DSJS/Projet du 02.12.2022

Rapport explicatif accompagnant le projet de règlement sur la sécurité de l'information (RSI)

1 INTRODUCTION

Se fondant sur des normes reconnues au plan national et international, le présent règlement crée une base légale uniforme pour la sécurité de l'information au niveau cantonal. Il met l'accent sur la création d'une organisation dédiée à la sécurité de l'information à l'échelon cantonal et sur l'élaboration d'une politique générale de sécurité de l'information comme instruments de gouvernance à l'ère du numérique. Un ou une délégué-e à la sécurité de l'information (ci-après : le ou la délégué-e SI) sera chargé de mettre en œuvre, de superviser et de coordonner l'exécution des normes prescrites conformément au règlement. Il ou elle sera aussi appelé-e, notamment, à conseiller le Conseil d'Etat et les Directions en matière de sécurité de l'information et à fournir aux organes publics les outils et l'assistance qui leur permettront de gérer la sécurité de leurs ressources informationnelles de façon optimale et rigoureuse. Dans ses fonctions, le ou la délégué-e SI sera amené-e à collaborer et à travailler étroitement avec l'Autorité de la transparence, de la protection des données et de la médiation (ci-après : ATPrDM) ainsi qu'avec le Service de l'informatique et des télécommunications (ci-après : SITel).

L'adoption de ce règlement entraînera l'abrogation de l'actuel règlement sur la sécurité des données personnelles daté du 29 juin 1999, devenu en partie obsolète. Le champ d'application doit désormais être étendu à l'ensemble des informations traitées par les organes de l'Etat.

2 CONTEXTE GÉNÉRAL DANS LEQUEL S'INSCRIT LE RÈGLEMENT

Les cyber-incidents sont en augmentation dans le monde entier, la Suisse n'en est pas épargnée. Le Centre national de cybersécurité (NCSC) reçoit en moyenne plus de 300 notifications par semaine concernant des cyberattaques réussies ou tentées. Ces évènements sont évidemment pris très au sérieux dans le canton de Fribourg. C'est pourquoi un groupe de travail a été constitué en automne

2021 sous l'égide de la Directions des finances avec des représentants de la Chancellerie d'Etat, du SITel et du Service de législation. En cours d'année 2022, dans le cadre des réflexions et nouvelles attributions liées au programme gouvernemental 2022-2026, la DSJS a été amenée à jouer un rôle prédominant en matière de sécurité de l'information. Pour cette raison, le groupe de travail s'est étoffé de membres issus de cette Direction qui ont apporté leur contribution au texte proposé.

Le groupe de travail a commencé par passer en revue les normes en vigueur au plan cantonal en matière de sécurité de l'information et identifier les lacunes qui pourraient exister. Il est ressorti de cet examen que le traitement des données personnelles bénéficie d'un arsenal de règles assez développé avec la loi du 25 novembre 1994 sur la protection des données (LPrD ; RSF 17.1) complétée par le règlement du 26 juin 1999 sur la sécurité des données personnelles (RSD ; RSF 17.15), mais que le traitement des autres informations en main des administrations publiques ne fait pas pour l'heure l'objet de dispositions spécifiques, à l'exception de quelques normes éparses issues de certaines législations sectorielles.

En pratique, le RSD, dont le champ d'application est pourtant formellement limité au traitement des données personnelles, a le plus souvent été appliqué également au traitement de données non personnelles, lorsqu'un besoin de protection était identifié. Il en va de même de la Politique de sécurité des systèmes d'information (ci-après : POSI) édictée en vertu de l'article 14 RSD. La quasi-totalité des dispositions prescrites ne sont en réalité pas des normes taillées spécifiquement pour la sécurité des données personnelles, mais elles relèvent du domaine plus large de la sécurité de l'information. Même si les deux matières sont naturellement unies, il existe néanmoins des différences justifiant qu'elles soient traitées séparément. Alors que la législation sur la protection des données concerne uniquement les données personnelles et tend de façon générale à protéger les personnes contre les traitements abusifs de données les concernant, la sécurité de l'information a pour objet la protection du capital informationnel des pouvoirs public pris dans sa globalité, en tant que ressource stratégique et indispensable au fonctionnement de l'administration.

L'absence d'une législation consacrée à la sécurité de l'information constitue ainsi une lacune qu'il convient de combler. La proposition de règlement mise en consultation constitue de la sorte une législation consolidée sur la sécurité de l'information, qui a vocation à s'appliquer à toutes les informations traitées et conservées par les pouvoirs publics.

3 NÉCESSITÉ DU PROJET ET OPTIONS ANALYSÉES

La proposition de règlement fait suite à la décision prise à la fin de l'année 2018 par le Bureau de la Commission informatique du Conseil d'Etat (remplacé en 2020 par la Délégation du Conseil d'Etat en matière de digitalisation et de systèmes d'information [ci-après : DSI]) de séparer le domaine de la sécurité de l'information de celui de la sécurité des moyens informatiques.

Jusqu'ici, le RSD et l'ancienne ordonnance du 3 novembre 2015 sur la gestion de l'informatique et des télécommunications dans l'administration cantonale confiaient ces deux domaines de manière générale au SITel. Sous réserve de la protection des données personnelle qui constitue un domaine à part confié à l'ATPrDM, on peut ainsi dire que le SITel était de manière générale l'organe principalement responsable de la sécurité de l'information au sein de l'administration. C'est pourquoi le Conseil d'Etat avait attribué à un collaborateur du SITel un cahier des charges en lien avec cette tâche.

Toutefois, le domaine de la sécurité de l'information au sens strict (traitement de données métiers) touche à des aspects qui sortent du périmètre d'action du SITel et sur lesquels ce dernier a peu d'influence. Face à ce constat, le Conseil d'Etat a pris la décision avec l'adoption de l'ordonnance du 28

juin 2021 sur la gouvernance de la digitalisation et des systèmes d'information de l'Etat (RSF 122.96.11), de sortir formellement le domaine de la sécurité de l'information des tâches incombant au SITel. Celui-ci doit se concentrer dorénavant sur la sécurité des moyens informatiques, domaine qui correspond à son cœur de métier (pour la différence entre les deux, se référer aux définitions données à l'article 4 du règlement). C'est ce changement qui a conduit à devoir repenser plus globalement la question de la sécurité de l'information au sein de l'administration.

Au départ, le groupe de travail est parti sur l'option de préparer une ordonnance organisationnelle qui se serait limitée à redistribuer la responsabilité de la sécurité de l'information aux différents échelons ainsi qu'entre les différentes unités spécialisées de l'administration. Cette solution a néanmoins été écartée dans un deuxième temps au profit d'un nouveau règlement consolidé sur la sécurité de l'information mettant non seulement sur pied une nouvelle organisation, mais énonçant aussi un ensemble de règles à suivre pour parvenir à établir un niveau de sécurité appréciable au sein de l'administration. C'est dans ce contexte qu'a surgi l'idée de réactualiser le RSD pour le mettre à niveau conformément aux standards existants et d'étendre son champ d'application à l'ensemble des informations détenues par les pouvoirs publics en l'intégrant dans un nouveau règlement sur la sécurité de l'information (RSI).

La question s'est toutefois posée si le RSI n'aurait pas dû, à l'instar de la nouvelle loi fédérale sur la sécurité de l'information (LSI), prendre la forme d'une loi. Le groupe de travail a toutefois écarté cette solution par souci d'efficience et au motif que les dispositions prévues correspondent essentiellement à des normes d'organisation qui relèvent de la compétence du Conseil d'Etat selon l'article 118 Cst./Fr. Il s'agit par ailleurs d'un domaine hautement technique pour lequel la compétence du Conseil d'Etat est en principe mieux indiquée que celle du Grand Conseil, aussi parce qu'il peut être soumis à des variations et à des besoins d'adaptation rapides. Enfin, plusieurs autres cantons ont procédé de la même manière.

4 PRÉSENTATION GÉNÉRALE DU RÈGLEMENT

La proposition de règlement a pour objectif de redistribuer et de préciser la répartition des responsabilités dans le domaine de la sécurité de l'information par l'introduction d'un nouveau paradigme. Le règlement tend ainsi à séparer le domaine de la sécurité de l'information au sens large – dont la supervision reviendra principalement au ou à la futur-e délégué-e SI et à l'organisation dédiée – de la sécurité des moyens informatiques, qui reste, elle, de la compétence du SITel. La création du poste de délégué-e SI (cf. art. 10) constitue l'une des principales nouveautés introduites par le règlement. Pour faciliter son travail, le règlement prévoit la désignation au sein de l'administration de correspondants et de correspondantes pour les questions de sécurité de l'information et de protection des données (cf. art. 9 al. 2 et 12).

L'organisation ainsi mise en place est expliquée ci-dessous dans le commentaire des articles.

5 MISE EN ŒUVRE DU RÈGLEMENT ET CONSÉQUENCES FINANCIÈRES ET EN PERSONNEL

La réalisation des objectifs visés par le règlement engendrera des coûts financiers et en personnel pour les unités administratives, qui ne sont pas négligeables. Mais ces conséquences ne doivent pas être surévaluées : d'une part, le règlement ne fait que formaliser des objectifs largement partagés dont personne ne saurait raisonnablement remettre en question le caractère indispensable et qui figuraient déjà pour l'essentiel dans l'actuel RSD ; d'autres part, les efforts requis sont infiniment moindres en comparaison avec les conséquences qui résulteraient d'incidents de sécurité paralysant

la poursuite des activités d'une ou plusieurs unités administratives et/ou mettant en danger les droits fondamentaux des citoyens et des citoyennes du canton.

Quoi qu'il en soit, le plus gros du travail reviendra au ou à la futur-e délégué-e SI dont le poste sera spécialement créé par l'entrée en vigueur du règlement. Au vu de l'ampleur de la tâche (cf. art. 10 ss), 1 à 2 EPT devront être débloqués pour cette fonction, l'ajout d'un 2ème EPT étant actuellement à l'étude. Ces EPT seront attribuées à la Direction qui deviendra responsable de la sécurité de l'information, à savoir la DSJS. Dans la pratique, le SITel qui était jusqu'alors responsable de la sécurité de l'information au sein de l'administration sera dorénavant déchargé des tâches liées à la sécurité de l'information. Dans la mesure où le Conseil d'Etat avait précédemment attribué à un collaborateur du SITel un cahier des charges en lien avec cette tâche, un transfert de poste entre le SITel et la DSJS devra être analysé.

Comme expliqué, le SITel sera pour sa part déchargé de ses tâches liées à la sécurité de l'information au sens large pour mieux se concentrer sur la sécurité des moyens informatiques. Il sera cependant appelé à collaborer étroitement et régulièrement avec le ou à la délégué-e SI dans de nombreuses tâches. Il reste également chargé d'implémenter concrètement les mesures techniques de sécurité décidées dans les moyens informatiques utilisés par l'administration et de veiller à leur efficacité. Le règlement lui impose dans cette perspective d'établir différents niveaux de sécurité adapté à la sensibilité des systèmes d'information et des informations traitées, et de prévoir des mesures spécifiques pour les infrastructures et les ressources jugées critiques. Il paraît néanmoins difficile, sinon impossible, de chiffrer à ce stade quelles seront les conséquences financières des solutions techniques qui devront être mises en œuvre afin de renforcer la sécurité des systèmes d'information de l'administration. En référence à la jurisprudence du Tribunal fédéral, on peut néanmoins ici préciser que ce type de dépenses est généralement considérées comme appartenant à la catégorie des dépenses liées les soustrayant aux règles relatives au referendum financier (arrêt du TF 1P.722/2000 du 12 juin 2001, consid. 3b).

Les Directions devront, pour leur part, désigner en leur sein au moins un correspondant ou une correspondante pour toutes les questions liées à la sécurité de l'information, capable d'assister en première ligne leur secrétariat général et les unités administratives subordonnées. A noter ici que cette charge pourra toutefois être partagée avec celle des correspondants et des correspondantes à la protection des données que l'avant-projet de loi sur la protection des données est sur le point d'introduire. Ces personnes recevront une formation appropriée au sein d'un réseau spécialement créé pour l'occasion et bénéficieront dans ce cadre d'un accès direct au ou à la délégué-e SI, ainsi qu'au ou à la préposé-e à la protection des données. Sachant que les deux fonctions sont très proches, elles pourront, en effet, être cumulées par une seule et même personne.

La charge de travail supplémentaire résultant de l'introduction d'un correspondant ou d'une correspondante à la sécurité de l'information est estimée à 0.25 EPT par Direction, plus la Chancellerie et le pouvoir judiciaire.

Parallèlement, il est clair qu'un effort d'information et de formation devra être fait lors de l'entrée en vigueur du règlement. Cet effort sera partagé entre le ou la futur-e délégué-e SI, le SITel, l'ATPrDM et le Service du personnel et d'organisation (ci-après : le SPO).

6 CONFORMITÉ AU DROIT SUPÉRIEUR ET EURO-COMPATIBILITÉ

Les dispositions prévues dans le règlement se rapportent pour l'essentiel au domaine de l'organisation pour lequel la Constitution fédérale reconnaît que les cantons sont autonomes (cf. art. 47 al. 2 Cst.). La Constitution cantonale prévoit pour sa part que ce type de règles est de manière générale

de la compétence du Conseil d'Etat (cf. art. 118 Cst./Fr). Le règlement est ainsi conforme à la Constitution fédérale et à la Constitution cantonale du point de vue du droit de l'organisation.

Les règles prévues ne portent pas atteinte aux règles de la protection des données au niveau européen mais, au contraire, les précisent et les renforcent. L'indépendance de l'autorité chargée de la protection des données n'est pas non plus remise en question par le présent règlement, celle-ci conservant, en effet, l'ensemble de ses prérogatives concernant le traitement des données personnelles. Il n'y a donc aucune incompatibilité avec les engagements internationaux de la Suisse.

7 COMMENTAIRE DES ARTICLES

Article 1 Objet

Il ressort de l'article 1 al. 1er que le RSI ne porte pas uniquement sur la sécurité des informations en tant que telles, mais sur l'ensemble des processus et des moyens par lesquels cette information est traitée.

La notion de sécurité de l'information repose, de manière générale, sur les normes reconnues. La sécurité de l'information englobe donc toutes les mesures techniques et organisationnelles visant à protéger l'intégrité, la disponibilité, la confidentialité, la traçabilité, la pérennité et la résilience des informations (cf. art. 5 al. 1). Ces mesures peuvent porter tant sur la sécurité des traitements que des moyens nécessaires à ceux-ci. La sécurité de l'information englobe toutes les procédures de traitement, qu'elles soient électroniques ou analogiques et couvre également la sécurité des données personnelles au sens de l'article 22 LPrD ou d'autres lois imposant une protection de l'information.

La sécurité de l'information n'est pas une fin en soi. Elle sert la capacité des pouvoirs publics de décider, d'agir et d'exécuter les tâches que la Constitution et les lois leur commandent d'accomplir, ce qui justifie les mesures énoncées à l'alinéa 2.

Article 2 Champ d'application

Idéalement, le règlement devrait s'appliquer le plus largement possible pour assurer un niveau de sécurité cohérent, peu importe l'auteur du traitement, de toutes les informations qui servent à l'accomplissement d'une tâche publique. Cela inclut donc en premier lieu les organes de l'administration cantonale ainsi que les particuliers et les organes d'institutions privées, lorsqu'ils accomplissent des tâches de droit public. Cette formule permet de s'aligner sur le champ d'application de la LPrD.

Le règlement tient cependant compte de certaines particularités :

- Il existe au sein de l'Etat certaines institutions qui sont autonomes du point de vue de la gestion de leur informatique. Ces institutions seront tenues d'appliquer les règles matérielles prévues par le règlement en matière de sécurité de l'information ainsi que la PGSI, mais conserveront leur autonomie d'organisation. Elles auront néanmoins l'obligation de mettre sur pied une organisation dédiée à la sécurité de l'information et de désigner une personne responsable de la sécurité de l'information (al. 2).
- Comme il est un acte du Conseil d'Etat, le règlement ne peut en principe pas être imposé tel quel au Grand Conseil ou au Pouvoir judiciaire pour des raisons liées à la séparation des pouvoirs. En principe, seule une loi votée par le Grand Conseil permettrait d'atteindre un tel résultat (sur le choix d'adopter un règlement, cf. § C ci-dessus *in fine*). Etant donné que le sujet de la sécurité de l'information concerne indistinctement l'ensemble des trois pouvoirs, le Conseil d'Etat part de l'idée que les organes concernés reprendront volontairement les règles prévues

que ce soit intégralement ou en partie. Cela se fera au moyen de conventions passées avec le pouvoir exécutif (al. 3).

L'alinéa 4 institue une réserve qui permet d'élargir, de restreindre ou de préciser le champ d'application du présent règlement en fonction d'autres lois adoptées au niveau fédéral ou cantonal.

Article 3 Application aux communes

Afin de préserver l'autonomie communale, tout en leur permettant d'accéder à des ressources mises à disposition par l'Etat, de telles situations seront réglées au moyen d'une convention passée avec les communes. Pour le reste, les communes peuvent en tout temps se référer à la PGSI qui sera librement accessible (cf. art. 18 al. 3).

Article 4 Définitions

Les définitions proposées servent à mettre un sens sur des termes techniques qui apparaissent à plusieurs endroits du règlement. Elles correspondent aux standards reconnus dans le domaine de la sécurité de l'information. Même si le texte retenu peut légèrement varier, le contenu des définitions s'aligne sur celui de la famille des normes applicables au management de la sécurité de l'information (ISO 27000 ss).

Article 5 Responsabilités

Cette disposition consacre le principe selon lequel tout organe qui détient et traite de l'information en est responsable (al. 1). Cela n'empêche cependant pas la création d'une organisation de gouvernance spécialement dédiée à ce thème avec un partage des tâches entre les organes stratégiques, opérationnels et exécutifs.

Il arrive de plus en plus souvent que plusieurs organes traitent conjointement des informations et assument sur celles-ci une responsabilité partagée. Comme cela est déjà exigé par la législation sur la protection des données (cf. art. 17 al. 2 et 19 al. 2 let. *e* LPrD), la répartition des responsabilités devra faire l'objet d'une convention entre les parties impliquées à moins que celle-ci ne ressorte déjà de la loi. La convention définira, en particulier, qui est responsable de quels traitements, sur quel périmètre et à quelles étapes.

Un cas où le partage des responsabilités est établi par la loi et ne nécessite par conséquent pas l'établissement d'une convention est celui qui existe entre l'organe-métier qui collecte et traite de l'information, d'une part, et le SITel qui met à disposition les ressources informatiques pour conserver et utiliser cette information, d'autre part (al. 3). Comme cette co-responsabilité concerne pratiquement l'ensemble des traitements au sein de l'administration cantonale, il a semblé opportun de la fixer directement dans le règlement (cf. ég. commentaire de l'article 13).

Article 6 Conseil d'Etat

Les articles 6 à 17 du règlement sont consacrés à la mise sur pied d'une organisation entièrement dédiée à la sécurité de l'information. Au sommet de cette organisation se trouve le Conseil d'Etat qui assure dans ce domaine un rôle stratégique.

C'est à lui qu'il reviendra de définir les principales orientations liées à la sécurité de l'information et les moyens alloués à ce domaine (al. 1 let. *a* et *c*). Il lui appartiendra aussi d'adopter la PGSI (cf. commentaire de l'article 18) dans laquelle seront énoncées la majeure partie des règles à appliquer en matière de sécurité de l'information (let. *b*).

Enfin, dans la mesure où le ou la futur-e délégué-e SI aura un statut comparable à celui d'un service central, il reviendra au Conseil d'Etat d'approuver son engagement (cf. art. 8 al. 1 let. *d* de loi sur le personnel ; LPers).

Article 7 Direction de la sécurité, de la justice et du sport

La disposition fait mention des attributions de la DSJS en lien avec la sécurité de l'information, puisqu'elle est la Direction qui reprend la charge de cette thématique. C'est elle qui assure le lien principal avec le Conseil d'Etat, en coordination avec la Conférence des Secrétaires généraux.

Article 8 Conférence des secrétaires généraux (CSG)

Organe administratif transversal, la CSG est la mieux placée pour assurer une bonne coordination avec le reste de l'administration sur toutes les questions relatives à la sécurité de l'information. Elle pourra aussi assumer le rôle d'arbitre en cas de divergence de vue entre le ou la délégué-e SI est une Direction par rapport à une question de sécurité de l'information.

Article 9 Directions du Conseil d'Etat

Sous l'empire de l'actuel RSD, les Directions ont jusqu'ici peu été mises à contribution en matière de sécurité de l'information. Avec la proposition de RSI, elles seront notamment obligées d'organiser en leur sein un centre de compétence de première ligne qui sera chargé de veiller au respect des prescriptions de sécurité par les unités subordonnées et au besoin de formation des employés. Les Directions devront en outre planifier leurs besoins budgétaires liés à la sécurité de l'information et résoudre les éventuelles divergences de vues entre une unité subordonnée et le ou la délégué-e SI (al. 1).

Pour permettre la mise sur pied d'un centre de compétence de première ligne, chaque Direction devra nommer au moins un correspondant ou une correspondante pour toutes les questions relatives à la protection des données et à la sécurité de l'information (al. 2). Il s'agit d'une fonction qui pourra être cumulée avec celle de correspondant/correspondante à la protection des données qui sera en principe imposée dans le cadre de la révision totale de la LPrD. Les correspondants et les correspondantes recevront une formation idoine au sein d'un réseau présidé par le ou la délégué-e SI et disposeront d'un accès privilégié soit au ou à la délégué-e SI, soit au ou à la préposée à la protection des données.

Article 10 Délégué-e à la sécurité de l'information – Tâches

Le règlement institue la nouvelle fonction de délégué-e à la sécurité de l'information (délégué-e SI). Il s'agit d'une fonction exigeante, conjuguant une maîtrise des outils technologiques à des qualités de communicateur, de stratège, d'auditeur, de formateur, de manager et de coordinateur. Une connaissance de base du cadre juridique est également requise.

La proposition de règlement décrit quelques-unes des tâches principales qu'aura à accomplir le ou la future délégué-e SI (al. 2). En pratique, il faut néanmoins s'attendre à un cahier des charges largement plus conséquent. De manière schématique, on peut néanmoins dire que le ou la délégué-e SI devra être en mesure non seulement d'élaborer et mettre à jour la PGSI, mais également d'identifier les nouveaux risques, de planifier et d'assurer le suivi de la mise en place des mesures de prévention, de détection et de corrections prescrites pour faire face à un (éventuel) incident de sécurité et, surtout, de conseiller et de sensibiliser l'ensemble des acteurs à tous les échelons de l'administration

de manière à ce que chacun puisse acquérir les bons réflexes, soit par la publication de directives, soit par des actions directement sur le terrain.

Le ou la futur-e délégué-e SI sera intégré-e directement au secrétariat général de la DSJS. Toutefois, dans l'exercice de ses fonctions, c'est le Conseil d'Etat qui lui donne ses instructions. La DSJS assumera ainsi, s'agissant de la sécurité de l'information, le rôle d'un service central.

Article 11 Délégué-e à la sécurité de l'information – Collaboration

Le ou la futur-e délégué-e SI n'a pas pour vocation de devenir un nouvel organe de contrôle ou de surveillance à proprement parler comme c'est le cas, par exemple, de l'ATPrDM à qui la LPrD attribue de telles fonctions. La personne désignée ne disposera ainsi pas de compétences décisionnelles ; il n'est pas non plus prévu qu'elle puisse rendre des recommandations ouvrant la voie à un contrôle judiciaire comme c'est le cas dans l'actuelle LPrD.

En revanche, le ou la délégué-e SI sera appelé à collaborer et à échanger des informations à tous les échelons de l'administration. S'il constate des lacunes en matière de sécurité de l'information auprès d'une unité administrative et que cette dernière ne prend pas volontairement les mesures destinées à y remédier, le ou la délégué-e SI pourra en rendre compte auprès de la Direction concernée (cf. art. 9).

Pour faciliter le travail du ou de la délégué-e SI, le règlement prévoit qu'il ou elle pourra demander (et obtenir) auprès des responsables du fichier/traitement et des autres organes de l'administration les informations utiles à l'accomplissement de ses tâches, sans possibilité de lui opposer le secret de fonction. Cela équivaut dans les faits à lui octroyer un pouvoir d'investigation, nécessaire à la conduite de ses activités.

Article 12 Réseau des correspondants et des correspondantes à la sécurité de l'information et à la protection des données

Même si chaque organisation a ses particularités propres, un niveau homogène de sécurité ne peut être atteint qu'à la condition de développer une compréhension commune et des pratiques partagées au sein de l'administration. En raison de leur statut, les correspondants et correspondantes, regroupés au sein d'un réseau, auront une bonne connaissance de la situation et des problèmes de sécurité de l'information dans leur domaine de compétence, notamment quant à l'applicabilité et à l'efficacité des prescriptions et mesures prises. Le réseau s'occupera principalement de la coordination transversale de l'exécution et de l'évaluation des normes proposées. Il pourra aussi contribuer à l'identification des risques et des mesures préventives qui s'imposent.

Le réseau sera présidé par le ou la futur-e délégué-e SI.

Article 13 Service de l'informatique et des télécommunications

Avec l'adoption du RSI, le SITel se concentrera dorénavant sur la sécurité des moyens informatiques qu'il gère et/ou qu'il met à disposition des bénéficiaires. Concrètement, cela signifie que le SITel est responsables de la sécurité des serveurs, des réseaux internes et externes de l'administration, des applications et des appareils avant, pendant et après leur mise en exploitation, mais uniquement par rapport au produit lui-même – peu importe qu'il soit matériel ou immatériel – et à ses composants. Le SITel n'endosse, en principe, pas de responsabilité par rapport aux traitements accomplis par les bénéficiaires de ces produits.

Article 14 Service du personnel et d'organisation

Le Service du personnel et d'organisation (ci-après : SPO), au titre de service central de l'administration, joue un rôle important dans le cadre de la digitalisation non seulement pour accompagner ou conseiller les unités administratives dans leur transformation, mais également pour concevoir et coordonner le développement de compétences nécessaires.

Article 15 Autorité de la transparence, de la protection des données et de la médiation

L'ATPrDM est l'autorité spécialisée du canton dans les questions de protection des données personnelles. Le présent règlement n'influe en rien sur les compétences et les prérogatives de l'Autorité, qui restent inchangées. Sous réserve de l'intégration du RSD dans le RSI, le principal changement apporté par le règlement est la création pour l'Autorité d'un interlocuteur de choix en la personne du ou de la délégué-e SI. En outre, la participation du ou de la préposé-e à la protection des données au réseau des correspondants et correspondantes à la protection des données et à la sécurité de l'information sera, en principe, aussi imposée par la LPrD révisée.

Article 16 Unités administratives

Bien que situé en bout de chaîne, la responsabilité principale de la sécurité des informations incombe en premier lieu à l'organe qui les traite, c'est-à-dire principalement au service ou à l'établissement. Les accords sur la répartition des responsabilités en cas de traitements conjoints sont réservés (cf. art. 5 al. 2).

Les alinéas 1 et 2 précisent les conséquences de cette responsabilité : nécessité d'une évaluation des risques et prescription des mesures techniques et organisationnelles adéquates conformément aux articles 23 à 27 et à la PGSI, contrôle de l'application de ces mesures et formation du personnel.

Article 17 Utilisateurs et utilisatrices

Dernier maillon de la chaîne de sécurité, les utilisateurs et les utilisatrices se doivent d'avoir un comportement exemplaire dans la manière dont ils traitent les informations auxquelles ils ont accès.

Le champ d'application du règlement étant essentiellement limité aux organes et au personnel de l'administration, si des tiers externes sont engagés et qu'ils ont accès à des systèmes d'information de l'Etat, le responsable du fichier/traitement devra s'assurer au moyen d'un contrat qu'ils respectent et appliquent les règles de sécurité en vigueur (al. 2). Des modèles de contrats pourront, au besoin, être établis par le ou la futur-e délégué-e SI.

Article 18 Politique générale de sécurité de l'information de l'Etat – Principes

La PGSI est appelée à devenir l'instrument principal de la sécurité de l'information au niveau du canton. Elle regroupera l'essentiel des comportements à adopter concernant la sécurité de l'information par les unités administratives et les employé-e-s conformément aux principes énoncés (al. 2). Même s'il ne s'agit pas d'un acte législatif, son adoption par le Conseil d'Etat rendra son contenu obligatoire pour l'ensemble des organes soumis au pouvoir exécutif du Conseil d'Etat, sous réserve des dérogations autorisées conformément à l'article 21. Elle peut aussi être rendue obligatoire dans certains cas particuliers prévus par le règlement (p. ex. : art. 20) ou si un contrat le prévoit. La PGSI sera mise à la disposition de chaque organe de l'Etat comme de chaque employé-e et publiée sur Internet (al. 3).

Article 19 Politique générale de sécurité de l'information de l'Etat – Contenu

Cette disposition fixe dans les grandes lignes le contenu de la PGSI (al. 1 et 2), précisant que celle-ci n'est pas un instrument figé. Les modifications successives de la PGSI seront proposées par le ou la futur-e délégué-e SI (cf. art. 10 al. 2 let. *b*), préavisées par la Direction de la sécurité, de la justice et du sport (cf. art. 7 al. 1 let. *b*) puis finalement adoptées par le Conseil d'Etat (cf. art. 6 al. 1 let. *b*).

Article 20 Politique générale de sécurité de l'information de l'Etat – Application aux communes

L'application de la PGSI aux communes, lorsqu'elles accèdent à des systèmes d'information du canton, est indispensable si on veut éviter une rupture dans la chaîne de sécurité.

Article 21 Directives sectorielles relatives à la sécurité de l'information

Il peut arriver que certains secteurs requièrent l'adoption de règles plus spécifiques en matière de sécurité de l'information et de protection des données. Dans ce cas, les Directions et les unités autonomes sont habilitées à édicter leurs propres règles au moyen de directives (al. 1). On peut citer à titre d'exemples les Directives du 28 mars 2018 de la DICS (aujourd'hui DFAC) relatives à l'utilisation d'Internet et des technologies numériques dans le contexte scolaire ou les directives du 27 avril 2009 sur la durée de conservation et l'élimination des données de police (RSF 551.181) de la DSJ (aujourd'hui DSJS). Au besoin, ces directives pourront déroger sur des aspects spécifiques à la PGSI (al. 2). Lors de l'élaboration d'une directive sectorielle, il sera obligatoire de consulter le ou la délégué-e SI ainsi que le ou la préposé-e à la protection des données (al. 3). Ne sont concernées ici que les directives adoptées par une Direction à destination de ses unités subordonnées, mais pas les directives internes propres à une unité administrative.

Article 22 Chartes de service relatives à la sécurité de l'information

Les services auront la possibilité, s'ils le jugent utile, d'édicter des chartes relatives à la sécurité de l'information et la protection des données à l'attention du personnel. Des modèles de charte seront mis à disposition par le ou la futur-e délégué-e SI. Ces chartes ne pourront cependant pas déroger aux autres règles fixées que ce soit au niveau de la PGSI ou d'une directive sectorielle.

Article 23 Evaluation des risques

L'évaluation des risques consiste à identifier pour chaque facteur de risque pertinent (disponibilité, intégrité, confidentialité, traçabilité, pérennité, résilience) les vulnérabilités sous-jacentes et leurs conséquences possibles pour être en mesure d'y apporter les correctifs les plus adaptés. En plus d'identifier les risques et les correctifs possibles, l'évaluation des risques doit aider les responsables du fichier/traitement à mieux apprécier la nature de leur patrimoine informationnel, les processus métiers et les ressources technologiques critiques. Le ou la futur-e délégué-e SI recommandera une méthode à suivre standardisée pour l'évaluation des risques.

Article 24 Définition des mesures

Sur la base de l'évaluation des risques, le responsable du fichier/traitement fixera les mesures de sécurité adaptées à ses activités et à la sensibilité des informations traitées (al. 1). La liste des mesures possibles ainsi que la manière de les appliquer seront détaillées dans la PGSI. Comme la disposition l'indique, il peut s'agir tant de mesures techniques ou organisationnelles, qu'informatiques ou

analogiques. De manière générale, on distingue usuellement entre les mesures qui visent à la diminution des risques d'atteinte (mesures préventives) et les mesures qui tendent à atténuer les suites d'une atteinte (mesures correctives).

Article 25 Conception et évolution

Le principe de sécurité dès la conception « *security by design* » signifie que les responsables du fichier/traitement qui veulent démarrer un nouveau traitement doivent penser dès les premières phases de la mise en place du traitement aux impératifs de sécurité. Cela inclut notamment la prise en compte des coûts liés aux mesures de sécurité.

Article 26 Risques résiduels

Même connus, certains risques ne peuvent pas être écartés ou seulement insuffisamment. Ils peuvent néanmoins être acceptés sur la base d'une pesée de tous les intérêts en présence. La disposition indique la procédure à suivre par rapport à ce type de situation. Elle est reprise en grande partie de l'article 14*d* al. 2 et 3 de l'ordonnance fédérale sur les cyberrisques (OPCy ; RS 120.73).

Article 27 Réévaluation périodique

Le besoin de réévaluation est une constante dans le domaine de la sécurité des technologies de l'information.

Article 28 Classification des informations – Principes

L'attribution d'un degré de confidentialité aux différentes catégories d'informations conservées constitue un standard de la sécurité de l'information. L'attribution concerne en principe un dossier dans son ensemble ; néanmoins, des catégories de classification différentes peuvent être appliquées à l'intérieur d'un même dossier si le besoin de protection diffère d'un document à l'autre.

La classification proposée s'aligne de manière générale sur les standards reconnus en la matière. La solution retenue part du principe que toute information en main des pouvoirs publics est toujours digne de protection, mais qu'elle n'est pas forcément publique. Le règlement propose dès lors de nommer désormais cette catégorie « non-classifiée ».

Le degré de confidentialité des données influe notamment sur la définition des mesures techniques et organisationnelles (art. 29 al. 1 et 39 al. 1) sur la détermination des autorisations d'accès (art. 29 al. 2 ; 30 al. 1 let. *b* et 32 al. 1) et sur les précautions à prendre en cas de destruction (art. 35 al. 2).

Article 29 Informations confidentielles ou secrètes

Dans le domaine de la sécurité de l'information, les termes confidentiel et secret ont un sens propre qui ne correspond pas nécessairement à celui de la LPrD ou des autres règles en matière de secret (cf. comparaison art. 13 LSI). L'élément déterminant de cette classification qui sera précisée dans la PGSI est le potentiel de nuisance résultant d'un accès non autorisé.

S'agissant des mesures de sécurité renforcées qui sont prévues, il s'agit à l'alinéa 1er principalement du chiffrement des données et à l'alinéa 2 de la détermination des autorisations d'accès.

Article 30 Authentification et contrôles des accès

La sécurité des systèmes d'information de l'Etat et des applications est assurée par un dispositif de contrôle se situant au niveau de leur admission. Il faut premièrement que les utilisateurs et utilisatrices soient « authentifiés » (al. 1 let. *a*) et, secondement, que leurs accès soient limités aux applications et aux données dont ils ont besoin pour l'accomplissement de leur tâche (al. 1 let. *b*). Dans certains cas, il peut s'avérer nécessaire de prévoir un système de contrôle des accès supplémentaire au niveau des dossiers. Concrètement, cela revient à déterminer quels sujets ou systèmes auront accès à quels objets, dans quelle mesure, dans quelles conditions, quand et pendant combien de temps.

Article 31 Journalisation

La journalisation des traitements est une mesure de sécurité permettant une reconstitution des opérations accomplies préalablement à la survenance d'un incident de sécurité. Il s'agit alors plus d'une mesure de sécurité des systèmes d'information et des applications que d'une mesure visant à assurer la confidentialité des informations. La journalisation peut également être ordonnée afin de renforcer les mesures destinées à protéger la confidentialité des données par un contrôle postérieur des traitements effectués sur un système d'information. L'étendue et la fréquence des journalisations dépendent des circonstances.

Cela étant, il convient de relever que la journalisation constitue un traitement de données personnelles et qu'il est susceptible de causer une atteinte aux droits des utilisateurs et des utilisatrices. C'est pourquoi un renvoi est opéré vers la LPrD de même qu'un rappel concernant la déclaration des traitements/fichiers (al. 2). Des instructions supplémentaires seront données dans la PGSI, notamment sur la question de la protection des données (al. 3).

Article 32 Procédure d'appel

L'article 21 RSD sur la procédure d'appel (cf. article 4 al. 1 let. *f*) est pratiquement la seule disposition du règlement qui se rapporte exclusivement au domaine de la protection des données personnelles. Pour cette raison, il ne devrait en principe pas être intégré dans le présent règlement sur la sécurité de l'information. Comme le RSD sera abrogé, cela a toutefois été fait à titre provisoire jusqu'à ce que la LPrD dispose de sa propre législation d'exécution. Lorsque ce sera le cas, cet article sera supprimé du RSI et déplacé vers l'acte idoine.

Article 33 Appareils privés

Avec l'essor de l'usage d'appareils privés à des fins professionnelles, il existe un besoin évident de règles dans ce domaine. Trop spécifiques, les mesures à prendre seront précisées dans la PGSI (cf. art. 18 et 19) ou pourront aussi faire l'objet de directives sectorielles (cf. art. 21).

Article 34 Systèmes d'information transversaux ou ouverts au public

L'audit de sécurité dont il est question peut soit être un audit interne, soit un audit externe en fonction des compétences et des ressources disponibles et/ou de la criticité des systèmes d'information concernés.

Article 35 Archivage et destruction

Les informations qui ne se rapportent plus à des affaires en cours et qui font l'objet d'un préarchivage (les archives courantes et intermédiaires au sens de la législation sur l'archivage) continuent de devoir être sécurisées et protégées (al. 1). Dans la mesure où ces informations sont conservées par les services et établissements, ces derniers demeurent responsables de la sécurité.

La destruction des documents contenant des informations confidentielles ou secrètes présente des particularités non seulement lorsqu'il s'agit de documents sur papier (nécessité d'un destructeur de documents) mais également et surtout lorsqu'il s'agit de documents sur support informatique : le simple effacement des données n'est souvent pas suffisant pour assurer l'exclusion de toute possibilité de reconstitution et d'autres mesures doivent être envisagées (al. 2). Des précisions seront apportées à ce sujet dans la PGSI.

Article 36 Protection des locaux et du matériel informatique

La sécurité de l'information ne se limite pas au domaine de l'informatique mais s'étend aussi au monde physique et analogique.

Article 37 Incidents de sécurité

Seuls les incidents qui atteignent les critères fixés sont concernés par cette disposition ; cela exclut les incidents de peu d'importance qui n'ont pas d'impact réel sur les activités d'une unité administrative (cf. définition à l'article 4 al. 1 let. *e*).

La gestion des incidents a pour objectif la détection et le traitement des incidents tant avant, pendant, qu'après leur survenance. Le suivi (« *reporting* ») et la capitalisation (« *bilan* ») sont aussi des éléments importants. Tout cela sera précisé dans une directive idoine (cf. al. 1 et 2).

La consultation de l'ATPrDM dans la phase d'élaboration de la directive (cf. al. 3) doit permettre d'assurer la coordination avec la LPrD révisée, laquelle devrait en principe également traiter cette question.

Article 38 Directive de sécurité des moyens informatiques

En charge de la sécurité des moyens informatiques et principal fournisseur de ces moyens à l'intérieur de l'administration, le SITel établira une directive qui fixera les standards et les normes minimales applicables, et réglera les modalités de leur mise en œuvre et de leur contrôle pour l'ensemble de l'administration (al. 1 et 2). Dans le cas où les responsables du fichier/traitement doivent accomplir certaines opérations eux-mêmes en raison de leur accès immédiat à ces moyens lorsqu'ils sont en leur possession, le SITel communiquera aux personnes responsables les instructions à suivre (al. 3).

Article 39 Niveaux de sécurité

Les moyens informatiques répondent de manière générale à deux niveaux de sécurité distincts : standard et renforcé. Chaque niveau entraîne l'application d'office d'un certain nombre de mesures de sécurité prédéfinies. L'application de l'un ou l'autre niveau dépend de différents critères tenant compte tant des besoins de protection de la confidentialité, de la disponibilité, de l'intégrité, de la traçabilité, de la pérennité ou de la résilience des informations que de la criticité du déroulement adéquat et sans retard des processus d'affaire soutenus par le moyen informatique.

La catégorie de sécurité « protection standard » s'applique aux moyens informatiques ne devant pas satisfaire à des exigences particulières de protection. La grande majorité des systèmes d'information de l'administration cantonale devrait relever de cette catégorie de sécurité. Les données personnelles, les informations classifiées « internes » et d'autres informations dont la confidentialité doit être protégée, mais qui ne requièrent pas une protection particulièrement élevée, peuvent être traitées par les moyens de cette catégorie.

Les moyens informatiques sont classés dans la catégorie « protection renforcée » lorsque l'utilisation abusive des informations qu'ils servent à traiter ou du moyen informatique lui-même est susceptible de causer un préjudice considérable en portant atteinte aux intérêts supérieurs de l'Etat. Sont concernés les moyens informatiques servant au traitement d'informations classifiées « confidentielles » ou « secrètes ». Lorsqu'un moyen informatique soutient un processus d'affaires dont la défaillance ou la perturbation peut entraver considérablement la marge d'action d'une autorité, le moyen informatique devrait également être classé dans cette catégorie.

L'alinéa 3 réserve les infrastructures et les applications critiques, dont la liste est établie par le Conseil d'Etat. Il prévoit une sorte de 3e niveau composé de mesures de sécurité « sur mesures » prévues pour répondre aux besoins particuliers de ces systèmes.

Article 40 Mesures techniques de sécurité

La définition des mesures standardisées de sécurité propres aux niveaux standard et renforcé est de la compétence comme de la responsabilité du SITel dont c'est le métier (al. 1). Ces mesures sont valables pour l'ensemble des unités administratives de l'Etat sous réserve des infrastructures et des applications critiques (cf. art. 39 al. 4).

De manière régulière, le SITel devra s'assurer que les mesures de sécurité prévues pour le niveau de sécurité renforcé fassent l'objet d'une évaluation permettant de confirmer qu'elles soient toujours en phase avec l'état de la technique (al. 2 en lien avec l'article 27).

Article 41 Procédure en cas de désaccord

Le règlement prévoit une procédure pour le cas où il existerait un désaccord entre l'organe bénéficiaire et le SITel sur le niveau de sécurité à attribuer à un système d'information ou une application. Ce type de désaccord pourra être soumis directement à la DSI qui tranchera.

Article 42 Collaboration dans le domaine de la sécurité de l'information

L'échange d'informations et d'expériences est essentielle en matière de sécurité de l'information. Il existe en Suisse plusieurs pôles de compétence dans ce domaine que ce soit à l'échelon de la Confédération ou des autres cantons. Il importe que le canton de Fribourg puisse également participer aux discussions qui ont lieu au sein de ces structures.

Autres modifications

A titre liminaire, il sied de préciser que l'ordonnance fixant les attributions des Directions du Conseil d'Etat et de la Chancellerie d'Etat (OADir) doit être modifiée, dans la mesure où la DSJS reprend en tant qu'attribution qui lui est propre la sécurité de l'information.

Les autres modifications apportées consistent dans des adaptations terminologiques.