déposés dans les communes, où ils peuvent être consultés pendant deux mois par an par toute personne ayant qualité de contribuable à l'impôt cantonal sur le revenu et la fortune. L'article 140 LICD spécifie à ses alinéas 2 à 7 certaines conditions, à savoir par exemple qu'aucune consultation ne peut avoir lieu par correspondance ou par téléphone et que

les communes doivent tenir un registre public des personnes ayant consulté les registres de l'impôt. Ces diverses conditions doivent être prises en compte dans le traitement de la demande.

L'ordonnance concernant la consultation des registres de l'impôt précise les modalités de la consultation des registres de l'impôt. Par exemple, l'ordonnance prévoit que les registres de l'impôt cantonal comprennent le nom, prénom et adresse de tous les contribuables de la commune dont la taxation est définitive ainsi que leurs cotes d'impôt sur le revenu et la fortune (art. 3 al. 1 de l'ordonnance), que les registres de l'impôt peuvent être consultés de début septembre à fin octobre par toute personne ayant qualité de contribuable à l'impôt cantonal sur le revenu et la fortune (art. 1 al. 1 de l'ordonnance) et que peuvent être consultés les registres de l'impôt qui précèdent de 2 ans l'année courante (art. 2 al. 1 de l'ordonnance).

Il ressort que les registres de l'impôt ordinaire contenant la mention des cotes d'impôt sur le revenu et la fortune peuvent être consultés conformément à l'article 140 LICD et à l'ordonnance concernant la consultation des registres de l'impôt. Une consultation des personnes concernées avant la consultation des registres de l'impôt ordinaire contenant la mention de la cote d'impôt sur le revenu et la fortune n'est pas prévue par la loi.

2. Statistiques

Durant la période considérée, 184 dossiers ont été introduits. Parmi ces dossiers, 28 sont pendants au 1^{er} janvier 2021, 45 conseils et renseignements, 21 avis, 30 examens de dispositions législatives, 10 présentations, 31 participations à des séances et autres manifestations, 20 demandes en médiation et 27 demandes diverses. 67 dossiers concernent des organes cantonaux ou des institutions chargées de tâches publiques, 18 des communes, 48 d'autres organismes publics (cantons, autorités de transparence et protection des données), 42 des particuliers ou institutions privées et 9 des médias (cf. statistiques annexées).

B. Protection des données

1. Points forts

Le domaine de la protection des données a, une nouvelle fois, fait face à une forte augmentation de la charge de travail (+15%). Toutefois, ce n'est pas uniquement le nombre de dossiers qui a augmenté mais plus encore leur complexité, qui nécessite des connaissances spécifiques et touche à différents acteurs. La digitalisation de l'administration cantonale n'a cessé d'amener de nouveaux projets complexes. En parallèle, la pandémie a donné un coup d'accélérateur à la digitalisation, entraînant une utilisation étendue des solutions informatiques et modifiant le mode de travail de l'administration. A ce jour, le domaine de la protection des données connaît une surcharge de travail due à l'augmentation constante des dossiers complexes et des ressources limitées dont la préposée dispose. C'est pourquoi, la préposée n'a pas pu, dans la mesure souhaitée, accomplir de manière satisfaisante ses tâches dans le domaine de la protection des données et de la sécurité de l'information.

1.1 Coronavirus

Malgré la pandémie COVID-19, la sphère privée et la protection de la personnalité doivent être garanties. Dans ce contexte, l'Autorité doit faire preuve de pragmatisme si elle veut avoir un impact puisque la pandémie a amené des changements importants et des restrictions drastiques de la sphère privée et de l'autodétermination. Toutefois, l'Autorité doit penser également à demain car la collecte systématique de données personnelles par l'Etat mais aussi par des acteurs privés est susceptible de modifier à long terme la question de l'autodétermination. Ainsi, la protection des données est prise en étau entre le droit que chacun a de protéger sa sphère privée et de gérer soi-même les informations le concernant et le devoir qu'ont la Confédération et les cantons de protéger les personnes d'un point de vue sanitaire.

Au vu de la situation du coronavirus, certains responsables de direction et d'établissement ont consulté la préposée à la protection des données dans le cadre de l'analyse préalable de leur projet informatique.

En effet, certains organes publics ont dû trouver rapidement des solutions informatiques leur permettant de mettre en œuvre des traitements de données et des moyens de communications. Les responsables de traitement ont alors dû négocier avec des entreprises privées pour la mise à disposition immédiate de solutions informatiques, conformes à la protection des données, indisponibles au sein de l'Etat.

L'Autorité a également dû faire face à de nombreuses demandes concernant l'utilisation des outils et applications informatiques ainsi qu'au traitement de données personnelles des collaborateurs de l'Etat mais également des citoyen-ne-s. Ci-dessous, vous trouvez quelques exemples représentatifs.

Systeme de traçage

Durant cette période particulière, des mesures ont été prises successivement pour endiguer la propagation du coronavirus. Dans ce cadre, un système de traçage a été mis en place dans différents secteurs, notamment auprès des établissements publics (restaurants, bars, etc.) ou lors d'événements culturels. Le canton de Fribourg a dû mettre rapidement le traçage en œuvre. Il est ressorti de diverses communications publiques que le canton a vivement recommandé l'utilisation de l'application OK-Resto et peu après OK-Visite. A cet égard, la préposée à la protection des données a pris contact avec les différentes personnes et services concernés, dans la mesure où les données collectées par le secteur privé doivent être transmises à l'Etat. Des questions relatives au flux des données mais également à l'accès, à la durée de conservation, à la communication des données ainsi qu'aux mesures de sécurité se posent.

De nombreux échanges ont eu lieu avec les autres autorités de protection des données et le PFPDT à ce sujet. Selon les solutions choisies, des analyses communes et concertées ont été effectuées. Dans la mesure où la sous-traitance est confiée à des acteurs privés et que des tâches publiques sont complétées par des tâches privées, une collaboration régulière est nécessaire entre les différentes autorités de protection des données au vu de leur compétence respective.

Service de télémédecine

Un établissement hospitalier a fait les démarches pour mettre en place un service de télémédecine afin de venir en aide aux personnes à risque. La possibilité est ainsi donnée de consulter un-e praticien-ne sans nécessairement devoir se déplacer, ceci par le biais d'une valise diagnostique (soignant en présentiel et médecin en consultation à distance). Dans sa détermination, la Commission a adressé au requérant différentes remarques concernant les documents transmis qui, vu le délai d'urgence accordé, ne se voulaient pas exhaustifs, ne permettant pas ainsi une analyse complète. Par ailleurs, la Commission a rappelé que, malgré la situation d'urgence, un contrat devait être négocié en amont et un concept SIPD décrivant les risques et les mesures pour les réduire devait également être établi au vu de l'externalisation du traitement de données personnelles sensibles. Il est demandé une précision quant au périmètre des données traitées, au lieu de localisation des *back-up*, à la durée de conservation des données, aux possibilités de modification des données et aux mesures techniques et organisationnelles (authentification, chiffrement, description des rôles, etc.).

Suite à la détermination de la Commission, une solution intermédiaire a été choisie afin de pouvoir procéder à un examen approfondi de la solution, à l'élaboration du concept SIPD ainsi qu'à la négociation du contrat. Pour ce faire, il a été décidé de ne pas mettre de données personnelles, ni même identifiables – ni ID ni image ni audio –, sur le «*Cloud*». Seul le flux transitera par le «*Cloud*».

Applications de visio- et vidéoconférence

Différents services et établissements de l'Etat ont consulté l'Autorité pour savoir si les outils utilisés à l'interne sont conformes à la protection des données ou pour connaître les outils disponibles au sein de l'Etat et respectant la protection des données. Une attention particulière est portée lors de traitement(s) de données sensibles et confidentielles.

Mesures économiques extraordinaires COVID

Suite aux restrictions mises en place fin 2020 pour lutter contre le coronavirus, le Conseil d'Etat a adopté des lois régissant les mesures économiques en faveur des entreprises et des indépendants contraints à la fermeture et leurs employé-e-s ainsi que des mesures urgentes visant à surmonter l'épidémie de COVID-19. Dans ce cadre, la Direction de l'économie et de l'emploi (DEE) a consulté la Commission concernant les projets législatifs et l'analyse de la solution informatique y relative. En effet, une solution externe à l'Etat a été privilégiée dans la mesure où aucune solution informatique interne ne permettait le traitement de manière électronique et dans les délais prévus. S'agissant d'une externalisation de traitement de données dans un *Cloud* privé, une analyse juridique mais également technique, a été effectuée.

1.2 CoPil, CoPro et groupes de travail

En 2020, la préposée à la protection des données a traité divers dossiers concernant des projets préliminaires. De plus, elle a participé régulièrement à des groupes de travail (notamment groupe de travail légal, comité de conformité du référentiel cantonal, groupe de travail santé intercantonale), à des CoPil (HAE, Cybersanté, référentiel cantonal) et à des CoPro (communication unifiée). La fréquence de ces différentes séances, plusieurs fois par mois, explique en partie l'augmentation de la charge de travail de l'Autorité. Ces dossiers se traitent sur le long terme avec de nombreux acteurs internes et externes à l'Etat.

Les exemples suivants démontrent la complexité toujours grandissante des projets. En effet, d'une part ceux-ci interconnectent des données de partenaires privés avec des données de l'administration publique limitant la compétence de l'Autorité à une partie du projet uniquement. D'autre part, les projets sont toujours plus denses et s'étendent sur plusieurs années. Pour rappel, le PFPDT est compétent en ce qui concerne le traitement de données par des privés et par des organes publics fédéraux. En outre, il arrive régulièrement que plusieurs cantons et/ou le PFPDT soient également concernés par les mêmes projets, de

sorte que l'Autorité se doit de travailler de concert avec les autres préposés cantonaux en protection des données et le PFPDT.

Révision totale de la LPrD

Les travaux en vue de la révision de la LPrD et de son adaptation à la législation européenne et fédérale ont été suspendus en 2020. Suite à la mise en consultation fin 2019, une analyse des retours de consultation a été faite. En septembre 2020, la nouvelle loi fédérale sur la protection des données a été adoptée, de sorte que la révision de la loi cantonale peut alors reprendre.

Mise en œuvre du Référentiel cantonal

La mise en œuvre du Référentiel cantonal de données de personnes, organisations et nomenclatures est un dossier très prenant. La préposée à la protection des données a participé à différents groupes de travail, tels que le Comité de conformité des données référentielles, le CoPil élargi et, avec voix consultative, à la Commission de gouvernance des données référentielles. La préposée a dispensé une formation modulaire aux personnes répondantes à la protection des données concernées par le projet et a participé au groupe de travail légal traitant de l'application des bases légales en matière de protection des données dans les processus liés au Référentiel cantonal. Cette mise en œuvre est actuellement toujours en cours et devrait se poursuivre. Pour plus d'informations, le site Internet de l'Etat de Fribourg publie les actualités y relatives (<https://www.fr.ch/cha/vie-quotidienne/demarches-et-documents/le-referentiel-cantonal>).

CoPil HAE

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 référence concernant les élèves, les enseignant-e-s et les employé-e-s des écoles du canton de Fribourg, les établissements scolaires, le cursus scolaire des élèves ainsi que les données de référence 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. La préposée à la protection des données a participé aux séances du CoPil par le biais de visioconférences.

Cybersanté

Dans le domaine de la santé numérique, la préposée à la protection des données est membre du groupe d'accompagnement du projet Cybersanté. En effet, le canton de Fribourg collabore étroitement avec d'autres cantons romands, notamment via l'Association CARA qu'ils ont fondée en mars 2018. L'Association a pour but de mettre en place une plateforme de santé numérique qui vise la mise à disposition du dossier électronique du patient (DEP) aux professionnels et aux patients des cantons concernés mais également d'autres services complémentaires de santé numérique, tels que les plans de médicaments partagés ou le plan de soin partagé. En raison des données personnelles sensibles, soumises aux secrets médical et de fonction, et de la diversité des bases légales applicables, il s'avère nécessaire d'établir une distinction entre les différents services de santé numérique qui seront proposés au travers de la plateforme de santé numérique. Le DEP est soumis à la législation fédérale spécifique de la LDEP et de ses ordonnances d'application qui réglementent de manière détaillée son utilisation et qui donnent la compétence en matière de surveillance au PFPDT. A l'inverse, les services complémentaires, qui n'ont actuellement aucune base légale, sont soumis aux différentes législations cantonales en matière de protection des données, ce qui a pour corollaire une compétence des autorités cantonales de protection des données.

Au cours de l'année 2020, la préposée à la protection des données a eu de nombreux échanges avec les autorités cantonales de protection des données, le PFPDT et CARA, durant lesquels un projet de convention intercantonale, de même que des projets de formulaire de consentement et des documents d'information aux personnes concernées ont été établis. En outre, CARA a organisé une démonstration du DEP pour les autorités de protection des données.

1.3 Dossiers complexes

Pendant l'année sous rapport, la préposée à la protection des données a été fortement intégrée dans le processus de digitalisation des systèmes d'information de l'Etat de Fribourg (stratégie Fribourg 4.0). Cette implication est grandement appréciée par la préposée, dans la mesure où elle permet d'obtenir des solutions conformes à la protection des données et de collaborer avec les différents acteurs dès les prémices. Cependant, le nombre de projets dans le domaine de la digitalisation et des systèmes d'information est en constante augmentation et leur complexité toujours plus importante. En raison des liens avec l'informatique et la digitalisation, ceux-ci nécessitent impérativement des connaissances spécifiques, qui touchent notamment le juridique, l'informatique, les nouvelles technologies et la procédure administrative. En sus des dossiers détaillés (cf. *supra* II. A. 2.), voici quelques exemples supplémentaires.

Plateforme eDéménagement

Le canton de Fribourg souhaite intégrer une procédure d'annonce des déménagements en ligne par le biais du guichet virtuel de cyberadministration. Dans ce contexte, l'Autorité a été consultée pour, d'une part, analyser le projet dans son intégralité et, d'autre part, émettre un préavis dans le cadre de la procédure de demande d'accès et d'interfaçage par *Webservices* aux données FriPers avec la plateforme eDéménagement.

S'agissant de la demande d'accès aux données FriPers du secrétariat de cyberadministration, l'Autorité a émis un préavis défavorable, duquel il ressort clairement l'absence de nécessité pour le guichet de cyberadministration d'accéder aux données FriPers. En effet, le flux des données envisagé est communiqué entre les plateformes eDéménagement et FriPers via Sedex (plateforme d'échange sécurisé de données appartenant à la Confédération), de sorte que le guichet de cyberadministration n'a pas accès aux données FriPers et n'en a pas la nécessité. Partant, la demande d'accès devrait être formulée par eOperations Suisse SA – qui détient eDéménagement – et non par le secrétariat de cyberadministration (par le biais de la Chancellerie d'Etat). Toutefois selon le droit actuel, eOperations Suisse SA, en tant que personne de droit privé, ne peut obtenir qu'un accès indirect aux données

FriPers (extraction de données) et ce pour autant qu'il soit chargé de l'exécution d'une tâche publique. En admettant qu'eOperations Suisse SA effectue des tâches de droit public, cet accès ne lui est, néanmoins, pas nécessaire et est disproportionné. Il faut aussi relever que la législation fribourgeoise, en particulier la Loi sur le contrôle des habitants (LCH), ne contient pas de disposition légale permettant l'utilisation systématique du numéro AVS, condition sine qua non pour son utilisation systématique.

Dans le cadre de l'analyse du projet dans son intégrité, l'Autorité a relevé des lacunes en matière de protection des données dans les documents transmis: notamment la convention et le concept SIPD. En outre, un contrat doit être négocié avec eOperations SA mentionnant les conditions minimales de protection des données dans le cadre d'une externalisation du traitement de données, comme le lieu d'hébergement, les mesures de sécurité, la confidentialité, etc.

Vu l'absence de base légale autorisant le traitement souhaité et conformément à la possibilité de traiter systématiquement des données sensibles dans le cadre d'un projet pilote, la Direction de la sécurité et de la justice (DSJ) a mis en consultation, en septembre 2020, un projet d'ordonnance concernant la mise en place d'un projet d'annonce électronique des déménagements (projet pilote). Dans sa détermination (cf. *supra* II. A. 1.2), la Commission a relevé différentes lacunes.

En parallèle, dans le cadre de la révision en cours de la loi sur le contrôle des habitants, une proposition de bases légales est ajoutée afin d'étendre l'accès par procédure d'appel aux données de FriPers en faveur des personnes privées au bénéfice d'une tâche publique, d'un mandat de prestations et/ou d'une subvention de l'Etat; en d'autres termes, à eOperations Suisse SA. Par la suite, un nouveau projet d'ordonnance remanié a été soumis à l'Autorité. Il ressort de la réponse de la Commission différentes contradictions et incohérences dans le projet, telles que la notion de procédure d'appel et de projet pilote, l'existence ou non d'une base légale pour l'utilisation systématique du NAVS par eOperations Suisse SA et le contenu du contrat à négocier avec eOperations Suisse SA.

L'Autorité a précisé que, dans le cadre de ce projet, elle est en étroite collaboration avec les autres autorités cantonales en vue d'une application uniforme des règles de protection des données. Le dossier est actuellement en cours de traitement, en particulier des négociations sont en cours avec eOperations Suisse SA.

Swiss Library Service Platform SA – mise en place d'un système de gestion commune des bibliothèques universitaires suisses

Depuis 2018, des contacts ont eu lieu au sujet du traitement des données personnelles dans le cadre du projet de la migration d'un système de gestion commune des bibliothèques universitaires suisses. En effet, à l'échelle nationale, la volonté est la fusion des catalogues des bibliothèques universitaires dans la plateforme suisse de services aux bibliothèques (SLSP). L'objectif est d'uniformiser l'accès au prêt au niveau suisse afin que chaque utilisateur puisse accéder à toutes les bibliothèques universitaires suisses avec un seul compte.

En 2020, une demande formelle quant à la conformité du projet à la législation sur la protection des données a été déposée auprès de l'Autorité. A cet égard, il a été précisé que les universités de Berne, Bâle et Zurich ont prévu d'effectuer des contrôles préalables auprès de leurs délégués cantonaux à la protection des données respectifs et ont demandé un contrôle coordonné de la situation de fait et de droit. Afin d'agir de manière coordonnée, la préposée à la protection des données a pris contact avec ses homologues pour faire un point de situation et établir une réponse commune. Un examen préalable a été élaboré par les autorités des cantons précités. Une analyse des contrats, voire leur élaboration, a été requise pour examiner la conformité du projet. S'agissant d'une externalisation du traitement des données dans un *Cloud*, il a été rappelé que la base légale concernant l'externalisation était en cours de discussion auprès du Grand Conseil. Du point de vue contractuel, les points problématiques relatifs à la conformité de la protection des données (durée du contrat, hébergement dans un Etat où la législation est adéquate, chiffrement des données, etc.) ont été communiquées à la requérante, en sus de la prise en compte des points relevés dans l'analyse préalable des autres autorités cantonales à la protection des données.

1.4 Demandes

Autant les unités de l'administration cantonale, les communes, les organes d'institutions privées chargées de tâches de droit public aussi bien que les particuliers, d'autres autorités en protection des données et organismes ainsi que les médias 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.

Les exemples suivants illustrent les questions posées et les prises de position de la préposée à la protection des données:

Demande de communication de l'adresse de la nouvelle école d'un enfant par une école privée

Aux termes de l'article 17 alinéa 1 de la Loi sur le contrôle des habitants (LCH), le ou la préposé-e au contrôle des habitants peut, dans un cas déterminé, communiquer à un particulier ou à une organisation privée qui rend vraisemblable un intérêt légitime les nom, prénom(s), sexe, date de naissance, état civil, profession, adresse et date d'arrivée, ainsi que, le cas échéant, la date de départ et la destination d'une personne déterminée. L'adresse de la nouvelle école d'un-e élève ne figurant pas sur la liste, cette communication à un privé n'est pas conforme à la législation précitée.

Coordonnées du dénonciateur ou de la dénonciatrice

Une commune a souhaité savoir quelle suite donner à la demande d'une détentrice d'un chien qui désirait connaître l'identité des personnes s'étant plaintes de son animal. En présence d'une procédure ouverte, l'Autorité a rappelé que ce sont les règles y relatives qui s'appliquent. A défaut de procédure pendante, la commune doit s'assurer que la communication est justifiée par une base légale, voire qu'elle résulte de l'accomplissement d'une tâche légale, d'un intérêt privé prépondérant, voire du consentement du dénonciateur ou de la dénonciatrice. Il est vivement recommandé d'obtenir le consentement écrit de la personne concernée. A défaut, il revient à la commune de faire une pondération des intérêts.

Transmission du nom d'un propriétaire à l'assurance accident

Une commune a sollicité le concours de l'Autorité suite à une demande de communication des données personnelles d'un habitant de la commune à une assurance, après qu'un de leur assuré ait chuté de son VTT en raison d'un fil barrant un chemin appartenant audit habitant. L'assurance concernée est un établissement autonome de droit public. Dans un cas déterminé, une communication de données personnelles est possible en présence d'une base légale, voire dans l'accomplissement d'une tâche. Dans ce cadre, une disposition légale de la Loi fédérale du 6 octobre 2000 sur la partie générale du droit des assurances sociales (LPGA) permet à la commune de communiquer à l'assureur les données nécessaires pour faire valoir une prétention récursoire contre le tiers responsable.

Rectification de décision judiciaire

Suite à la demande d'un administré quant aux possibilités face à l'inexactitude d'information le concernant figurant dans une ordonnance pénale, l'Autorité a rappelé que la LPrD ne s'applique que pour autant qu'une procédure judiciaire est close – à l'exception de la procédure administrative de 1^{re} instance (Message N° 104 du 13 septembre 1994 accompagnant le projet de Loi sur la protection des données, BGC novembre 1994, 3041 ss, 3046). En matière procédurale, c'est la législation y relative qui s'applique.

Toutefois, la procédure pénale close, l'administré peut alors obtenir que l'organe public rectifie les données le concernant. Eu égard à la protection des données, les prérogatives sont notamment la rectification des données incorrectes ou non-conformes à la vérité. Il est précisé que l'appréciation portée sur un état de fait relève, quant à elle, de la procédure et donc des règles y relatives.

1.5 Violations de la sécurité des données

Envoi par erreur d'un courriel à plus de 1000 destinataires visibles

La protection des données est violée lorsque les données personnelles sont irrémédiablement détruites ou perdues, accidentellement ou illicitement altérées ou divulguées ou que des personnes non autorisées y ont accès. Dans ce cas précis, un service a envoyé un courriel à de nombreux destinataires non cachés. Ces derniers étant informés de la violation de la protection

des données impliquant leurs données personnelles, le service concerné a reçu des réclamations de certains d'entre eux. Selon la nature des collaborations, des répercussions peuvent être possibles sur les personnes concernées par ce traitement illicite, comme par exemple une perte financière, une perte de contrôle sur les données personnelles, une atteinte à la réputation, voire un autre dommage économique ou social. L'Autorité a été informée du traitement illicite. En outre, elle a renseigné les personnes concernées au sujet de leurs droits.

Piratage informatique

Une institution a été attaquée par des pirates informatiques. Les hackers ont obtenu l'accès au profil de collaborateurs de l'institution et ont modifié leurs coordonnées bancaires utilisées pour le versement des salaires. Les pirates ont obtenu les mots de passe des collaborateurs par le biais d'actions de phishing (hameçonnage). Suite à cet événement, l'Autorité a contacté l'institution afin de connaître les mesures mises en place concernant la sécurité informatique et de l'information. Il a été recommandé de sensibiliser et de former régulièrement son personnel à ce sujet. L'institution a confirmé mettre en place une double authentification pour éviter que cela se reproduise.

2. Contrôles

D'entente avec la Commission, la préposée à la protection des données a procédé à plusieurs contrôles axés sur le respect des principes de la protection des données au sein de deux administrations communales et de deux services de l'Etat. Le contrôle a été confié à une spécialiste externe, néanmoins la préposée à la protection des données a assisté à tous les contrôles. Ces derniers peuvent prendre différentes formes, à savoir un contrôle planifié, annoncé et organisé, ou un contrôle spontané, un contrôle général voire un contrôle limité à certaines activités de l'organe public. Afin de pouvoir sensibiliser le plus grand nombre d'organes publics au sujet de la sous-traitance et de la digitalisation de l'administration, la préposée à la protection des données a procédé à des contrôles organisés et limités à certaines activités. Il convient de relever la bonne coopération des responsables et des collaborateurs concernés lors des audits. Toutefois, un contrôle de grande envergure dans un service cantonal a dû être repoussé à 2021.

Le but des contrôles est d'examiner le travail des services désignés sous l'angle des dispositions légales en matière de protection des données, notamment les droits et profils d'accès aux applications informatiques et aux bases de données utilisées, l'externalisation de traitement de données personnelles (sous-traitance, délégation de tâches) et les mesures de sécurité. Les rapports sont en cours de rédaction.

Faute de ressources, l'Autorité n'a pas été en mesure d'effectuer d'autres contrôles de ce type, ni de contrôle SIS II (système d'information Schengen) et VIS (système central d'information sur les visas) coordonnés avec les autres cantons et le PFPDT.

Recommandations et suivi de l'évaluation Schengen 2018

Dans le cadre du suivi des recommandations émises par le Conseil de l'Union Européenne à l'égard de la Suisse lors de la troisième évaluation Schengen en 2018, la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) a pris contact avec les différents responsables des cantons pour la suite donnée.

Suite aux recommandations émises, l'Autorité a répondu que, selon le droit actuel, elle ne dispose pas de pouvoir décisionnel dans son domaine de compétence. Elle peut uniquement effectuer des enquêtes et rendre des recommandations à l'attention des organes publics qui ne respecteraient pas ou pas complètement leurs obligations en matière de protection des données et les inviter à remédier aux manquements constatés. La recommandation n'a cependant pas de caractère contraignant. Lorsque l'organe public refuse d'y donner suite, l'Autorité a néanmoins la possibilité de porter l'affaire en justice. Elle a précisé que la LPrD est en cours de révision totale. Cela étant, celle-ci ne devrait pas entrer en vigueur avant 2022. L'avant-projet de loi mentionne un renforcement de la position de l'Autorité en lui attribuant non seulement le pouvoir d'investigation, mais aussi d'intervention lui permettant d'ordonner, le cas échéant, que des mesures soient prises en cas de non-respect des prescriptions en matière de protection des données. Si la proposition de l'avant-projet est adoptée tel que proposé, la Commission de l'Autorité pourra prononcer des décisions contraignantes en matière de protection des données.

S'agissant des ressources adéquates, il est relevé que l'Autorité manque de ressources humaines pour s'acquitter des tâches confiées dans le cadre de l'acquis relatif au SIS II et au VIS. Malgré l'augmentation du taux d'activité de la préposée à la protection des données de 30% depuis avril 2020, l'Autorité manque de ressources humaines, notamment en informatique, pour s'acquitter de ses tâches. Les demandes de ressources supplémentaires en personnel (en informatique et spécialiste en protection des données) n'ont pas été octroyées. Toutefois, une augmentation des ressources financières pour les prestations de service a été accordée à l'Autorité. Finalement, l'Autorité s'est engagée à remédier, en collaboration avec le PFPDT, aux lacunes sur son site Internet.

3. FriPers et vidéosurveillance

3.1 FriPers

L'Etat de Fribourg exploite une plateforme centrale, FriPers, 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 départ ou d'arrivée, 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, d'émettre 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.

Contrôles

Le SPoMi, en tant que responsable des données FriPers procède, à intervalles réguliers, au contrôle des autorisations délivrées. Des contrôles plus poussés peuvent être faits en collaboration avec l'Autorité. Toutefois, pendant l'année sous revue, aucun contrôle de ce type n'a été réalisé. Dans le cadre des contrôles axés sur le respect des principes de protection des données effectués au sein de l'administration (cf. III. B. 2.), l'Autorité a, par la même occasion, vérifié le nombre de collaborateurs au bénéfice d'un accès et leur nécessité.

3.2 Vidéosurveillance

La préposée à la protection des données doit être informée au préalable lors de demandes d'installation de systèmes de vidéosurveillance 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 LVID).

Il ressort de plus en plus des différentes demandes d'installation de vidéosurveillance que les particuliers, les entreprises, 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.

L'Autorité a pris position sur divers projets de vidéosurveillance pendant l'année objet du rapport. La fréquence et la complexité des demandes ont nécessité la tenue de visions locales. Ces rencontres permettent un échange avec les différents spécialistes et les autorités ainsi qu'une meilleure compréhension de la situation. La collaboration avec les préfetures est bonne. Elles suivent généralement les préavis de l'Autorité.

Certaines prises de position de l'Autorité sont mises en ligne sur son site Internet. Enfin, il est rappelé que les préfetures publient régulièrement sur leur site Internet la liste des installations de vidéosurveillance au bénéfice d'une autorisation ainsi que le nom des personnes responsables de l'installation.

Dénonciations

Durant l'année sous rubrique, quelques dénonciations de système de vidéosurveillance filmant le domaine public, sans autorisation, ont été portées à la connaissance de l'Autorité. 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. A noter que certaines d'entre elles ont débouché sur le dépôt en bonne et due forme d'une demande d'autorisation d'installation d'un système de vidéosurveillance.

Installation de webcam sur un clocheton d'une collégiale

Une commune a annoncé à l'Autorité ainsi qu'à la préfeture concernée la mise en service d'une webcam sur le clocheton de la collégiale. Cette technologie est mise en place afin de pouvoir profiter de la vue panoramique, de sorte qu'elle n'entre pas dans le champ d'application de la LVID. Toutefois, la législation en matière de protection des données reste applicable. En présence d'une éventuelle identification des personnes filmées, un système de floutage, un cache, voire un changement de champ de vision doit être effectué. A tout le moins, la commune ainsi que la préfeture concernée doivent s'assurer que les principes de protection des données sont respectés.

Annonce d'un système de vidéosurveillance sans enregistrement.

La vidéosurveillance sans enregistrement nécessite l'information préalable par le responsable du système à la préposée à la protection des données et au préfet (art. 7 LVID et art. 7 OVID). Il sied de rappeler qu'avec ou sans enregistrement le but de la vidéosurveillance est le même, soit «de prévenir les atteintes aux personnes et aux biens et de contribuer à la poursuite et à la répression des infractions» (art. 3 al. 1 LVID). L'annonce ne prive pas le ou la requérant-e de fournir des informations quant au matériel envisagé ainsi que sa fonctionnalité. À tout le moins, la sécurité des données (notamment quand du matériel privé est utilisé) ainsi qu'une absence d'enregistrement doivent être attestées. À défaut, une demande avec enregistrement doit être déposée auprès de la préfeture concernée.

Surveillance d'un tronçon de route cantonale et/ou communale

La préposée a préavisé favorablement la demande d'installation d'un système de vidéosurveillance avec enregistrement pour prévenir des actes de vandalisme sur les barrières. Toutefois, afin de limiter l'atteinte aux droits de la personnalité, il a été rappelé que le consen-

tement des propriétaires des habitations avoisinantes susceptibles d'être régulièrement filmées étaient requis. Enfin, un cache doit être installé pour dissimuler les habitations privées qui entrent dans le champ de vision. Afin de faciliter les travaux d'entretien hivernal des routes, d'éviter aux employés des déplacements inutiles et surtout de devoir veiller toute la nuit, une commune souhaitait mettre en place une vidéosurveillance d'observation (c'est-à-dire sans enregistrement). Quand bien même il s'agit d'une vidéosurveillance sans enregistrement, l'article 3 alinéa 1 L_{Vid} doit être respecté. Partant, l'installation doit viser «à prévenir les atteintes aux personnes et aux biens et de contribuer à la poursuite et à la répression des infractions». Le but de la demande n'étant pas conforme, une détermination défavorable a été émise.

Surveillance par des privés

Des entreprises privées ont sollicité une autorisation à l'installation d'un système de vidéosurveillance avec et sans enregistrement filmant le domaine public (rue, route, espace public, entrée et sorties de parking, etc.). Dans le cadre de ces demandes, seul le domaine public filmé est préavisé, le domaine privé ne faisant pas l'objet d'une demande d'autorisation. Ces préavis rappellent chaque fois aux responsables de l'installation que si le système de vidéosurveillance filme des collaborateurs, voire des entreprises locataires de l'immeuble, ces derniers doivent être expressément informés de la pose des caméras, de leur champ de vision et de leurs droits y relatifs.

Déchetteries

L'année 2020 a enregistré une forte demande des communes pour l'installation d'un système de vidéosurveillance dans les déchetteries. Les risques fréquemment soulevés sont les dépôts de déchets sauvages dans l'enceinte de la déchetterie et plus particulièrement près des bennes (incivilités). La volonté est ainsi de contrôler l'utilisation conforme des biens communaux dans le respect des règlements communaux. La jurisprudence est claire à ce sujet. Le but tendant à l'«utilisation conforme aux instructions du matériel» est manifestement contraire à la L_{Vid} et ne peut être admis (cf. Arrêt TC FR 601 2014 46 du 20 août 2015, consid. 3a).

Par surabondance, la préposée recommande une grande retenue face au matériel utilisé notamment lorsqu'il s'agit de caméras achetées sur Internet avec un abon-

nement gratuit qui permettent d'héberger les enregistrements dans un *Cloud* et de visionner en direct les images. A noter que généralement les serveurs sont basés à l'étranger. En outre, le ou la requérant-e doit établir, au moment du dépôt de la demande (avec ou sans enregistrement), la sécurité du système, l'étendue et la gestion des accès aux images, la confidentialité, etc.

Recommandation et recours – suite

Pour rappel, la Commission a adressé une recommandation à une préfecture dans le cadre d'une autorisation d'installation d'un système de vidéosurveillance dans une école publique. Dans la mesure où le préfet n'est pas entré en matière, la Commission a déposé un recours auprès du Tribunal cantonal contre la décision préfectorale émise rejetant la recommandation de l'Autorité. Comme le préfet reconnaît que la cause n'a pas suffisamment été instruite, le Tribunal cantonal a pris acte qu'il annule implicitement la décision en vue de la remplacer par une autre, de sorte que la décision attaquée est annulée et la cause est rayée du rôle, le litige étant devenu sans objet.

Par la suite, une vision locale a été organisée par la préfecture en date du 17 octobre 2019. Le 14 janvier 2020, la préposée à la protection des données a communiqué son préavis partiellement favorable à la préfecture. Par courrier du 28 juillet 2020, la Préfecture a demandé à la préposée de se déterminer suite aux modifications opérées par la requérante ainsi qu'à la production des champs de vision finaux. La détermination a été communiquée le 8 octobre 2020 et une décision finale de la préfecture est parvenue à l'Autorité en date du 14 octobre 2020.

4. ReFi – registre des fichiers¹⁵

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'Autorité¹⁶.

Des adaptations techniques de l'application sont nécessaires pour une utilisation adéquate du ReFi. Toutefois, avant de pouvoir entamer les travaux, l'Autorité est dans l'attente de la mouture définitive de la loi cantonale sur la protection des données, dans la mesure où cette dernière fixe le cadre.

5. Echanges

5.1 Collaborations

La préposée à la protection des données met une importance toute particulière à collaborer avec le PFPDT et avec les autorités en la matière dans les autres cantons. Ces collaborations prennent différentes formes.

Privatim

Comme les autres autorités cantonales, la préposée à la protection des données fait partie de la *Conférence des commissaires suisses à la protection des données, privatim*¹⁷. En 2020, l'Autorité a pu également profiter des travaux effectués par *privatim* sur des questions générales d'importance internationale, nationale et intercantonale. Cette collaboration est très utile, voire indispensable, pour échanger des informations, des expériences et coopérer sur des projets communs. Dans le cadre de certaines négociations contractuelles, *privatim* a un plus grand poids pour négocier les garanties de base en matière de protection des données que chaque

canton individuellement. De nombreux échanges ont lieu concernant l'utilisation de Microsoft Office 365 dans l'administration mais également dans le cadre scolaire. A cet égard, *privatim* associée à la CSI (Conférence suisse informatique) sont en discussion avec les représentants de Microsoft SA concernant les différents points contractuels qui rendent difficiles l'utilisation des services en ligne de Microsoft Office 365 dans l'administration.

En 2020, *privatim* a fêté ses 20 ans. Toutefois, les festivités ont été repoussées à deux reprises au vu de la situation sanitaire. L'assemblée générale du printemps et celle d'automne ont eu lieu par voie circulaire.

La préposée à la protection des données a collaboré activement dans différents groupes de travail spécifiques, notamment concernant des dossiers communs. Ces échanges ont eu lieu dans le domaine de la santé (dossier électronique du patient, traçage, etc.) et de la digitalisation de l'administration (eDéménagement, Microsoft Office 365, etc.).

Par ailleurs, *privatim* a organisé pour ses membres et ses collaborateurs une séance de formation continue et a publié une Check-list concernant le déchiffrement de connexions web encryptées. Dans le cadre de la pandémie, *privatim* a établi une analyse sous forme de liste des diverses applications de visio- et vidéoconférence. Enfin, elle a transmis ses prises de position concernant divers projets de législation fédérale.

Groupe des préposés latins à la protection des données

En général deux fois par an, le Groupe des préposés latins à la protection des données se réunit, permettant aux préposés de Suisse romande ainsi qu'à l'adjoint du PFPDT de discuter des thèmes actuels et d'échanger leurs expériences en détail. En 2020, la réunion printanière a eu lieu en Valais, alors que celle d'automne prévue à Fribourg s'est déroulée par visioconférence. En outre, la préposée à la protection des données a eu plusieurs échanges spécifiques concernant des dossiers communs, à savoir des thématiques d'envergure nationale dont les prestataires, fournisseurs ou mandataires sont les mêmes dans les différents cantons.

¹⁵ <https://www.fr.ch/atprd/institutions-et-droits-politiques/transparence-et-protection-des-donnees/registre-des-fichiers-refi>

¹⁶ <http://appl.fr.ch/refi/etat/client/index.aspx>

¹⁷ <https://www.privatim.ch/fr/>

Groupe de coordination Schengen des autorités suisses de protection des données

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 1^{er} 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, n'a pas pu se réunir cette année, au vu de la situation particulière. Toutefois, des échanges électroniques ont eu lieu.

Personnes de contact au sein de l'administration fribourgeoise

Au vu de la situation sanitaire, la préposée à la protection des données s'est vue dans l'obligation de repousser à plusieurs reprises la rencontre avec les personnes de contact (personnes répondantes en matière de protection des données dans chaque direction et établissement autonome). Toutefois, de manière ponctuelle, elle a pris contact avec certaines d'entre elles pour des échanges d'informations et de points de vue. En outre, des renseignements leur sont fournis sur différents thèmes par le biais notamment des newsletters, d'actualités ou d'autres invitations à des manifestations.

Collaboration interne à l'Autorité

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.

5.2 Formations et sensibilisations

Formation continue de l'Etat de Fribourg

A l'occasion des formations continues proposées par l'Etat de Fribourg, la préposée a donné un cours à la HEG. Cette formation se veut interactive, permettant ainsi aux participants de l'administration publique d'échanger plus spécifiquement dans leur domaine. En effet, ces derniers font parvenir à la préposée, de manière préalable, les questions relatives à leur domaine, facilitant ainsi les points à mettre en exergue.

Cours interentreprises AFOCI

Dans le cadre des cours interentreprises AFOCI comprenant tous les stagiaires 3+1 et les apprentis de l'Etat de Fribourg, la formation administration publique «Protection des données, droit de l'information et archivage» a uniquement été dispensée en français. Ces cours permettent aux stagiaires 3+1 ainsi qu'aux apprentis d'être sensibilisés aux questions relatives à ces trois domaines qui s'interconnectent.

Formation pour les délégués sectoriels à la protection des données

Dans le cadre de la mise en œuvre du Référentiel cantonal (base de données communes à plusieurs applications et/ou systèmes d'information contenant des données de personnes, organisations et nomenclature)¹⁸, la préposée à la protection des données a dispensé une formation de base aux différents intervenants concernés par ce projet. Cette formation a eu lieu sous la forme de modules et a traité des thèmes suivants: l'introduction à la protection des données, la législation relative à la protection des données – responsabilité de l'organe de traitement –, les nouveautés de la loi fédérale sur la protection des données, la sécurité de l'information et de l'informatique, les tâches et les outils des délégués sectoriels à la protection des données dans l'administration publique.

En 2020, 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 le Secrétariat général de la DICS, le SPO et le centre de compétences Fritic.

¹⁸ <https://www.fr.ch/vie-quotidienne/demarches-et-documents/le-referentiel-cantonal>

5.3 Travaux divers

Feuilles informatives

L'Autorité a actualisé le guide pratique à l'attention des communes en français. En outre, l'Autorité publie régulièrement des actualités en lien avec la protection des données.

6. Statistiques

Protection des données en général

Durant la période considérée, 425 dossiers en matière de protection des données (sans les demandes Fri-Pers et vidéosurveillance, voir ci-dessous) ont été introduits, dont 86 sont pendants au 1^{er} janvier 2021. Ces dossiers comprennent 123 conseils et renseignements, 86 avis, 30 examens de dispositions législatives, 41 communications de décisions (art. 27 al. 2 LPrD), 9 contrôles et inspections ou suivis de contrôle, 9 présentations, 70 participations à des séances et autres manifestations et 57 demandes diverses. 218 dossiers concernent des organes cantonaux ou des institutions chargées de tâches publiques, 49 des communes, 93 d'autres organismes publics (cantons, autorités de protection des données), 49 des particuliers ou des institutions privées et 6 des médias (cf. statistiques annexées). Pour les dossiers pendants des années précédentes, 79 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 2020, 3 demandes ont été soumises à la préposée à la protection des données pour préavis: 1 demande d'accès, 1 détermination et 1 modification de préavis. De ces requêtes, la demande d'accès est toujours en traitement, les 2 autres demandes étant closes. La collaboration avec la DSJ est bonne, cette dernière suivant généralement les préavis de l'Autorité. L'évolution des technologies permet de développer les modes d'utilisation de la plateforme Fri-Pers. Partant, 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 2020, la préposée à la protection des données a reçu 12 demandes d'installation de vidéosurveillance avec enregistrement pour préavis, 6 annonces d'installation de vidéosurveillance sans enregistrement, 1 demande d'étude préliminaire d'une installation de vidéosurveillance. Elle a dû se déterminer à 3 reprises dans des cas de dénonciations d'installations sans autorisation, à 1 reprise suite à une vision locale et à 1 autre suite à un préavis défavorable. Des requêtes avec enregistrement, 1 préavis partiellement positif avec des conditions, 1 préavis provisoire, 5 préavis défavorables ont été émis alors que les 5 restantes sont encore en cours de traitement. Certains préavis positifs peuvent être assortis de conditions, notamment de satisfaire à l'exigence de signalisation des systèmes de vidéosurveillance. Par ailleurs, 19 dossiers émanaient des services de l'Etat ou de communes, et 5 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 2020. 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

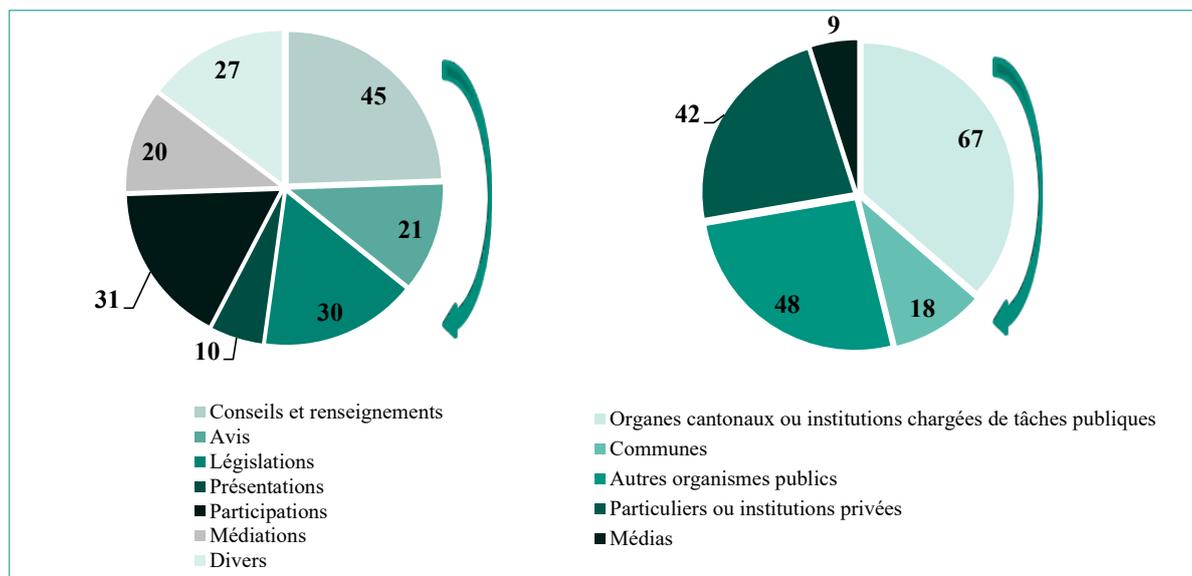
L'Autorité cantonale de la transparence et de la protection des données **remercie** tous les organes publics pour la collaboration développée jusqu'ici, pour l'intérêt manifesté envers le droit d'accès à l'information ainsi qu'envers leur obligation de respecter les dispositions légales sur la protection 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.

Table des abréviations et termes utilisés

AFOCI	Association fribourgeoise pour l'organisation des cours interentreprises
AP	Avant-projet
ATPrD	Autorité cantonale de la transparence et de la protection des données
AVS	Assurance-vieillesse et survivants
BCU	Bibliothèque cantonale universitaire
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CICI	Conférence internationale des commissaires à l'information
CoPil	Comité de pilotage
CPJA	Code de procédure et de juridiction administrative du 23 mai 1991
DAEC	Direction de l'aménagement, de l'environnement et des constructions
DEP	Dossier électronique du patient
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
EDU	Education
EPT	Equivalent plein temps
FriPers	Plateforme informatique cantonale du contrôle des habitants
Fritic	Centre de compétences
HAE	Harmonisation des administrations des écoles
HEG	Haute école de gestion
LGCyb	Loi du 2 novembre 2016 sur le guichet de cyberadministration de l'Etat
LICD	Loi du 6 juin 2000 sur les impôts cantonaux directs
LInf	Loi du 9 septembre 2009 sur l'information et l'accès aux documents
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
OAD	Ordonnance du 14 décembre 2010 sur l'accès aux documents
OVID	Ordonnance du 23 août 2011 sur la vidéosurveillance
PF PDT	Préposé fédéral à la protection des données et à la transparence
Privatim	Conférence des Préposé(e)s suisses à la protection des données
ReFi	Registre des fichiers
RHT	Réduction de l'horaire de travail
SIPD	Sûreté de l'information et protection des données
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
VIS	Système central d'information sur les visas
UE	Union européenne

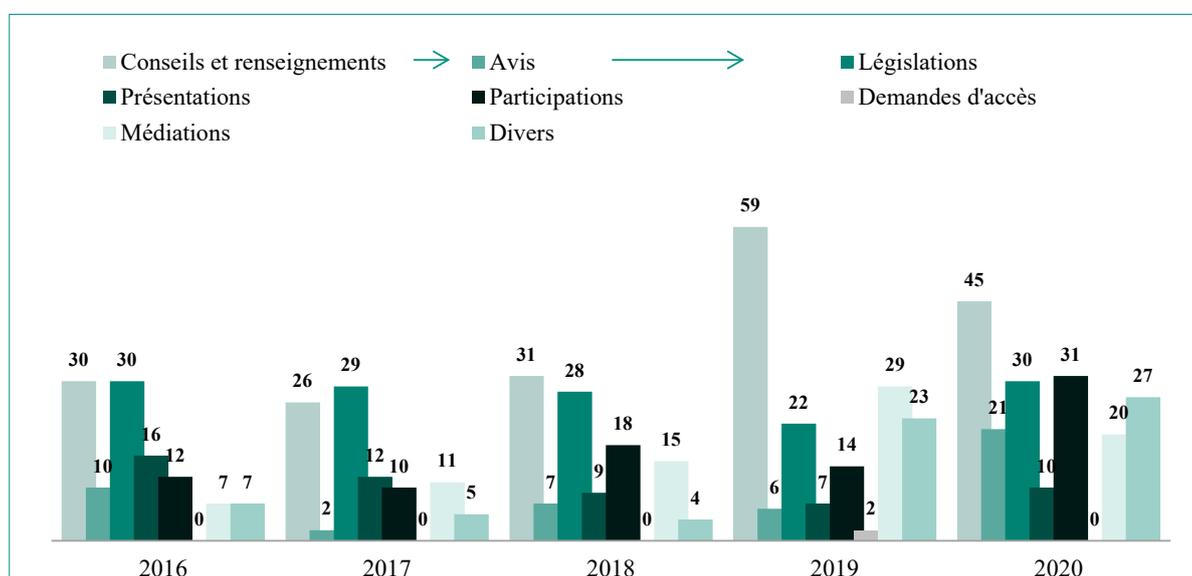
Statistiques de la transparence

Demandes / interventions en 2020



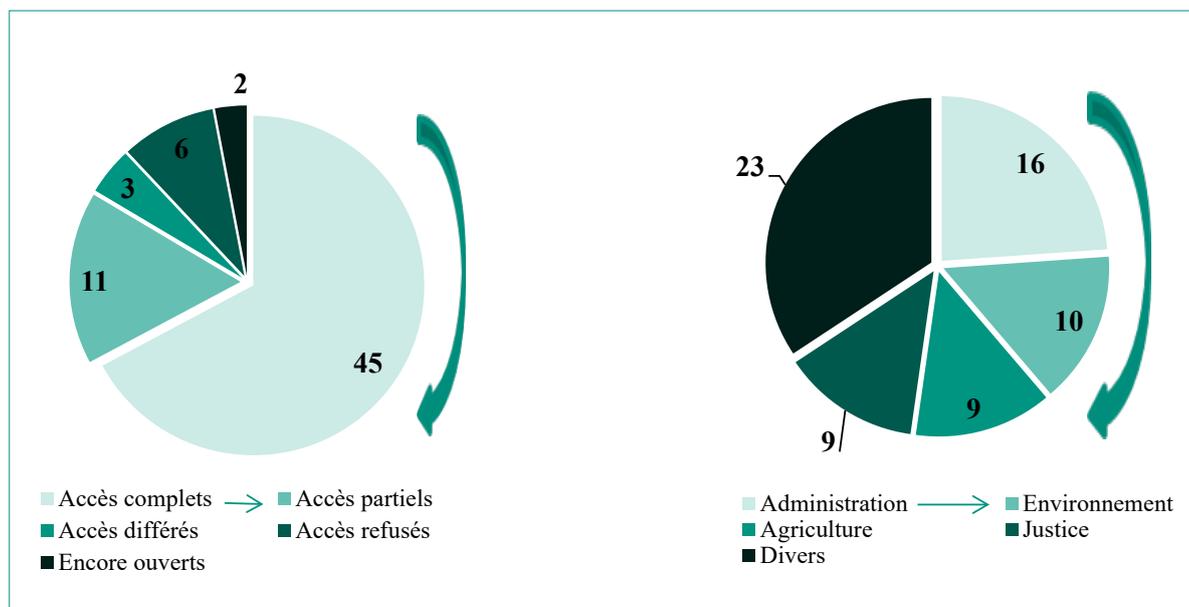
- > Les «conseils et renseignements» sont donnés par la préposée à la transparence.
- > Le terme «législations» comprend les travaux de réflexion sur des dispositions législatives et les réponses aux consultations.
- > La notion de « présentations » recouvre par ex. les exposés dans le cadre de la présentation 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 184 dossiers ouverts en 2020, 68 dossiers sont communs avec ceux de la protection des données, dont 30 consultations.

Comparatif



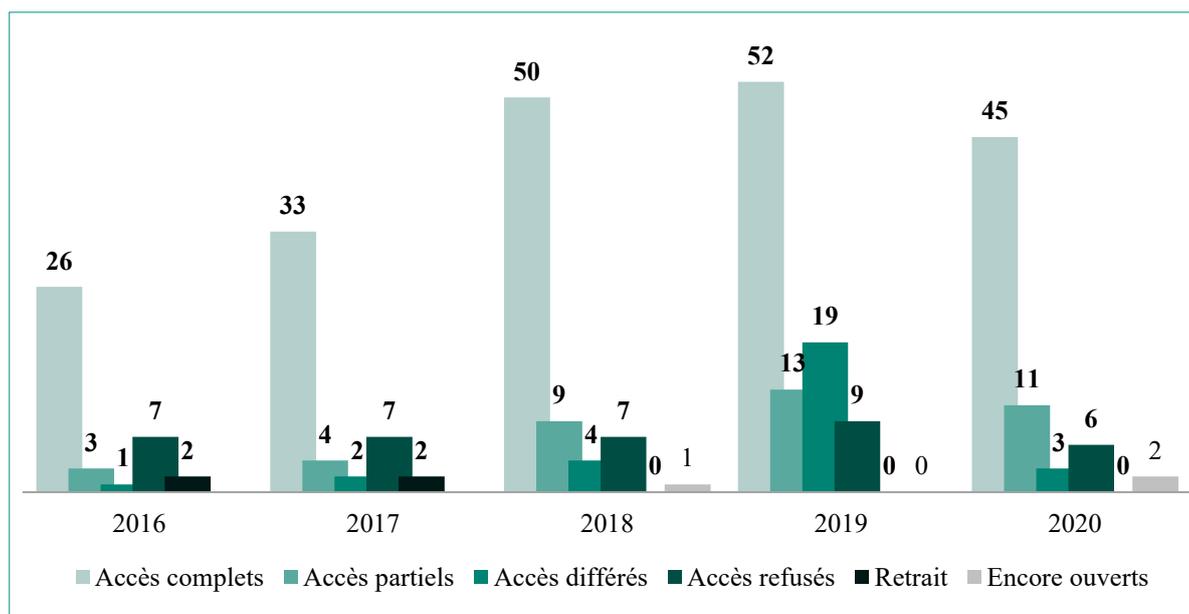
Evaluation du droit d'accès en 2020

—



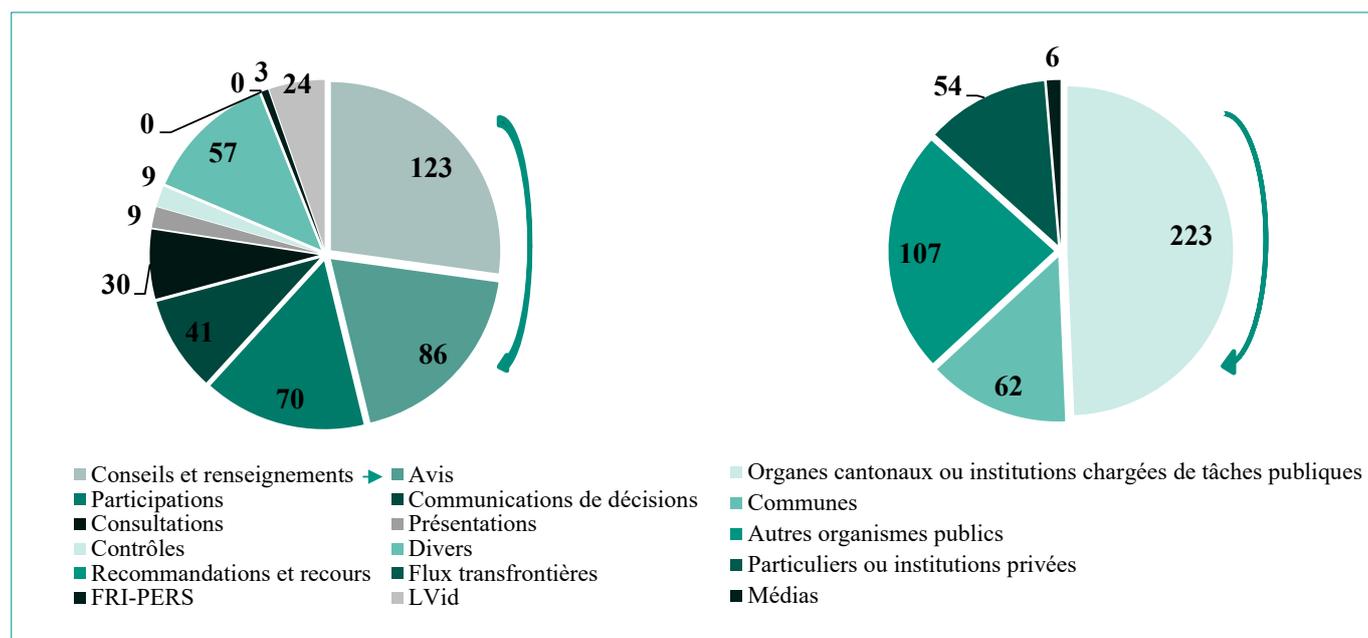
Comparatif

—



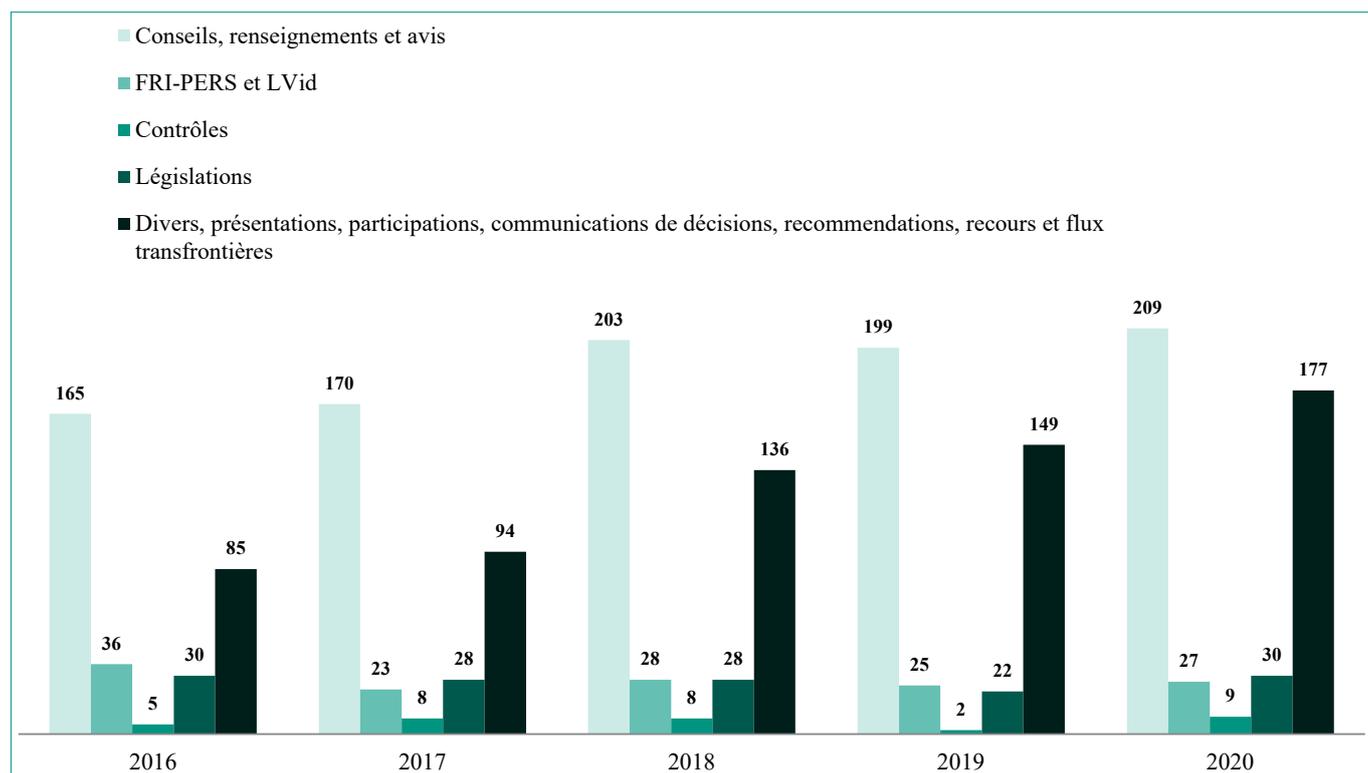
Statistiques de la protection des données, FRI-PERS et LViD

Demandes / interventions en 2020



- > 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 452 dossiers ouverts en 2020, 68 dossiers sont communs avec ceux de la transparence, dont 30 consultations.

Comparatif



Demandes / interventions

Années	Avis	Conseils et renseignements	Contrôles	Législations	Présentations	Participations	Communications de décisions	Recommandations et recours	Flux transfrontières	FRI-PERS	L'Vid	Divers	Total
2020	86	123	9	30	9	70	41	0	0	3	24	57	452
2019	61	138	2	22	9	46	35	2	0	12	13	57	397
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