PAR E-MAIL UNIQUEMENT
Direction de la sécurité, de la justice et du sport
Grand-Rue 27
Case postale
1701 Fribourg

Fribourg, le 5 février 2023

Règlement sur la sécurité de l'information – Consultation

Monsieur le Conseiller d'Etat,
Mesdames, Messieurs,

Nous avons pris connaissance avec grand intérêt du projet de règlement sur la sécurité de l'information.

Nous saluons dans l'ensemble ce règlement sur la sécurité de l'information. Avec la forte augmentation des cyber-attaques, il est absolument nécessaire d'avoir des exigences et une gouvernance claires et mises à jour. L'institution d'une organisation dédiée à la sécurité de l'information et surtout d'un délégué dédié sont également des points très positifs. La coordination des tâches transversales et surtout une application de l'état de l'art pourront être mieux garanties. Les principes énumérés font sens et sont conformes aux standards de l'industrie pour faire ressortir les points à la base de la sécurité : confidentialité, intégrité et disponibilité.

Toutefois, la proposition du groupe de travail d'établir un règlement sur la sécurité de l'information et non une loi nous interpelle. Comme indiqué dans le rapport explicatif, le fait de ne pas dipsoser d'une loi-cadre pose un problème pour imposer certaines décisions, en raison du principe de séparation des pouvoirs. La sécurité de l'information est un domaine assez important pour ne pas laisser aux 3 pouvoirs l'application du règlement selon la bonne volonté de chacun. Les questions d'une adaptation rapide et d'un contenu trop technique auraient pu être résolues en créant une loi énumérant les principes essentiels et laissant les détails dans le règlement d'application.

Nous sommes conscients des coûts financiers engendrés par les mesures induites par ce règlement. Mais celles-ci sont nécessaires. Une perte des données ou pire, une corruption de celles-ci, aurait des coûts nettement supérieurs, sans compter l'impact d'une perte de confiance des citoyens.

Nous notons l'absence d'un point essentiel : l'établissement d'un état-major de crise. Ses compétences doivent être assez larges pour prendre la direction totale des opérations IT autant dans les départements que les entités autonomes. Les conditions pour être appelé et refermé, de manière préventive lors d'un risque hautement critique avéré ou de manière réactive à la suite d'un incident majeur de longue durée, doivent également être définies. La composition, le fonctionnement et la collaboration avec les départements ainsi que la nécessité d'exercer par temps calme doivent être établies.

Dans ce contexte, il manque également un concept de gestion et d'attribution des droits d'accès.

Vous trouverez ci-après quelques remarques spécifiques aux articles :

Art. 2. Le fait de laisser les unités autonomes fixer leur propre organisation au niveau des responsables de la sécurité de l'information est compréhensible. Cependant, une application inadéquate de la PGSI crée un risque dans tout le système. Afin de limiter le risque, le délégué SI devrait jouer un rôle de réviseur.

Le Centre Fribourg I Die Mitte Freiburg Beaumont 20, CH-1700 Fribourg
T 079 820 50 92, info@fr.le-centre.ch, www.fr.le-centre.ch, IBAN CH07 0076 8011 0400 3060 5

Art. 7. L'autonomie d'action du délégué SI est un point essentiel à la réussite de ses tâches. Le fait de devoir obtenir l'autorisation préalable du DSJS pourrait poser un problème. Cependant, il est clair que le lancement d'audit et l'attribution à des tiers, vu son aspect financier, doit être validé par la direction.

Art. 9. L'approche décentralisée des tâches opérationnelles dans les directions est certainement un bon moyen d'atteindre les objectifs, pour autant que le délégué SI ait suffisamment d'autonomie et de poids. Le fait de laisser les directions arbitrer les désaccords pourrait poser un problème, même si in fine le désaccord résultant peut ensuite être arbitré par la conférence des secrétaires généraux.

Art. 10. Si les responsabilités entre le SITel et le délégué SI sont définies, leurs frontières ne seront pas toujours étanches. Dans ses tâches, le délégué SI doit se coordonner avec les SITel sur les domaines conjoints afin d'éviter toute zone grise et également mener des actions conjointes. L'art. 11 qui suit ne fait état que de collaboration.

Art 11. L'impossibilité d'opposer un secret de fonction et ainsi offrir un pouvoir d'investigation réel est une proposition que nous soutenons et estimons absolument nécessaire. Il en va de même si le délégué SI demande un audit externe.

Art. 18. Il manque dans la politique générale de sécurité de l'information un concept de gestion et d'attribution des droits d'accès.

Art.19. Le concept de gestion et d'attribution des droits d'accès doit également être intégré dans le contenu de la PGSI.

Art. 21. Le niveau global de la sécurité est défini par son élément le plus faible. Les dérogations à la PGSI sont des risques et elles devraient n'être autorisées que dans des cas très limités. De plus, le délégué SI devrait donner son accord à ces directives sectorielles.

Art.22. Une charte, à l'inverse d'une directive, n'a pas de valeur contraignante. Le risque est d'y intégrer des points qui auraient dû figurer dans la directive sectorielle et ne seront que suivis au bon vouloir des employés. Pour y remédier, il faudrait ajouter que la charte ne peut intégrer que des aspects non essentiels et complémentaires à la PGSI.

Art.24. Le risque est défini selon sa probabilité et son impact ; le risque zéro n'existe pas. Nous soutenons la proposition demandant des mesures proportionnées aux circonstances, techniquement adaptées, économiquement supportables et applicables en pratique.

Art 26. Le fait de trouver une personne qui assume un risque ne réduit en rien sa gravité. C'est même souvent une échappatoire pour ne pas prendre les mesures nécessaires. Ce point est dangereux et ne devrait pas être autorisé. Chaque risque non acceptable, s'il ne peut être corrigé tout de suite, devrait donner lieu à une proposition de mitigation et une planification de correction.

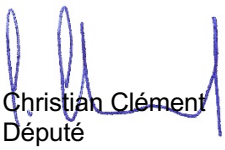
Art. 29. L'organe public doit également déterminer la gestion des droits (validation, attribution, vérification).

Art.33. L'utilisation d'appareils privés est devenue une généralité dans les systèmes d'information. Les nouvelles techniques permettent d'accéder de manière sécurisée à tous les systèmes sans devoir passer par des machines exclusivement gérées par l'Etat. Un de points critiques demeure la confidentialité des données. Aussi le règlement ne devrait autoriser l'utilisation d'appareil privés qu'une fois les mesures techniques et organisationnelles prises pour limiter les accès et l'enregistrement local des documents, selon leur degré de confidentialité.

Art 37. Dans le cadre des incidents de sécurité, un état-major de crise doit être préétabli. Cet état-major peut être appelé à la demande du délégué SI ou d'un département de manière préventive lors de l'établissement d'un risque hautement critique ou à la suite d'un incident majeur de longue durée. De plus, la simple énumération d'une information au public contenue dans une directive nous semble insuffisante. Le règlement devrait clairement faire état des obligations de transparence envers tout le public ou envers les personnes concernées, lors d'incidents ou de fuites d'informations.

En conclusion, nous tenons encore une fois à remercier toutes les personnes qui ont participé à l'élaboration de cet excellent projet. Nous espérons que nos remarques constructives contribueront à son amélioration.

Nous vous adressons, Monsieur le Conseiller d'Etat, Mesdames, Messieurs, nos meilleures salutations.



Christian Clément
Député

Charles Navarro
Secrétaire politique