ETAT DE FRIBOURG
STAAT FREIBURG

Service de législation SLeg
Amt für Gesetzgebung GeGA

Grand-Rue 26, Case postale, 1701 Fribourg

T +41 26 305 14 45, F +41 26 305 14 08
www.fr.ch/sleg

Courriel: servicedelegislation@fr.ch

Fribourg, le 28 avril 2021

Avis de droit

Déploiement de Microsoft Office 365 auprès de l'Autorité de la transparence et de la protection des données

(n/réf.: EDS2021_053)

Le présent avis de droit a été rédigé à la demande de la délégation du Conseil d'État pour la digitalisation et les systèmes d'information. Il fait suite à un courrier de l'ATPrD concernant le déploiement de Microsoft Office 365 en son sein. Dans ce courrier, l'ATPrD conditionne l'installation de Microsoft Office 365 au respect de 7 recommandations/exigences. Parmi ces recommandations/exigences, certaines d'entre elles correspondent au droit en vigueur, tandis que d'autres vont sensiblement plus loin que ce que la loi prévoit. L'avis analyse si et dans quelle mesure l'ATPrD est habilitée à former ses propres exigences face à un traitement de données d'abord en tant qu'autorité responsable du traitement des données et ensuite en tant qu'autorité chargée de la surveillance des données.

1. En fait

1.1. Le 4 décembre 2018, le Conseil d'État a adopté **une ordonnance autorisant le Service de l'informatique et des télécommunications (ci-après le SITel) à externaliser à titre de projet pilote le traitement de certaines données dans le « cloud »** (RSF 184.15). Conformément à cette ordonnance, les outils bureautiques collaboratifs de **Microsoft Office 365** ont, dans un premier temps, été testés sur un périmètre limité dans le but d'en explorer les possibilités techniques ainsi que les mesures de sécurité à mettre en place.

1.2. Le 27 novembre 2019, le SITel a remis au Conseil d'État un rapport d'évaluation concluant au succès du projet pilote *cloud* concernant Microsoft Office 365 et recommandant **son déploiement auprès de l'ensemble des unités administratives de l'État**. Suivant cette recommandation, le Conseil d'État **a demandé l'élaboration d'un projet de loi** destiné à créer les bases légales nécessaires à l'utilisation du *cloud* au sein de l'administration cantonales et des communes fribourgeoises.

1.3. Dans le courant de l'année 2020, **la pandémie de coronavirus** est apparue avec pour conséquence que **le télétravail** a d'abord été recommandé puis rendu obligatoire pour un grand nombre d'empoyé-e-s de l'État, de même que **l'enseignement à distance** pour les collégien-ne-s et pour les étudiant-e-s de l'Université et des Hautes Écoles.

1.4. Face à cette situation, le Conseil d'État a décidé **d'anticiper l'adoption des bases légales** concernant le recours au *cloud* afin d'assurer la poursuite des activités de l'État comme de l'enseignement, mais à distance. Par plusieurs arrêtés et décisions, il **a chargé le SITel** d'assurer la disponibilité des prestations informatiques de l'État durant la crise et de déployer auprès des organes de l'administration des outils numériques de communication unifiée (ACE n° 2020-251 du 23 mars 2020 concernant la disponibilités des prestations informatiques de l'Etat dans le cadre de la gestion de crise ; Décision du CE autorisant la mise en production de Microsoft Office 365 pour l'éducation ; ACE n° 2020-272 concernant le déploiement de la vidéoconférence en appui du télétravail dans le contexte de la crise COVID-19 ; ACE 2020-481 concernant le bilan et les modalités de retour à une situation normale des prestations informatiques de l'État suite à la pandémie de coronavirus du 16 juin 2020).

1.5. Le 18 décembre 2020, le Grand Conseil fribourgeois **a adopté la loi adaptant la législation cantonale à certains aspects de la digitalisation** (ROF 2020_195). Selon le Message du Conseil d'État, un des objectifs principaux de cette loi était de poser les bases légales permettant **le passage en phase de production** des projets pilotes menés par l'État en matière d'informatique en nuage et ainsi de permettre leur déploiement à plus large échelle (cf. Message 2019-CE-239 du 21 avril 2020 accompagnant le projet de loi adaptant la législation cantonale à certains aspects de la digitalisation, p. 1).

1.6. La loi adaptant la législation cantonale à certains aspects de la digitalisation est entrée en vigueur le 1er mars 2021. L'adoption de cette loi a entraîné une modification de la loi du 25 novembre 1994 sur la protection des données (LPrD ; RSF 17.1). Cette dernière a, en particulier, été complétée par **les articles 12b à 12e**. Selon l'article 12b al. 1, le traitement de données personnelles, y compris de données sensibles, **peut être externalisé** aux conditions posées par les dispositions précitées. S'ensuit une série de règles fixant les conditions auxquelles le traitement de données personnelles peut être externalisé dans le « cloud ». Des règles similaires ont été introduites simultanément aux articles 27 à 30 de la loi du 18 décembre 2020 sur la cyberadministration (LCyb ; RSF 184.1 / anciennement la loi du 2 novembre 2016 sur le guichet de cyberadministration de l'État) concernant l'externalisation de données non-personnelles.

1.7. Dans un courrier du 26 février 2021, le SITel a informé l'Autorité de la transparence et de la protection des données (ci-après : l'ATPrD) de **son intention de déployer** Microsoft Office 365 au sein de l'Autorité et **de remplacer la plateforme iExtranet** par la solution MS-Teams.

1.8. Selon les informations qui nous ont été confirmées par le SITel, ce changement implique un traitement de données dans **un *cloud* géré par Microsoft** des données relatives à la communication unifiée (visioconférence, téléphonie, messages texte) à partir de **MS-Teams**, des données créées et échangées au moyen de la messagerie **Microsoft Outlook**, des **données d'authentification des utilisateurs et des utilisatrices**, et des données sauvegardées dans **OneDrive**. Ne sont en revanche pas concernées les données créées à partir des outils **Word, Excel, PowerPoint et OneNote** aussi longtemps qu'elles ne sont pas sauvegardées par l'utilisateur ou l'utilisatrice dans **OneDrive**.

1.9. Toujours selon le SITel, les lieux de traitements (*clouds*) sont situés **en tout temps sur le territoire suisse ou d'un État garantissant un niveau de protection des données équivalent** au sens de l'article 12b al. 2 LPrD et les données hébergées dans le cloud **sont chiffrées**.

1.10. Par réponse du 25 mars 2021, l'Autorité de la transparence et de la protection des données (ci-après l'ATPrD) a formulé, en sa qualité de responsable du traitement et afin de garantir la sécurité et

la protection des données qu'elle traite, **sept « recommandations »** concernant le déploiement en son sein de Microsoft Office 365.

1.11. Les sept recommandations portaient sur les points suivants :

1. Toutes données, documents, traitements de données (courriels, dossiers, échanges téléphoniques, documents, etc.) effectués par l'Autorité **sont traités, stockés et hébergés sur des serveurs sécurisés en Suisse** ;
2. Le transfert et l'hébergement des traitements de données **sont chiffrés**. Les clés de chiffrement **sont en main du SITel**. Le cas échéant, le SITel s'engage à mettre en place des mesures techniques supplémentaires (tels que chiffrement du contenu et pseudonymisation des utilisateurs par l'organe) ;
3. Tout sous-traitant est désigné avec **l'accord écrit du SITel** qui s'est assuré que le sous-traitant **est en mesure de garantir la sécurité des données**. L'Autorité doit être **informée de manière préalable** à l'accord. Le traitement des données est effectué uniquement par des sous-traitants venant de pays ayant un niveau de protection des données suffisant (selon liste du PFPDT et LPrD 12ss) ;
4. Les personnes autorisées à traiter les données personnelles sont soumises **au respect de la confidentialité et du secret de fonction**. Les données ne sont pas accessibles par des personnes non-autorisées ;
5. Les contrats y relatifs mentionnent **le for et le droit applicable en Suisse**, **l'interdiction de toute activité commerciale** avec les données de l'Autorité, l'information immédiate de l'Autorité en cas de **demande d'autorités étrangères et de failles de sécurité** ;
6. La gestion des comptes utilisateurs et des droits d'accès informatique au sein de l'Autorité **est effectué par l'Autorité elle-même**.
7. La Commission dispose **d'une plateforme sécurisée**, dont les données et documents sont stockés et hébergés sur un serveur sécurisé du SITel et accessible par des personnes hors périmètre de l'État [*recte* : non-accessible ?].

1.12. L'ATPrD a fixé au SITel un délai au 31 mars 2021 pour qu'il lui confirme la mise en place des garanties précitées ou qu'il lui précise, le cas échéant, lesquelles d'entre elles ne peuvent pas être appliquées et quelles solutions alternatives sont prévues.

1.13. Parallèlement, la Préposée à la protection des données a formulé **des exigences semblables** auprès d'une Direction de l'État. Elle a indiqué à la DICS qu'en cas d'externalisation de données sensibles, ces données doivent être chiffrées et les clés de déchiffrage être uniquement en main de l'État, que les données doivent être stockées dans un *cloud* privé et que le for juridique et le droit applicables doivent être suisses. Elle a aussi indiqué que la responsabilité en matière de traitement de données lors d'une externalisation ne serait pas partageable (cf. courriel du 21 janvier 2021 de Mme Florence Henguely à M. Michel Perriard).

1.14 Par courriel du 31 mars 2021, la délégation du Conseil d'État pour la digitalisation et les systèmes d'information a demandé au Service de législation d'analyser sur la base des dispositions en vigueur si l'ATPrD est en droit de formuler ses propres exigences en matière de *cloud*, que ce soit en tant qu'unité administrative ou en tant qu'autorité chargée de la surveillance du traitement des données.

2. En droit

2.1. Sur la nature du courrier de l'ATPrD du 25 mars 2021

2.1.1. Dans son courrier du 25 mars 2021, l'ATPrD indique agir en qualité de « **responsable de traitement** ». À ce titre, elle déclare émettre un certain nombre de **recommandations/exigences** concernant le traitement de ses propres données.

2.1.2. L'emploi du terme recommandation peut faire penser à l'instrument prévu à l'article **22a LPrD** qui traite la question de **la procédure en cas de non-respect des prescriptions de protection des données**. Dans ce cas, l'Autorité peut émettre à l'attention du responsable du traitement une « recommandation » par laquelle elle l'invite à prendre les mesures nécessaires pour remédier à la situation (al. 1). Lorsque l'organe concerné est une unité subordonnée, l'invitation est directement adressée à l'organe hiérarchiquement supérieur (al. 2). Celui-ci doit alors adopter dans le délai imparti par l'Autorité une décision sur la suite qu'il entend donner à la recommandation. En cas de rejet total ou partiel de la recommandation, l'Autorité **peut recourir** contre cette décision au Tribunal cantonal (al. 4).

2.1.3. En l'espèce, le courrier du 25 mars 2021 ne présente à l'évidence **pas les caractéristiques** d'une recommandation au sens de l'article 22a LPrD. D'une part, il a été adressé directement au SITel et non à la Direction des finances comme le prévoit l'article 22a al. 2 LPrD ; d'autre part le terme recommandation ne figure pas sur l'entête du courrier mais apparaît uniquement une seule fois en page 2 du document sans être mis en évidence d'aucune manière ; enfin, l'ATPrD précise que les recommandations contenues dans son courrier sont formulées **en sa qualité de responsable du traitement** (et non d'autorité).

2.1.4. Au vu de ce qui précède, le courrier de l'ATPrD du 25 mars 2021 doit être compris comme **une simple demande de l'ATPrD**. La question de savoir si elle **précède une future recommandation** au sens de l'article 22a LPrD peut demeurer ouverte.

2.2. Sur la légalité des exigences et des recommandations formées par l'ATPrD en tant qu'unité administrative

2.2.1. L'ATPrD déclare que les recommandations contenues dans son courrier du 25 mars 2021 sont formulées en sa qualité de « **responsable du traitement** ».

2.2.2. À l'heure actuelle, la notion de responsable du traitement est **inconnue de la LPrD**. Le terme en vigueur est celui de **responsable du fichier,** par quoi on entend « l'organe public qui décide du but et du contenu du fichier » (cf. art. 3 al. 1 let. g LPrD). Une interprétation littérale de cette disposition pourrait ainsi exclure que le responsable du fichier assume la responsabilité **des moyens du traitement** de données personnelles et donc aussi de leur choix. En vertu de l'ordonnance sur la gestion de l'informatique et des télécommunications dans l'administration cantonale (RSF 122.96.11), cette compétence **revient, en effet, principalement au SITel** en sa qualité de service en charge de l'informatique et des télécommunications au sein de l'État (cf. art. 5, al. 1 let. b, e, g, i, j).

2.2.3. Il est toutefois admis que la notion de responsable du fichier, qui date de 1994, est aujourd'hui **dépassée,** et qu'elle doit être comprise dans le sens plus large de « responsable du traitement ». Selon une définition admise unanimement, il s'agit « de la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, **seul-e ou conjointement avec d'autres**, détermine **les finalités et les moyens du traitement** de données personnelles » (cf. article 5 let. j de la loi fédérale sur la protection des données révisée du 25 septembre 2020 ; art. 4 ch. 7 du règlement (UE)

2016/679 sur la protection des données [RGPD] ; voir également l'art. 4 let. g de l'avant-projet du 27 novembre 2019 de révision totale de la LPrD).

2.2.4. Pareille définition tient compte de **la complexité croissante** de l'environnement dans lequel les technologies de l'information et de la communication sont utilisées, et en particulier d'une tendance de plus en plus nette, tant dans le secteur privé que dans le secteur public, **à la différenciation organisationnelle** (cf. ARTICLE 29, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »*, p. 6 et 19). Dans les structures d'une certaine taille, il est en effet d'usage que les responsabilités du traitement **soient réparties** entre l'entité qui détient les données et qui les traite de manière directe à raison de la matière (*Data Owner*) et l'entité qui fournit les infrastructures et les applications nécessaires à l'exécution des traitements mis en œuvre (*System /Application Owner*).

2.2.5. Dans ce cas, le *System/application Owner* n'a généralement pas le statut de sous-traitant par rapport au *Data owner* mais celui de **co-responsable du traitement** (*Joint Controller*). Le statut de co-responsable du traitement revenant au SITel est par ailleurs **expressément admis** par l'ATPrD à deux reprises dans son courrier du 25 mars. Une fois lorsqu'elle formule l'exigence que toute sous-traitance ne peut avoir lieu **qu'avec l'accord écrit du SITel** (cf. art. 12c al. 1 let. b ch. 5 LPrD). Une deuxième fois, lorsqu'elle déclare : « *Il est bien entendu relevé que le SITel* ***est responsable*** *de la sécurité informatique, mais également des applications informatiques (Application owner)* ».

2.2.6. La qualification de co-responsable du traitement reconnue au SITel ressort également indirectement de **la définition du sous-traitant** introduite dans le cadre de l'adoption de la loi du 18 décembre 2020 adaptant la législation cantonale à certains aspects de la digitalisation (ROF 2020_195). En vertu de l'article 3 al. 1 let. i nouveau, le sous-traitant ne peut, en effet, être qu'une personne privée ou un organe public **relevant d'une autre collectivité**.

2.2.7. Le Message du Conseil d'État révèle qu'il s'agit d'un **choix délibéré**. « *À l'intérieur d'une même collectivité, le fait de confier le traitement de données ou la gestion d'outils informatiques à un service central, comme c'est le cas, par exemple, du SITel, n'est* […] *pas considéré comme un cas de sous-traitance* » (cf. Message 2019-CE-239 du 21 avril 2020 accompagnant le projet de loi adaptant la législation cantonale à certains aspects de la digitalisation, p. 7).

2.2.8. Signe de son importance dans ce domaine, l'existence d'une responsabilité conjointe entre le responsable du traitement à raison de la matière et le SITel a ensuite été **rappelée et précisée** une deuxième fois par le législateur par rapport à la question spécifique de **l'externalisation du traitement de données**. Selon l'article 12 al. 3 LPrD, la responsabilité de la mise en œuvre et du suivi des règles édictées dans ce domaine est assumée **conjointement** par l'organe compétent à raison de la matière et par le service en charge de l'informatique.

2.2.9. L'article 12c al. 2 LPrD réserve en outre le cas particulier où une solution de *cloud computing* concerne **plusieurs organes différents** au sein d'une même collectivité publique. Dans pareil cas, un organe **principalement responsable** doit être désigné. Selon le Message du Conseil d'État, l'organe principalement responsable est, en particulier, « l'interlocuteur principal » du fournisseur de service au sein de l'État (cf. Message précité, p. 11). C'est à lui que revient en particulier la charge **de négocier et de passer** les contrats d'externalisations qui serviront de base au traitement des données des organes concernés.

2.2.10. Même si la loi ne le précise pas expressément, l'autorité compétente pour décider d'une externalisation concernant plusieurs organes différents et pour désigner l'organe principalement

compétent se détermine conformément aux **règles générales en matière de gestion et d'organisation de l'administration** prévues dans la loi du 16 octobre 2001 sur l'organisation du Conseil d'État et de l'administration (LOCEA ; RSF 122.0.1).

2.2.11. En vertu de l'article 6 al. 2 LOCEA, le Conseil d'État accomplit lui-même les actes d'administration qui, **en raison de leur importance ou de par la législation**, ne peuvent être attribués ni délégués à une autre autorité. Quant aux Directions, l'article 45 al. 2 LOCEA énonce qu'elles règlent les affaires qui leur ressortissent en vertu de la législation et celles que le Conseil d'État les charge de traiter.

2.2.12. Sur la base de ces règles, on en déduit qu'en principe la décision de procéder à une externalisation concernant les données traitées par **l'ensemble des organes de l'État dans une matière transversale** relève des compétences **du Conseil d'État**, tandis que la décision de procéder à une externalisation concernant **plusieurs organes au sein d'une même Direction ou qui concerne une matière propre à une Direction** relève des compétences de **la Direction concernée**. S'il juge le sujet suffisamment important, le Conseil d'État, en tant qu'organe directorial suprême, conserve néanmoins la possibilité **de se réapproprier** une matière ou, à l'inverse, **charger une Direction** de traiter un sujet qui lui revient. Les dispositions qui attribueraient dans un domaine particulier une compétence à un organe spécifique restent réservées.

2.2.13. L'introduction d'une responsabilité conjointe par rapport au déroulement du traitement des données **ne signifie pas** que chaque co-responsable du traitement **assume l'entier** de la responsabilité sur l'ensemble des opérations de traitement effectuées ni, non plus, que chaque responsable du traitement **doive prendre part à l'ensemble des décisions** relatives au traitement des données.

2.2.14. Selon la doctrine en Suisse, **une coopération basée sur la division du travail est suffisante** (**«** *Nicht erforderlich ist, dass alle Entscheide gemeinsam gefällt werden; ein arbeitsteiliges Zusammenwirken genügt.* ») (cf. ROSENTHAL David, *Das neue Datenschutzgesetz*, in : Jusletter 16 novembre 2020, n° 13 ; ég. WEBER Rolf H., *Outsourcing von Informatikdienstleistungen in der Verwaltung*, in ZBI 1999, p. 119 ; *contra* : BAERISWYL Bruno, in : Stämpflis Handkommentar zum Datenschutzgesetz, ad art. 10a LPD, n° 11). La répartition des responsabilités peut également **résulter de la loi elle-même,** laquelle peut assigner certaines responsabilités à certains organes spécifiquement (cf. CONTRÔLEUR EUROPÉEN À LA PROTECTION DES DONNÉES, *projet de Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, version 1.0 du 2 septembre 2020, § 21). Dans ce cas, il faut toutefois bien évidemment qu'il existe une relation de fait effective entre le responsable désigné dans la loi et le traitement de données visé.

2.2.15. À titre d'illustration, la jurisprudence de la Cour de justice de l'Union européenne (ci-après : la CJUE) révèle que la notion de responsables conjoints du traitement de données est large et qu'elle couvre **de nombreux cas de figure** :

- Dans son arrêt *Témoins de Jéhovah*, la CJUE a jugé que la communauté des témoins de Jéhovah était responsable conjoint avec ses membres prédicateurs des traitements de données personnelles liés au porte à porte qu'ils réalisent. Car même si ses prédicateurs peuvent décider d'eux-mêmes de procéder au traitement des données à caractère personnel dans le cadre de leur porte à porte, la communauté des témoins de Jéhovah est aussi à l'origine de ces traitements qu'elle **encourage et coordonne** (CJUE [Grande chambre], 10.7.2018, affaire C_25/17, *Témoins de Jéhova*, § 63 ss).
- Dans son arrêt *Wirtschaftsakademie*, la CJUE a jugé que l'administrateur d'une page fan Facebook n'est pas un simple utilisateur de ce réseau social, mais un responsable conjoint avec Facebook du

traitement par ce réseau des données personnelles de ses visiteurs. Car celui-ci participe, **par son action de paramétrage**, en fonction, notamment, de son audience cible ainsi que d'objectifs de gestion ou de promotion de ses activités, à la détermination **des finalités et des moyens du traitement** des données personnelles des visiteurs de sa page fan CJUE [Grande Chambre], 5.6.2018, affaire C-210/2016, *Wirtschaftsakademie Schleswig-Holstein GmbH c. Facebook Ireland Ltd*, § 25 ss).

- Dans son arrêt *Fashion ID*, la CJUE a jugé que le gestionnaire d'un site Internet qui insère sur celui-ci le bouton « j'aime » de Facebook peut être considéré comme co-responsable (avec Facebook) du traitement des données personnelles des visiteurs de son site Internet pour la collecte et la transmission de ces données à Facebook. En particulier, le fait que Fashion ID **n'ait pas elle-même accès aux données personnelles** collectées et transmises à Facebook ne lui enlève pas pour autant sa qualité de co-responsable du traitement (CJUE, 29.7.2019, affaire C-40/17, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV*, § 64 ss).

En outre, la CJUE considère de manière constante que « *l'existence d'une responsabilité conjointe ne se traduit pas nécessairement **par une responsabilité équivalente**, pour un même traitement de données à caractère personnel, des différents acteurs. Au contraire, ces acteurs peuvent être impliqués **à différents stades** de ce traitement et **selon différents degrés**, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte **de toutes les circonstances** pertinentes du cas d'espèce* » (CJUE, 29.7.2019, affaire C-40/17, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV*, § 70 ; ; CJUE [Grande chambre], 10.7.2018, affaire C_25/17, *Témoins de Jéhova*, § 66 CJUE ; [Grande Chambre], 5.6.2018, affaire C-210/2016, *Wirtschaftsakademie Schleswig-Holstein GmbH c. Facebook Ireland Ltd*, § 43).

2.2.16. Dans le canton de Fribourg, la responsabilité de la sécurité des données au sens large **est assumée conjointement** par les unités administratives qui traitent des données à raison de la matière, et par le SITel en sa qualité de service de l'État en charge de l'informatique et des télécommunications (cf. les articles 4 à 7 du Règlement du 29 juin 1999 sur la sécurité des données personnelles [RSD ; RSF 17.15]).

2.2.17. En accord avec la jurisprudence précitée de la CJUE, cette responsabilité conjointe n'est cependant **pas globale mais différenciée** selon une clé de répartition fondée à la fois sur la division du travail et sur la loi :

> De manière générale, l'article 4 RSD prévoit que les unités administratives qui traitent des données à raison de la matière sont principalement responsables de ces dernières (***Data Owner* = sécurité des informations**). Le SITel, de son côté, est responsable de manière générale de la sécurité des moyens informatiques de l'État (***System / Application Owner* = sécurité des infrastructures et des applications**) (cf. art. 7 RSD *cum* art. 5 al. 2 let. b, e, i et j de l'ordonnance du 3 novembre 2015 sur la gestion de l'informatique et des télécommunications) ;

> S'agissant plus spécifiquement **de l'externalisation du traitement de données**, l'article 12b al. 3 prévoit expressément qu'au sein de l'administration cantonale, la responsabilité de la mise en œuvre et du suivi des règles dans ce domaine est **assumée conjointement** par l'organe compétent à raison de la matière et par le service en charge de l'informatique ;

> Enfin, s'agissant d'une externalisation qui concerne **plusieurs organes différents**, l'article 12b al. 2 prévoit, ainsi qu'on l'a vu, la désignation d'un **organe principalement responsable**.

2.2.18. Au vu de ces éléments, il ne semble pas possible de partager l'avis de l'ATPrD selon lequel la responsabilité du traitement des données **ne pourrait pas être partagée** entre plusieurs organes différents.

2.2.19. Sur la base des informations qui nous ont été communiquées, force est de constater qu'il **n'existe cependant pas une décision** prévoyant formellement le déploiement de Microsoft Office 365 auprès de l'ensemble des organes de l'État et désignant le SITel comme organe principalement responsable au sens de l'article 12c al. 2 LPrD. Cette qualité ressort malgré tout d'un **faisceau d'indices convergents** :

> Premièrement, **le SITel a été expressément autorisé** à mener le projet pilote Microsoft Office 365 dans le cadre de l'ordonnance du 4 décembre 2018 précitée ;

> Deuxièmement, c'est lui **l'auteur du rapport d'évaluation** sur lequel le Conseil d'État s'est fondé pour décider de créer les bases légales nécessaires à son déploiement ;

> Troisièmement, l'ACE 2020-481 du 16 juin 2020 retient que **le SITel est chargé de déployer** une solution pour intégrer les fonctionnalités de téléphonie Cisco de manière transparente pour l'utilisateur au sein de Microsoft Teams et qu'il doit élaborer une solution pour les fonctionnalités des centrales téléphoniques.

À l'avenir, **il serait cependant souhaitable** que le Conseil d'État – ou les autres organes amenés à prendre ce type de décision – accomplisse ces actes **de manière plus claire et plus proche du texte de la loi** en prévoyant systématiquement au moyen d'un arrêté ou d'une décision le déploiement d'une solution et la désignation de l'organe principalement responsable. On peut par ailleurs se demander s'il ne serait pas indiqué que, basé sur les trois points susmentionnés, le Conseil d'État prenne lors d'une de ses prochaines séances **une décision destinée à formaliser** le déploiement de Microsoft Office 365 au sein de l'État.

2.2.20. Bien que la répartition des responsabilités soit effectuée directement par la loi, il conviendrait en sus de la faire ressortir une deuxième fois au moment d'établir **la déclaration du traitement** dans le Registre des fichiers (REFI) au sens des articles 19 al. 2 let. e LPrD et 6 RSD. En tant qu'organe principalement responsable, cette déclaration devrait être faite **par le SITel** pour Office Microsoft 365 en précisant l'existence d'une responsabilité conjointe entre le SITel et les différents organes de l'État selon la clé de répartition évoquée plus haut. Une indication devrait être donnée sur le fait que l'organe compétent pour traiter toute demande d'accès au sens de l'article 23 LPrD est l'organe responsable du traitement à raison de la matière.

2.2.21. En qualité d'organe principalement responsable, le SITel doit en particulier **négocier le contrat d'externalisation et veiller** à ce que celui-ci respecte les exigences fixées dans la loi en matière de sécurité et de protection des données. Il doit pour ce faire **prévoir les mesures de sécurité adéquates** à mettre en place afin d'assurer l'intégrité, l'authenticité, la disponibilité, la pérennité et la confidentialité des données externalisées et s'assurer du fait que ces mesures sont effectivement mises en pratique (cf. art. 12d LPrD).

2.2.22. Le fait que la négociation du contrat d'externalisation et le choix des mesures de protection et de sécurité à mettre en place incombent prioritairement au SITel **n'empêche bien évidemment pas**, bien au contraire, que l'organe qui traite des données à raison de la matière s'assure lui aussi du respect des règles prescrites et qu'il signale au SITel, si besoin est, **tout éventuel manquement** aux règles en vigueur. Le cas échéant, il n'est **pas non plus exclu** que l'organe qui traite des données à raison de la matière et qui peut donc avoir une meilleure sensibilité par rapport au contenu des données communique pour information **ses recommandations** en matière de sécurité et de protection.

2.2.23. Pour des raisons **d'efficacité et de rationalité**, et aussi **de cohérence** au sein de l'État, il n'est cependant pas envisageable que n'importe quel organe qui traite des données **décide lui-même**

de toutes les mesures de sécurité qu'il voudrait voir appliquer à ses propres données, surtout si celles-ci dépassent ce qui est prévu par la loi. La loi fixe **un cadre général applicable à l'ensemble des organes de l'État** qui correspond à la volonté du législateur. Il n'appartient pas à un organe de l'État de remettre ce cadre en question simplement parce qu'il le juge à titre personnel inadéquat, ni de le modifier. Une telle attitude irait en effet à l'encontre des principes **de la légalité, de la séparation des pouvoirs et de la primauté de la loi** en vertu desquels l'administration est tenue dans ses activité de se soumettre à l'ordre juridique et aux prescriptions adoptées par le législateur, et de n'exercer ses activités que dans le cadre tracé par la loi (ATF 144 V 411, consid. 4.6 et 4.7 ; ATF 131 II 562, consid. 3.1 ; TANQUEREL Thierry, *Manuel de droit administratif*, 2e éd., Genève / Zurich / Bâle 2018, no 467 ; DUBEY / ZUFFEREY, *Droit administratif général*, Bâle 2014, no 499 s ; MOOR / FLÜCKIGER / MARTENET, *Droit administratif, vol. I Les fondements*, Berne 2012, p. 651 ; STEINAUER Paul-Henri, *Traité de droit privé suisse – Le titre préliminaire du Code civil*, Bâle 2009, no 324).

2.2.24. Du point de vue du pouvoir hiérarchique du Conseil d'État sur l'administration, un organe étatique quel qu'il soit ne peut pas non plus, contre la décision du Conseil d'État, **refuser que les données qu'il traite soient mises dans le *cloud* ni conditionner l'usage du *cloud* à des règles qu'il fixerait lui-même**. Selon la Constitution et la loi, il revient, en effet, au Conseil d'État en tant que gouvernement **de diriger, d'organiser et de contrôler l'administration** (cf. art. 110 Cst./Fr ; ég. MOOR / BELLANGER / TANQUEREL, *Droit administratif, vol. III L'organisation des activités administratives. Les biens de l'État*, Berne 2018, p. 69 ; EHRENZELLER Bernhard, in : Ehrenzeller Berhard et alii (édit.), *St-Galler Kommentarz zur Bundesverfassung*, Zurich / Bâle / Genève 2014, ad art. 174 Cst., no 4).

2.2.25. Les compétences organisationnelles et directoriales du Conseil d'État ressortent en particulier de la LOCEA. Selon cette dernière, le Conseil d'État doit **diriger l'administration à l'aide d'instruments modernes d'organisation et de gestion** (cf. art. 5 al. 1 LOCEA). Il définit notamment les objectifs généraux de l'administration et fixe ses priorités et il accomplit les tâches d'organisation et de gestion qui lui sont dévolues (cf. art. 5 al. 1 let. a et b LOCEA). En outre, il **pourvoit à l'exécution de la législation**, notamment en accomplissant lui-même les actes d'administration qui, en raison de leur importance ou de par la législation, ne peuvent être attribués ni délégués à une autre autorité (cf. ar. 6 LOCEA).

2.2.26. Le Conseil d'État a usé de son pouvoir organisationnel et directorial en adoptant **l'ordonnance du 3 novembre 2015 sur la gestion de l'informatique et des télécommunications dans l'administration** (RSF 122.96.11). Selon cette ordonnance, les compétences en matière de gestion de l'informatique sont réparties entre différents organes (Conseil d'État, Délégation du Conseil d'État en matière de digitalisation et de systèmes d'information, Direction des finances, SITel ainsi que différentes commission spécialisées).

2.2.27. Il ressort en particulier de cette ordonnance que le Conseil d'État adopte **les mesures nécessaires à la transformation digitale** de l'État de Fribourg, lesquelles lui sont proposées par la Délégation du Conseil d'État en matière de digitalisation et de systèmes d'information (cf. art. 3a al. 1 let. c et 3a al. 2 let. a). Cette dernière est en outre compétente pour **décider des projets informatiques importants**. Quant au SITel, il **fournit en particulier les prestations informatiques** ayant reçu l'aval des autorités compétentes aux organes de l'administration (cf. art. 5 al. 2 let. b).

2.2.28. Bien qu'elle pourrait être formulée de manière un peu plus claire, cette répartition des compétences voulue par le Conseil d'État de même que les décisions et autres actes pris conformément à celle-ci par les organes désignés sont **opposables à l'ensemble des unités**

administratives de l'État. Demeurent réservés les cas où une unité administrative est habilitée à gérer son informatique de manière autonome.

2.2.29. En sa qualité d'unité administrative ne gérant pas son informatique de manière autonome, l'ATPrD ne peut ainsi pas exiger **l'application d'un régime spécial** concernant le traitement de ses propres données.

2.2.30. Ne paraissent ainsi **pas recevables** les exigences suivantes formées dans le courrier de l'ATPrD du 25 mars 2021 :

> *toutes données, documents, traitements de données (courriels, dossiers, échanges téléphoniques, documents, etc.) effectués par l'Autorité sont traités, stockés et hébergés sur des serveurs sécurisés en Suisse.* Car en application de l'article 12b al. 2 LPrD, les lieux de traitement doivent être situés en tout temps sur le territoire suisse **ou sur le territoire d'un Etat garantissant un niveau de protection des données équivalent**.

> *Les clés de chiffrement sont en main du SITel. Le cas échéant, le SITel s'engage à mettre en place des mesures techniques supplémentaires (tels que chiffrement du contenu et pseudonymisation des utilisateurs par l'organe)*. Car cette exigence **ne tient pas compte de l'article 12e al. 2 LPrD** en vertu duquel le sous-traitant peut également disposer d'une clé de déchiffrage lorsque cela est absolument nécessaire pour des raisons techniques et à condition que les garanties contractuelles et techniques mentionnées soient respectées.

> *Les contrats d'externalisation mentionnent le for et le droit applicable en Suisse*. Car, même s'il juge que cela est souhaitable, le législateur **a expressément renoncé à introduire une telle exigence** (cf. Message 2019-CE-239 du 21 avril 2020 accompagnant le projet de loi adaptant la législation cantonale à certains aspects de la digitalisation, p. 11).

> *la Commission dispose d'une plateforme sécurisée, dont les données et documents sont stockés et hébergés sur un serveur sécurisé du SITel et accessible par des personnes hors périmètre de l'État*. En effet, **aucune base légale** ne prévoit la mise à disposition d'une telle plateforme sécurisée. Si, sur la base du droit en vigueur, la mise à disposition d'une plateforme sécurisée ne peut pas en tant que telle être exigée par l'ATPrD comme solution unique, il est toutefois clair que les outils mis à disposition de la Commission pour travailler doivent eux être sécurisés et respecter les exigences du droit de la protection des données.

2.2.31. En revanche, basée sur le droit en vigueur, l'ATPrD à l'instar de toute autre unité administrative ayant **le statut de co-responsable du traitement**, paraît légitimée à demander au SITel, le cas échéant, **des garanties** concernant le respect des règles suivantes :

> *le transfert des données* [est] *chiffré*. En effet, le chiffrement des données lors de leur transfert correspond aujourd'hui à **un standard minimal** en matière de sécurité des données et équivaut de ce fait à une concrétisation de l'article 12d LPrD.

> *les données hébergées dans le cloud sont chiffrées*. En soi, l'article 12e LPrD réserve cette mesure aux données sensibles qui présentent un risque concret d'atteinte aux droits des personnes et aux données protégées par une obligation légale ou contractuelle de garder le secret. Toutefois, dans la mesure où ce type de données **sont susceptible d'être échangées** au moyen des outils de communication unifiée et qu'il n'est pas possible de différencier dans ce cadre les données sensibles des autres données afin de leur appliquer un régime différent, il se justifie d'appliquer les mesures de protection les plus élevées **à l'ensemble des données concernées**.

> *les personnes autorisées à traiter les données sont soumises au respect de la confidentialité et du secret de fonction. Les données ne sont pas accessibles par des personnes non-autorisées.* Car ces

obligations **découlent des articles 12c al. 1 let. b ch. 3 et 12d LPrD**. En principe, les fournisseurs de service *cloud* sont considérés comme **des auxiliaires du responsable du traitement**, ce qui implique que les obligations du droit pénal liées au respect des secrets rejaillissent sur eux de plein droit (cf. art. 321 CP in fine ; ég. MÉTILLE Sylvain, *L'utilisation de l'informatique en nuage par l'administration publique*, in PJA 2019, p. 609 ss, p. 613). Par précaution, cela devrait toutefois également figurer dans les contrats. L'application de la protection des secrets au sens du droit pénal suisse n'est toutefois généralement **pas possible à l'étranger**. Dans ce cas, le contrat devrait prévoir **une peine contractuelle** suffisamment dissuasive pour garantir la confidentialité des données (ROSENTHAL David, *Mit Berufsgeheimnissen in die Cloud : So geht es trotz US CLOUD Act*, in : Jusletter10 août 2020, n° 53 ss).

> *tout sous-traitant est désigné avec l'accord écrit du SITel qui s'est assuré que le sous-traitant est en mesure de garantir la sécurité des données. L'Autorité doit être informée de manière préalable à l'accord. Le traitement des données est effectué uniquement par des sous-traitants venant de pays ayant un niveau de protection des données suffisant (selon liste du PFPDT et LPrD 12ss)*. Car ces exigences **correspondent aux articles 12b al. 2 et 12c al. 1 let. a et b ch. 5 et 6 LPrD**. À noter qu'il s'agit ici uniquement d'une information et non pas d'une demande d'autorisation.

2.2.32. La recommandation/exigence tendant à mettre en place un « *Chinese Wall* » entre les collaborateurs de l'ATPrD selon qu'ils exercent leurs activités dans le domaine de la transparence ou de la protection des données et celle de pouvoir gérer les droits d'accès des collaborateurs de l'Autorité de manière autonome seront analysées au point 2.3 (cf. § 2.3.28 - 3.3.33).

2.3. Sur la légalité des exigences et des recommandations formées par l'ATPrD en tant qu'autorité indépendante chargée de la surveillance de la protection des données

2.3.1. En plus des activités de traitement qu'elle accomplit pour son propre compte, l'ATPrD est chargée, de par la loi, **de la surveillance de la protection des données** au sein de l'État (cf. art. 29 ss LPrD).

2.3.2. Lorsqu'elle agit ou qu'elle est directement concernée par une affaire en sa qualité d'autorité de contrôle en matière de protection des données, l'ATPrD est considérée comme **une autorité indépendante** rattachée administrativement à la Chancellerie d'État (cf. art. 32 al. 1 et 2 LPrD).

2.3.3. L'indépendance reconnue aux autorités de contrôle en matière de protection des données tire son fondement **de conventions internationales** qui lient la Suisse, en particulier le Protocole additionnel du 8 novembre 2001 à la Convention STE 108 du 28 janvier 1981 concernant les autorités de contrôle et les flux transfrontières de données (RS 0.235.1) et la Directive (UE) 2016/680 sur la protection des données dans le domaine de la police et de la justice (cf. art. 41 ss). La doctrine en Suisse considère que la mise sur pied d'une autorité indépendante en matière de protection des données découle également **directement des articles 13 al. 2 et 35 Cst.** (cf. WALDMANN / SPIELMANN, *L'indépendance de l'autorité cantonale de surveillance en matière de protection des données*, 2010, n° 35).

2.3.4. La doctrine a mis en évidence **différents critères** tendant à concrétiser cette indépendance, tels que l'indépendance institutionnelle, fonctionnelle, structurelle, matérielle et enfin personnelle. De manière générale, ces différents critères visent à permettre aux autorités de contrôle en matière de protection des données d'exercer les différentes tâches que leur assigne la loi **sans influence externe, de manière effective, efficace et avec les ressources adéquates, et de façon impartiale** (WALDMANN / SPIELMANN, *op. cit.*, 2010, n° 57 ss ; EPINEY Astrid, *Die Unabhängigkeit der*

datenschutzrechtlichen Aufsichtsbehörden: der europarechtliche Rahmen, in : Epiney / Hänni / Brülisauer (édit.), L'indépendance des autorités de surveillance et autres questions actuelles en droit de la protection des données, Zurich / Bâle / Genève 2012, p. 16 ss).

2.3.5. L'indépendance des autorités chargées de la protection des données n'implique en revanche **pas qu'elles seraient entièrement soustraites à la surveillance** du Conseil d'État. Selon l'art. 110 Cst./Fr., le Conseil d'État **exerce le pouvoir exécutif, dirige l'administration et conduit la politique du canton**. En sa qualité d'unité rattachée administrativement à l'Etat, l'ATPrD fait également partie de l'administration cantonale, et de la sorte **elle est soumise, aux termes de la Constitution, au contrôle du Conseil d'État**. L'indépendance de l'Autorité dans l'exercice de ses attributions restreint, il est vrai, sensiblement l'étendue de ce contrôle. S'il ne peut s'immiscer dans une affaire de l'Autorité, le Conseil d'Etat reste néanmoins habilité à contrôler de manière générale **son bon fonctionnement,** notamment en matière d'efficacité et d'efficience (WALDMANN / SPIELMANN, *op. cit.*, 2010, n° 69 ; SÄGESSER Thomas, *Institutionelle Stellung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten*, in: PJA 2009, p. 1421 s ; *contra* : HUBER René, in : Maurer-Lambrou / Blechta (édit.), Basler Kommentar DSG, Bâle 2014, ad art. 26 LPD, n° 30a).

2.3.6. L'indépendance des autorités chargées de la protection des données **n'a pas non plus pour conséquence** que celles-ci seraient également indépendantes dans **la gestion de leur informatique.** Au contraire, la doctrine considère que l'indépendance des autorités chargées de la protection des données ne donne **pas droit à une indépendance organisationnelle** par rapport au reste de l'État. Au vu du rattachement administratif qui les lient à l'État rien ne s'oppose à ce qu'elles **utilisent généralement les ressources et les infrastructures** que celui-ci met à disposition de l'ensemble des unités administratives (WALDMANN / OESCHGER, *Aufsicht (§15)*, in : Datenschutzrecht – Grundlagen und öffentliches Recht, Berne 2011, n° 40 ; HÄNNER Isabelle, *Unabhängigkeit der Aufsichtsbehörden – Umsetzung am Beispiel der Datenschutzaufsicht des Kantons Zürich*, in : Digma 2008 cahier 3, n° 59).

2.3.7. Il s'ensuit que l'ATPrD, en tant qu'autorité chargée de la protection des données, n'est en principe **pas non plus en droit d'exiger un régime spécial** concernant le traitement de ses propres données, qui diffèrerait de celui appliqué aux autres organes de l'État traitant des données présentant un degré de sensibilité équivalent.

2.3.8. Par contre cela fait partie des tâches de l'ATPrD que de **contrôler que le droit de la protection des données est correctement appliqué,** que ce soit à l'égard de ses propres données ou des données des autres organes de l'État (cf. art. 29 al. 1 LPrD).

2.3.9. En tant qu'autorité indépendante chargée de la surveillance du traitement des données, l'ATPrD est dotée dans ce but de **larges pouvoirs d'investigation,** lesquels découlent à la fois des textes internationaux précités et du droit interne. En droit fribourgeois, l'article 31 al. 3 LPrD énonce que le ou la préposé-e **recueille les informations nécessaires** à l'accomplissement de ses tâches. Il ou elle peut notamment demander des renseignements, exiger la production de documents, procéder à des inspections et se faire présenter des traitements de données (1ère et 2e phr.).

2.3.10. En outre, l**e secret de fonction ne peut pas être opposé au ou à la préposé-e** (art. 31 al. 3, 3e phr.). Il s'ensuit que le ou la préposée à la protection des données dispose en principe d'un accès **à toutes les informations** qui sont utiles à l'exercice de ses fonctions tels des contrats, des expertises, des règlements d'utilisation etc. Il ou elle peut aussi, le cas échéant, accéder aux locaux, aux installations et aux logiciels servant au traitement des données, procéder à l'audition de personnes impliquées dans le traitement des données ou réaliser ou faire réaliser des audits (comparaison : art.

50 al. 1 LPD du 25 septembre 2020 ; art. 58 ch. 1 let. a à f RGPD ; ég. art. 56 al. 2 de l'avant-projet de révision totale de la LPrD ; voir aussi : WALDMANN / OESCHGER, *op. cit.*, n° 46).

2.3.11. Bien qu'étendus, les pouvoirs d'investigation dont disposent les autorités chargées de la surveillance du traitement des données ne sont **pas illimités** pour autant. Comme pour toute activité, ils sont encadrés par **la loi** et par **les principes de l'activité de l'État régi par le droit** (cf. art. 4 Cst./Fr et 5 Cst. fédérale).

2.3.12. En particulier, l'ATPrD, lorsqu'elle exerce ses activités de surveillance, n'est **pas un électron libre** mais elle est considérée comme une autorité administrative soumise aux règles du **Code de procédure et de juridiction administrative** (CPJA ; RSF 150.1) (cf. Message du Conseil d'État n° 56 accompagnant le projet de loi modifiant la loi sur la protection des données [adaptation au droit international, en particulier aux accords de Schengen/Dublin du 4 mars 2008], in BGC 2008, p. 661)

2.3.13. À ce titre, elle est tenue notamment d'appliquer **sous l'angle matériel** les principes de la légalité, de l'égalité de traitement, de la proportionnalité, de la bonne foi et de l'interdiction de l'arbitraire (cf. art. 8 CPJA). En tant qu'autorité, l'ATPrD est aussi soumise à **l'interdiction de l'abus de droit** (de manière générale : DUBEY / ZUFFEREY, n° 733). Elle doit dans ce cadre se garder d'utiliser son statut d'autorité pour se livrer à des activités ne poursuivant aucun intérêt objectif, sérieux et digne de protection ou fondées sur des motifs qui ne constituent manifestement qu'un prétexte, ou pourvues d'une motivation contradictoire ou purement chicanière (ATF 143 III 279, consid. 3.1 ; arrêt du TF 5A_536/2019, consid. 2.2 ; arrêt du TF 4A_460/2020, consid. 2.2).

2.3.14. Il est vrai toutefois que la doctrine **se montre prudente** quant aux possibilités pour le gouvernement de contrôler le travail des autorités chargées de la protection des données sous l'angle de ces différents principes, car celait pourrait aboutir à remettre leur indépendance en question (EPINEY Astrid, *Zum Urteil des EuGH vom 9. März 2010 i.S. Kommission/Deutschland in der Rs. C-518/07 und seinen Auswirkungen auf die Schweiz*, in : PJA 2010 659, p. 661).

2.3.15. Sous l'angle formel, elle doit, à l'instar de n'importe quelle autorité administrative, respecter la **structure organisationnelle** des entités soumises à sa surveillance et **les règles en matière de représentation** en découlant. En particulier, si un représentant lui a été désigné, elle ne peut pas contourner celui-ci en s'adressant directement aux différents collaborateurs de l'organe surveillé afin d'obtenir de leur part des informations sans passer par le représentant désigné (cf. art. 13 *cum* art. 34 al. 2 CPJA).

2.3.16. Pour le reste, l'ATPrD doit respecter les règles relatives à **l'établissement des faits** et au **droit d'être entendu** (cf. art. 45 ss et 57 ss CPJA) sous réserve, le cas échéant, des dispositions contraires prévues dans la LPrD, cette dernière intervenant dans ce cas en tant que *lex specialis* par rapport au CPJA.

2.3.17. L'organe surveillé est de son côté soumis **à l'obligation de collaborer** prévue par le CPJA (cf. art. 48 CPJA). Bien que cela ressorte déjà de l'article 31 al. 3 LPrD, il est tenu à ce titre de produire les documents et de fournir les renseignements en sa possession nécessaires à l'établissement des faits, de comparaître aux auditions qui sont ordonnées et de tolérer l'inspection de ses locaux ou de son matériel, ou de se soumettre à une expertise.

2.3.18. L'article 50 al. 3 CPJA renvoyant aux articles 18 ss CPJA concernant les conflits qui peuvent exister entre autorités n'est **pas applicable aux procédures menées par l'ATPrD**. La LPrD

intervient ici également en qualité de *lex specialis* s'agissant des activités de surveillance de l'ATPrD.

2.3.19. Dans l'appréciation qu'elle fait des situations soumises à sa surveillance, l'ATPrD doit respecter **le droit en vigueur.** Cela vaut pour le droit cantonal, le droit international et le droit fédéral dans le mesure où celui-ci trouve application.

2.3.20. À moins qu'une disposition ne soit **manifestement irrégulière**, l'ATPrD n'est ainsi **pas habilitée à agir en opportunité** et à substituer ses propres exigences au texte de la loi (cf. art. 10 al. 4 CPJA ; voir ég. MOOR / FLÜCKIGER / MARTENET, *op. cit.*, p. 634 s). En tant qu'autorité, l'ATPrD appartient, en effet, à la branche exécutive de l'État chargée d'appliquer les lois. Elle est **une autorité administrative et non pas une autorité politique, législative ou judiciaire.**

2.3.21. En tant qu'autorité indépendante chargée de la protection des données, elle peut en revanche, dans un cas particulier, **contester la conformité** d'une disposition adoptée par le législateur avec les exigences formées dans ce domaine par le droit constitutionnel et/ou par le droit supranational. Dans ce cas, il lui appartient cependant d'agir en conséquence **en motivant et en démontrant cette incompatibilité** et en **la faisant constater,** le cas échéant, par l'autorité judiciaire compétente selon la procédure prévue à cet effet.

2.3.22. Dans la mesure où à notre connaissance l'ATPrD n'a jusqu'à ce jour **pas formellement contesté** la conformité des articles 12b ss LPrD aux exigences du droit de la protection des données et **qu'aucune décision de justice** n'a été rendue concluant à leur non-conformité, il s'ensuit qu'en tant qu'autorité l'ATPrD est tenue **de s'y tenir comme de veiller à leur application correcte**.

2.3.23. Comme cela a déjà été exposé plus haut (cf. § 2.2.9 - 2.2.12), l'article 12c al. 2 LPrD prévoit que pour les projets d'externalisation concernant plusieurs organes différents au sein d'une même collectivité, **un organe principalement responsable** doit être désigné. L'organe principalement responsable est l'interlocuteur principal du fournisseur de service. À ce titre, il lui revient en particulier de **négocier et de passer le contrat d'externalisation** conformément aux exigences prévues par la loi et aussi de veiller à leur respect.

2.3.24. En tant qu'organe principalement responsable (cf. § 2.2.19), le SITel dispose d'un certain **pouvoir d'appréciation** au moment de négocier et d'établir le contrat d'externalisation. Ce pouvoir d'appréciation qui ressort de plusieurs dispositions de la loi porte, en particulier, sur **le choix du prestataire** (cf. art. 12c al. 1 let. a LPrD, sur **certains éléments du contenu du contrat** (cf. art. 12c al. 1 let. b LPrD) et sur **les mesures de protection et de sécurité à mettre en place** (cf. art. 12d LPrD).

2.3.25. Tant qu'il s'inscrit dans le cadre prévu par la loi et qu'il respecte les exigences du droit de la protection des données, l'usage de ce pouvoir d'appréciation n'a, en principe, **pas à être remis en cause,** car il reflète la volonté du législateur qui a voulu laisser par là une certaine **marge de manœuvre** à l'organe compétent (ATF 140 I 201, consid. 6.1 ; TANQUEREL Thierry, *op. cit.*, n° 508 ; voir aussi le Message 2019-CE-239 du 21 avril 2020 accompagnant le projet de loi adaptant la législation cantonale à certains aspects de la digitalisation d'où il ressort que le législateur a voulu laisser aux organes compétents le soin de fixer les mesures de protection et de sécurité appropriées au regard de l'ensemble des circonstances et d'établir les contrats y résultant, p. 10).

2.3.26. En sa qualité d'autorité chargée de la surveillance du traitement des données, l'ATPrD a pour mission de **vérifier la conformité** des traitements effectués avec le droit en vigueur. Même si pareille tâche implique nécessairement **une part d'interprétation**, celle-ci est toutefois limitée par **le**

***sens littéral possible* de la règle**. « *Comme le cadre d'un tableau ou la barrière d'un pont, il balise le champ de réflexion de l'interprète. Il s'impose comme l'un des critères de toute méthode d'interprétation objective, car la confiance que le destinataire de la norme peut placer dans le législateur* […] *ne sera protégée que si cette norme ne reçoit pas un sens qui ne trouve aucune assise dans l'expression que lui a donné son auteur* » (cf. STEINAUER Paul-Henri, *op. cit.*, n° 336).

2.3.27. Face à un texte clair, l'ATPrD en sa qualité d'autorité chargée d'appliquer la loi n'est ainsi pas habilitée à **agir en opportunité ni à se substituer au législateur** en formant des exigences nouvelles. Comme cela a déjà été évoqué plus haut (cf. § 2.2.23), pareil agissement équivaudrait à **une violation des principes de la légalité, de la séparation des pouvoirs et de la primauté de la loi**.

2.3.28. Sur la base de ce qui précède, on peut appliquer ***mutatis mutandis*** les conclusions auxquelles nous sommes déjà parvenus en lien avec les différentes recommandations/exigences formées par l'ATPrD en sa qualité de responsable du traitement. **Les recommandations/exigences qui contredisent le cadre fixé par la loi (cf. § 2.2.30) devraient être déclarées irrecevables. Les recommandations/exigences qui correspondent à ce que la loi prévoit devraient être suivies (2.2.31).**

2.3.29. En comparaison avec les autres unités administratives de l'État, l'ATPrD n'est pas limitée à simplement demander des garanties concernant la mise en œuvre correcte des exigences fixées dans la loi (cf. § 2.2.31). En sa qualité d'autorité chargée de la surveillance du traitement des données, **elle dispose de tous les moyens d'investigations précités afin de vérifier que tel est bien le cas**.

2.3.30. Cela étant dit, il y a lieu de revenir sur l'exigence particulière de **maintenir un « *Chinese Wall* » au sein de l'ATPrD** entre ses activités relevant du domaine de la transparence et celles relevant du domaine de la protection des données.

2.3.31. Dans son courrier du 25 mars, l'ATPrD fait valoir qu'elle gère, en effet, aussi bien le domaine de la transparence que celui de la protection des données et que ces deux domaines sont indépendants l'un de l'autre, nécessitant **une organisation spécifique** au sein même de l'autorité. Elle demande pour ces raisons une **séparation claire de ces deux domaines sous l'angle informatique** et la possibilité de **gérer les comptes utilisateurs et les droits d'accès de manière autonome**.

2.3.32. Bien qu'une telle exigence ne ressorte peut-être pas explicitement de la loi, elle découle néanmoins **directement du critère de l'indépendance structurelle** reconnue aux autorités chargées de la surveillance de la protection des données. En outre, la volonté d'une **séparation radicale** entre le domaine de la transparence et de la protection des données a aussi été largement mise en évidence au moment d'adopter la loi du 9 septembre 2009 sur l'information et l'accès et aux documents (LInf ; RSF 17.5) (cf. Message du Conseil d'État accompagnant le projet de loi sur l'information et l'accès aux documents du 26 août 2008, in : BGC 2009, p. 937).

2.3.33. Du point de vue structurel, **il est normal** que les dossiers relatifs aux questions de transparence et les dossiers relatifs aux questions de protection des données, dans la mesure où ils dépendent de **deux entités différentes au sein de l'autorité** (le ou la préposée à la transparence et le ou la préposé-e à la protection des données) soient soumis à **une séparation nette**.

2.3.34. Cette séparation doit être assurée tant par des mesures **organisationnelles que techniques**. Sous l'angle technique, il convient en particulier de **garantir l'existence d'un « Chinese Wall »** entre les activités relevant du domaine de la transparence et les activités relevant du domaine de la

protection des données. A supposer que cette séparation ne pourrait plus être appliquée par le passage à Microsoft Office 365, il conviendrait alors de trouver **une solution de remplacement**. Dans la mesure toutefois où **les dossiers de l'Autorité** ne sont pas dans *le cloud* mais qu'ils continuent d'être hébergés sur les serveurs du SITel (cf. § 1.8), cela ne devrait, en principe, pas poser de problèmes particuliers.

2.3.35. S'agissant maintenant de la recommandation/exigence tendant à laisser l'autorité s'occuper elle-même de **la gestion de ses comptes utilisateurs et les droits d'accès**, nous ne sommes pas en mesure de nous prononcer là-dessus dans la mesure où nous n'en percevons pas les enjeux.

3. Conclusions

3.1. Le courrier de l'ATPrD du 25 mars 2021 n'est formellement **pas une recommandation** au sens de l'article 22a LPrD. Il n'ouvre donc à ce stade pas la voie à **une procédure devant le Tribunal cantonal**.

3.2. Dans le domaine du traitement des données au sein de l'État, il existe une **responsabilité conjointe** entre le SITel et les organes qui traitent des données à raison de la matière.

3.3. L'existence d'une responsabilité conjointe ne se traduit pas nécessairement **par une responsabilité équivalente**, pour un même traitement de données à caractère personnel, des différents acteurs. Au contraire, ces acteurs peuvent être impliqués **à différents stades** de ce traitement et **selon différents degrés**, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte **de toutes les circonstances** pertinentes du cas d'espèce.

3.4. En tant que *System / Application owner*, le SITel est responsable **de la sécurité des moyens informatiques** qu'il met à disposition des organes de l'État. En tant que *Data owner*, les organes qui traitent des données à raison de la matière sont responsables **des informations qu'ils traitent**.

3.5. En matière d'externalisation, l'article 12c al. 2 LPrD prévoit que lorsqu'une externalisation concerne plusieurs organes différents au sein d'une même collectivité publique, **un organe principalement responsable** est désigné.

3.6. Le SITel est l'organe principalement responsable par rapport au déploiement de Microsoft Office 365. En cette qualité, il est chargé **de passer le contrat d'externalisation avec Microsoft, de prévoir les mesures de sécurité à mettre en place et de veiller à leur respect**. Le contrat passé par le SITel **lie** l'ensemble des unités administratives de l'État.

3.7. En tant que responsable du traitement, les unités administratives de l'État sont autorisées à demander au SITel **de leur fournir des garanties** à propos du fait que les exigences du droit de la protection des données sont respectées. À moins que la loi ne le prévoie expressément, elles ne peuvent cependant **pas exiger l'application d'un régime spécial** qui leur serait propre.

3.8. Cela s'applique **aussi globalement à l'ATPrD** s'agissant du traitement de ses propres données. L'indépendance de l'ATPrD concerne la manière dont elle **exerce ses activités**. Elle ne confère pas à l'autorité **une indépendance organisationnelle** qui la rendrait indépendante du reste de l'État et qui lui permettrait de gérer son informatique de manière autonome. Dans ce domaine, l'ATPrD est soumise **au pouvoir organisationnel** du Conseil d'État. En outre, l'indépendance de l'ATPrD ne la préserve pas non plus **de toute surveillance** de la part du Conseil d'État. Si le Conseil d'État ne peut pas s'immiscer dans une affaire de l'Autorité, il reste néanmoins habilité à contrôler de manière générale **son bon fonctionnement**.

3.9. En tant qu'autorité chargée de la surveillance du traitement des données, l'ATPrD dispose de **larges pouvoirs d'investigation** lui permettant de contrôler le respect des prescriptions en matière de protection des données. Elle peut exiger l'accès aux documents utiles tels que des contrats et des résultats d'expertises, procéder à des inspections ou se faire présenter des traitements de données. **Le secret de fonction ne lui est pas opposable**. Les organes soumis à sa surveillance sont en outre **tenus de collaborer** aux enquêtes menées par l'ATPrD.

3.9. Bien qu'étendus, les pouvoirs d'investigation dont disposent l'ATPrD ne sont **pas illimités** pour autant. Comme pour toute activité, ils sont encadrés par **la loi** et par **les principes de l'activité de l'État régie par le droit.** Lorsqu'elle exerce ses activités de surveillance, elle n'est **pas un électron libre** mais elle est considérée comme une autorité administrative soumise aux règles du **Code de procédure et de juridiction administrative.** Il s'ensuit qu'elle est tenue de respecter certaines règles **de fond** (légalité, proportionnalité, bonne foi, interdiction de l'arbitraire et de l'abus de droit) comme **de forme** (échanges et représentation).

3.10. Lorsqu'elle apprécie une situation en droit, l'ATPrD est soumise aux principes de la légalité, de la séparation des pouvoirs et de la primauté de la loi. Elle doit donc s'en tenir à ce que dit la loi et ne peut pas **agir en opportunité ni se substituer au législateur** en formant de nouvelles exigences extralégales.

3.11. Si elle estime qu'une règle adoptée par le législateur ne respecte pas la protection des données, elle peut, dans un cas particulier, **contester sa conformité** avec les exigences formées dans ce domaine par le droit constitutionnel et/ou par le droit supranational. Dans ce cas, il lui appartient cependant d'agir en conséquence **en motivant et en démontrant cette incompatibilité** et en **la faisant constater,** le cas échéant, par l'autorité judiciaire compétente selon la procédure prévue à cet effet (cf. art. 22a LPrD).

3.12. Tant que la non-conformité d'une règle au droit de la protection des données n'a pas été constatée, ni même invoquée, l'ATPrD, en tant qu'autorité chargée d'appliquer la loi est tenue **de s'y tenir comme de veiller à son application correcte**.

3.13. Sur la base de ce qui précède, les recommandations/exigences formées par l'ATPrD peuvent être réparties en **deux catégories** :

> Les recommandations/exigences qui **contredisent le texte de la loi** et qui devraient être déclarées irrecevables (cf. § 2.2.30) ;

> Les recommandations/exigences qui **correspondent à ce que la loi prévoit** et qui devraient être suivies et appliquées (cf. 2.2.31).

En outre, conformément au critère de l'indépendance structurelle, l'ATPrD est légitimée à demander le maintien d'un **« Chinese Wall »** au sein de l'autorité entre ses activités relevant du domaine de la transparence et ses activités relevant du domaine de la protection des données.

Michael Montavon, Juriste