

Mercredi (matin) 16 septembre 2015

Interpellations de la Direction des finances

76 2015.RRGR.199 Interpellation 060-2015 Streit-Stettler (Berne, PEV) Sécurité informatique de l'administration cantonale

N° de l'intervention: 060-2015
Type d'intervention: Interpellation
Déposée le: 19.02.2015
Déposée par: Streit-Stettler (Berne, PEV) (porte-parole)
Cosignataires: 0
N° d'ACE: 903/2015 du 12 août 2015
Direction : FIN

Sécurité informatique de l'administration cantonale

La protection des données et de l'information revêt une grande importance dans l'administration cantonale, c'est indéniable. L'échange de données se fait aujourd'hui presque exclusivement par la voie électronique. La protection des données passe donc logiquement par la sécurité informatique. On peut dans ces conditions se demander si la surveillance de la sécurité informatique est assurée correctement et de manière indépendante dans l'administration cantonale. Si le Bureau pour la surveillance de la protection des données est bien une autorité indépendante, le délégué à la sécurité informatique du canton (DSI BE) est quant à lui subordonné à la direction de l'OIO et ne peut donc exercer ses importantes fonctions de surveillance que dans une mesure restreinte.

Dans ces conditions, le Conseil-exécutif est prié de répondre aux questions suivantes :

1. L'ordonnance de Direction sur la sûreté de l'information et la protection des données (OD SIPD) prévoit à l'article 10 que le Bureau pour la surveillance de la protection des données collabore avec le DSI BE. Quelles sont les modalités institutionnelles de cette collaboration ?
2. Le Conseil-exécutif pense-t-il que le Bureau pour la surveillance de la protection des données et le DSI BE doivent coopérer étroitement ?
3. En vertu de l'article 11 OD SIPD, les Directions et la Chancellerie d'Etat désignent un ou une responsable de la sécurité informatique (RSI BE) en tant que principale personne de contact du DSI BE. Cette règle est-elle traduite en faits ? Comment fonctionne la collaboration entre le DSI BE et les RSI BE ? Combien qu'équivalents plein temps les Directions ont-elles dégagés ? Toutes les Directions ont-elles un ou une RSI BE ?
4. Que peut faire le DSI BE si une Direction ou un service ne respecte pas ses consignes ?
5. Veille-t-on dans l'administration cantonale aux questions de sécurité quand un nouveau projet informatique est lancé ou une nouvelle application introduite ?
6. L'indépendance du DSI BE est-elle assurée au sein de l'OIO ?
7. Le Conseil-exécutif pourrait-il envisager d'intégrer le DSI BE au Bureau pour la surveillance de la protection des données ?

Réponse du Conseil-exécutif

1. La sûreté de l'information et la protection des données (SIPD) sont des facteurs décisifs de succès dans la mise en œuvre des technologies de l'information et de la communication (TIC). La protection des données (PD) a pour but de protéger les personnes contre les abus dans le traitement des données réalisé par les autorités. La sûreté de l'information (SI) recouvre la confidentialité, la disponibilité et l'intégrité des informations traitées.

Le respect des dispositions sur la protection des données et la sûreté de l'information dans le traitement des données personnelles par l'administration est soumis au contrôle du Bureau cantonal pour la surveillance de la protection des données (BPD), autorité indépendante de

l'administration. En ce qui concerne le traitement de données non personnelles, c'est le ou la déléguée cantonale à la sécurité informatique du canton (DSI BE) de l'Office d'informatique et d'organisation (OIO) qui est chargée de surveiller que la sûreté de l'information est garantie.

La sûreté de l'information et la protection des données dépendent fortement l'une de l'autre : il n'est pas possible de garantir la protection des données si la sûreté de l'information n'est pas assurée. De plus, elles utilisent souvent toutes deux les mêmes mesures pour atteindre efficacement leurs objectifs. Une mise en œuvre performante et conforme aux normes SIPD des projets de l'administration cantonale implique donc une étroite coopération entre le BPD et le ou la DSI BE. C'est pour cette raison que l'ordonnance de Direction sur la sûreté de l'information et la protection des données (OD SIPD) prévoit, à l'article 10, que le BPD travaille conjointement avec le ou la DSI BE, qui l'assiste dans sa tâche de surveillance.

Tous les projets et applications TIC de l'administration cantonale doivent remplir les exigences d'une protection de base standard, quel que soit le degré de protection qu'ils requièrent. Cette protection de base est soumise au contrôle et à la surveillance du ou de la DSI BE. Les projets nécessitant une protection plus poussée font en outre l'objet d'un contrôle préalable du BPD, comme le prévoit l'article 17a de la loi cantonale sur la protection des données (LCPD). Le BPD peut poser cette protection de base comme condition préalable lors de ce contrôle.

Conformément à l'article 6 OD SIPD, les demandes d'autorisation de crédit et les documents destinés au contrôle préalable doivent contenir les documents SIPD élaborés. Lorsque les exigences sont élevées en matière de sûreté de l'information et de protection des données, ces documents doivent être soumis à la fois au BPD et au ou à la DSI BE, qui examinent tous deux si les documents SIPD respectent les dispositions SIPD dans leur domaine de compétence. En l'absence de documents SIPD ou si ceux-ci montrent que la sûreté de l'information ou la protection des données ne sont pas garanties, la mise en service ne peut intervenir qu'après la correction de ces défauts (art. 7 OD SIPD).

2. Oui. Une coopération étroite et constructive entre le BPD et le ou la DSI BE, telle qu'elle existe aujourd'hui, est indispensable pour mettre en œuvre les dispositions SIPD de manière efficace et performante.

Le Bureau cantonal pour la surveillance de la protection des données est une autorité de surveillance indépendante du Conseil-exécutif mais, à notre connaissance, le bureau est également convaincu de l'importance d'une coopération étroite.

3. Les Directions, la Chancellerie d'Etat, les autorités judiciaires (DIR/CHA/JUS) et le Contrôle des finances affectent, selon leurs propres indications, les ressources de personnel suivantes à la fonction de responsable de la sécurité informatique (RSI BE):

Chancellerie d'Etat	3%
Direction de l'économie publique	30%
Direction de la santé publique et de la prévoyance sociale	10%
Administration de la justice	10%
Direction de la justice, des affaires communales et des affaires ecclésiastiques	50%
Direction de la police et des affaires militaires (sans la Police cantonale)	30%
Police cantonale	5%
Direction des finances	50%
Direction de l'instruction publique	40%
Direction des travaux publics, des transports et de l'énergie	35%
Contrôle des finances	2%

Le ou la déléguée cantonale à la sécurité informatique du canton (DSI BE) occupe un poste à plein temps à l'OIO. Le ou la DSI BE et les RSI BE des DIR/CHA/JUS disposent d'un important instrument institutionnel : le groupe de travail Sûreté de l'information de la Conférence informatique cantonale (CIC), qui est l'organe chargé de la conception et de la coordination de l'utilisation des TIC dans l'administration cantonale.

Le groupe de travail Sûreté de l'information, dirigé par le ou la DSI BE, est l'organe spécialisé du canton pour ce qui concerne la sûreté de l'information. Il veille à l'actualisation et à l'exécution des dispositions relatives à la sûreté de l'information, suit l'évolution dans ce domaine et élabore des outils et des consignes en la matière. Les RSI BE des DIR/CHA/JUS sont membres de plein droit du groupe de travail Sûreté de l'information, tandis que le BPD y est représenté à titre consultatif.

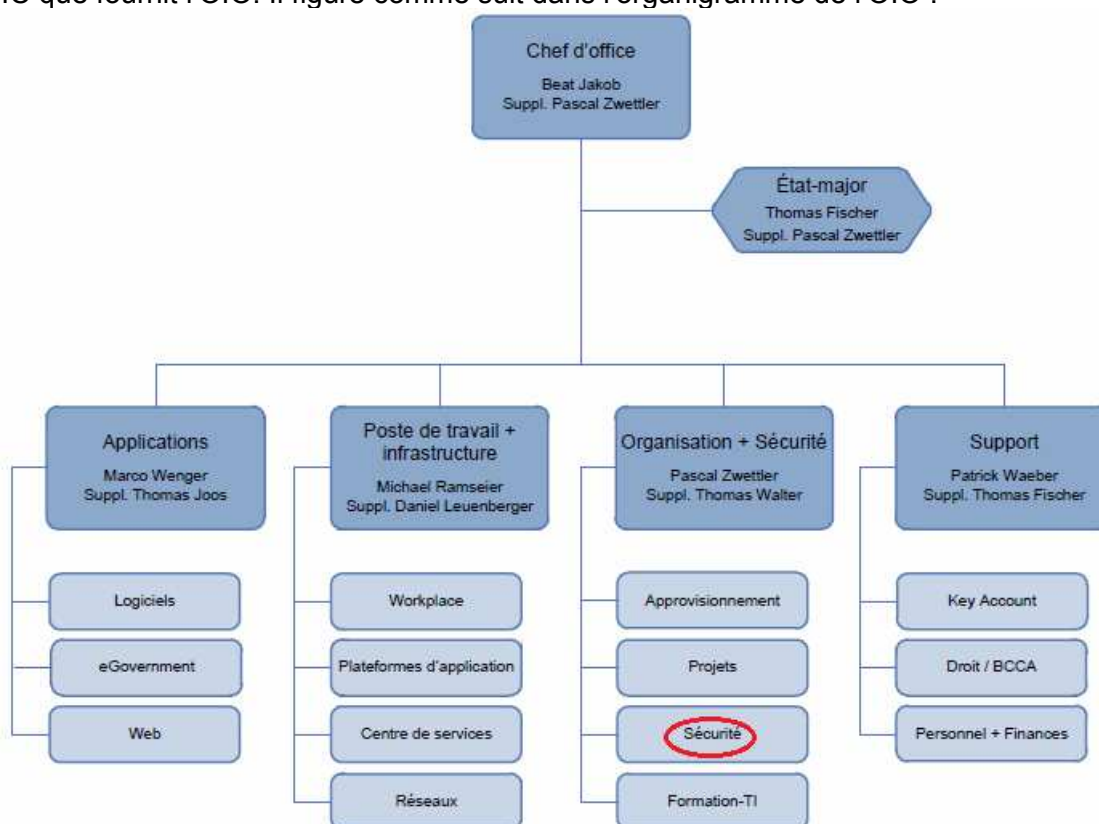
4. Le ou la DSI BE n'est pas habilitée à donner des instructions à l'échelle cantonale. Si une unité administrative n'applique pas les consignes en matière de sûreté de l'information et de protection des données, il ou elle peut le constater lors de l'examen des documents SIPD conformément à l'article 6 OD SIPD ou dans le cadre de son activité de surveillance au sens de l'article 10, alinéa 3 OD SIPD. Il ou elle peut alors en rendre compte à sa hiérarchie ou, en sa qualité de responsable du groupe de travail Sûreté de l'information, à la CIC. Les DIR/CHA/JUS décident des conséquences à en tirer dans le cadre de leurs compétences de direction.

5. L'OD SIPD et la méthode de gestion de projet HERMES prescrite dans l'administration cantonale règlent cette question comme suit :

Le comité de projet de chaque projet TIC désigne un ou une responsable SIPD dans le cadre de l'organisation du projet. Cette personne réalise une analyse SIPD durant la phase d'analyse préliminaire, afin d'évaluer la conformité du projet à la législation sur la protection de données, et détermine à l'aide d'une classification des besoins de protection si le projet présente des exigences poussées en matière de SIPD. Si l'analyse met en lumière des exigences SIPD poussées, un concept SIPD doit être élaboré au plus tard durant la phase de conception. Ce concept comprend une analyse des risques dont découlent les mesures SIPD d'ordre technique et organisationnel à définir.

Les concepts SIPD des projets présentant des exigences SIPD poussées sont soumis pour prise de position au BPD et portés à la connaissance du ou de la DSI BE (art. 6 OD SIPD).

6. Le ou la DSI BE dirige le domaine Sécurité de la section Organisation + Sécurité de l'OIO. Ce domaine spécialisé est chargé de garantir la sûreté de l'information dans les prestations de base TIC que fournit l'OIO. Il figure comme suit dans l'organigramme de l'OIO :



L'implantation de la fonction de DSI BE dans cet office transversal qu'est l'OIO garantit son indépendance par rapport à l'administration cantonale (OIO excepté). Le ou la DSI BE n'est certes pas indépendante vis-à-vis des dirigeants de sa section, de son Office et de sa Direction en raison de sa subordination hiérarchique, mais il ou elle l'est en revanche à l'égard des spécialistes et des cadres assumant la responsabilité opérationnelle des prestations TIC, car ceux-ci appartiennent à d'autres sections de l'OIO ou d'autres offices de l'administration cantonale. De plus, une surveillance indépendante de la sûreté de l'information garantie par l'OIO est déjà assurée par le BPD et le Contrôle des finances, qui disposent également de personnel spécialisé en matière de SI.

7. Il convient à cet égard d'établir une distinction entre les tâches de surveillance du ou de la DSI BE, d'une part, et ses activités de soutien et de direction spécifiques, d'autre part :

La surveillance indépendante de la sûreté de l'information est déjà assurée à l'heure actuelle par le BPD et le Contrôle des finances, dans le cadre des points de contact (très étendus) avec la protection des données et la révisibilité des systèmes TIC. Il serait en principe envisageable, du point de vue du Conseil-exécutif, de modifier la loi pour conférer à l'une de ces autorités de surveillance existantes une mission étendue de contrôle de la sûreté de l'information. Mais du fait de leur indépendance, ces autorités sont aujourd'hui déjà libres de décider dans quelle mesure elles tiennent compte des aspects de la sûreté de l'information dans le cadre de leur activité de surveillance.

Le Conseil-exécutif estime en revanche que les autres tâches du ou de la DSI BE (notamment la direction et la coordination techniques des activités SI de l'administration ainsi que l'élaboration d'outils, de prescriptions administratives et de bases) sont des activités exécutives qui doivent relever de l'administration et non d'une autorité de surveillance. La proximité organisationnelle du ou de la DSI BE avec les personnes et les domaines spécialisés de l'OIO garantit en outre qu'il ou elle est à tout moment en contact direct avec les responsables des installations techniques, de la fourniture des prestations TIC de base du canton ainsi que de la planification et la réalisation des projets TIC. Détacher la fonction de DSI BE de l'OIO au plan organisationnel compromettrait ces facteurs de succès.

Le pilotage et l'organisation des TIC de l'administration cantonale sont actuellement remaniés dans le cadre du le projet IT@BE. Le rôle futur du ou de la DSI BE dépendra donc aussi des résultats de ce projet.