Politique de sécurité de l'information – Projet de directive transversale

Avis du 24 février 2014

Mots clés: projet de directive, protection des données personnelles, sécurité de l'information

Contexte: Par courrier électronique du 29 janvier 2014, la direction de la sécurité de l'information et évènements spéciaux (ci-après DSIES) de la direction générale des systèmes d'information rattachée au département de la sécurité et de l'économie (DES) a soumis pour avis au Préposé cantonal à la protection des données et à la transparence un projet de directive transversale relative à la politique de sécurité de l'information.

Cette directive a pour objectif de répondre à une exigence posée par le règlement sur l'organisation et la gouvernance des systèmes d'information et de communication, du 26 juin 2013, (ROGSIC – B 4 23.03)

Bases juridiques: art. 56 al. 3 let. e LIPAD

Considérations

Le ROGSIC, fondé sur la loi sur l'exercice des compétences du Conseil d'Etat et l'organisation de l'administration, du 16 septembre 1993 (B 4 23.03), est un règlement qui définit le cadre organisationnel des systèmes d'information relatif aux projets informatiques dont le chapitre III concernant la gouvernance comporte une section 4 spécifique à la sécurité de l'information.

L'art. 3 al. 4, lettres h et i, donne les définitions de ce qu'il convient d'entendre par *« sécurité de l'information »* et *« politique de sécurité de l'information »* :

> *h) sécurité de l'information : la protection de la confidentialité, de l'intégrité et de la disponibilité de l'information – en outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité, peuvent également être concernées;*
>
> *i) politique de sécurité de l'information : les intentions et dispositions générales relatives à la sécurité de l'information formellement exprimées par l'Etat de Genève*

L'article 35 renvoie à la définition d'une politique qui doit être publiée sous une forme qui n'est pas définie[1].

> ***Art. 35 Elaboration d'une politique de sécurité de l'information***
> *1 Les principes directeurs de la sécurité de l'information sont déclinés en objectifs et en mesures générales dans une « politique de sécurité de l'information ».*
> *2 La politique de sécurité de l'information doit notamment :*
> *a) constituer le cadre de gouvernance, de référence et de cohérence de la sécurité de l'information au sein de l'administration cantonale;*
> *b) être conforme à la législation et à la réglementation en vigueur;*

[1] En revanche, la notion de directive figure dans le ROGSIC à l'art. 3 al. 3 qui précise que : « *Les ressources matérielles et immatérielles sont précisées dans une directive par la commission de gouvernance des systèmes d'information et de communication (ci-après : la commission) »*.

c) s'appuyer sur des normes internationales reconnues;

d) être en adéquation avec les besoins de l'administration cantonale;

e) définir les responsabilités dans le domaine de la gestion de la sécurité de l'information, traitant en particulier de la remontée d'incidents de sécurité;

f) présenter les besoins de communication, de formation et de sensibilisation.

3 La politique de sécurité de l'information définit également :

a) les règles pour sa mise en œuvre;

b) les mesures et les contrôles;

c) les règles de révision et de mise à jour.

4 Elle est publiée à l'intention de l'ensemble des utilisateurs des systèmes d'information et de communication de l'administration cantonale.

Dans son courriel accompagnant l'envoi de la directive transversale, la DSIES précise notamment qu'il s'agit là du document fondateur duquel découleront *« les directives, procédures et autres guides assurant la mise en œuvre mesurable des principes et règles décrits »* et que ce dernier a d'ores et déjà été validé par le Comité de sécurité de l'information - au sein duquel chaque département est représenté - et le directeur général de la DGSI.

En tant que non spécialiste dans le domaine des technologies de l'information et tout à la fois garant du respect de la protection des données personnelles par l'administration cantonale, le Préposé cantonal a procédé à une lecture attentive du projet de directive transversale qui a été porté à son attention en se demandant :

- d'une part, si les principes directeurs régissant la protection des données ont bien été pris en compte et,
- d'autre part, si toute collaboratrice et collaborateur concerné par ce texte peut être efficacement sensibilisé à ces questions. Dans cette matière technique, chacune et chacun peut, par son comportement au quotidien, contribuer efficacement, ou non, à ce que la sécurité de l'information soit assurée dans l'exercice des tâches.

Conformément à l'art. 56 al. 6 LIPAD, nous nous sommes, en outre, concertés avec l'Archiviste d'Etat, auquel le projet de directive transversale a été transmis.

De cet examen, il apparaît que la directive s'inscrit bien dans le respect des principes relatifs à la protection des données. Cela dit, s'agissant de son volet sensibilisation à l'attention du personnel, nous observons qu'elle est relativement longue (10 pages) surtout si l'on considère le fait qu'elle devrait encore être complétée par d'autres directives et procédures, tel qu'indiqué dans le courriel d'accompagnement. Dès lors, la directive pourrait vraisemblablement être allégée en retirant tous les aspects qui relèvent du simple rappel du cadre existant.

Nous nous permettons ci-après quelques remarques ou suggestions :

Ad point 1 de l'encadré Objet de la directive, plutôt que d' apporter le soutien de la part du Conseil d'Etat, l'objet n'est-il pas, conformément à ce que réclame l'art. 35 du ROGSIC, de définir les objectifs poursuivis par la politique de sécurité de l'information de l'Etat de Genève et les mesures générales à prendre à cet effet ?

Ad 1 But du document : au 1er §, plutôt que de traiter d'« intentions » et de « dispositions générales », il serait préférable de reprendre les termes utilisés par l'art. 35 du ROGSIC d' « objectifs » et de « mesures générales ». Le texte qui dit fixer l'engagement du Conseil d'Etat nous semble donner des indications en faveur d'un instrument d'une autre forme qu'une telle directive transversale. Le Conseil d'Etat est l'autorité qui définit une politique qui est mise en œuvre au travers d'une directive.

Ad 2 Au point 1 comme au point 2 ou encore au point 6, le Conseil d'Etat s'exprime au travers de la directive émanant de l'administration (il « considère », « s'engage » et « démontre sa volonté »). De la sorte, nous nous demandons si le choix de la directive transversale correspond au bon niveau de document ou si cette politique de sécurité de l'information ne devrait pas plutôt être affirmée par le Conseil d'Etat lui-même dans un extrait de procès-verbal à l'attention de l'administration, au vu de l'importance que l'expression de cette politique revêt.

Les notions de « capital informationnel de l'Etat», de ressources « immatérielles » et les cinq critères fondamentaux pourraient être explicités dans un langage plus courant. S'agissant du critère de confidentialité, nous proposons d'ajouter à la fin du § « dans le respect de la protection des données ».

Le terme « parties prenantes » figurant dans le dernier § devrait être remplacé par « collaborateurs et collaboratrices de l'administration cantonale ».

Ad 3 Quant au champ d'application, il serait probablement utile de faire la différence entre le champ d'application personnel et le champ d'application matériel de la directive.

En lieu et place de « ressources », il serait préférable de parler de personnes soumises aux obligations de respecter la politique de sécurité de l'information.

Quant aux personnes qui ne travaillent pas au sein de l'administration cantonale, au plan juridique, la directive ne porte pas d'effets à leur égard. De telles obligations doivent, pour être effectives, découler de clauses contractuelles spécifiques introduites dans les contrats signés avec les entreprises mandatées par l'Etat de Genève.

Ad 4 Dans la mesure où le cadre de référence est précisé dans l'encadré de la page 1, peut-être n'est-il pas vraiment nécessaire de le rappeler également dans ce point.

La dernière phrase du point 4 devrait être supprimée dans la mesure : « En principe, la version ... ».

Ad 5 et 6 Ces deux points constituent le cœur de la politique à mettre en œuvre et la déclinaison qui y figure est précieuse. Il serait probablement intéressant d'y introduire les axes relatifs à la sensibilisation, la formation et l'information des collaboratrices et des collaborateurs qui puissent induire cette défense en profondeur voulue par le gouvernement.

A ce stade, nous comprenons que le dispositif à mettre en place réside beaucoup dans des documents écrits : guide, directive, procédure, certes essentiels mais un accompagnement à l'aide d'une campagne de prévention et de promotion sur le terrain serait bienvenu dans un domaine qui constitue sans aucun doute l'un des défis majeurs à l'heure actuelle.

Le 3^{e} § de la p. 5 est rédigé d'une manière assez complexe et devrait être simplifié. Entre l'Archiviste d'Etat et le Préposé cantonal, sachez que nous n'avons pas la même compréhension dudit §.

Le dernier § de la page 5 qui commence par « Pour chaque document de portée transversale… » est peu explicite. Si nous comprenons bien, l'objectif est de rappeler que chaque département ou service reste libre, dans le cadre du respect de la directive transversale, d'adopter lui aussi ses propres directive et autres procédures. Nous nous demandons s'il ne s'agit pas là d'un rappel général qui n'est pas absolument indispensable dans le cadre de la définition d'une politique de sécurité de l'information.

Au milieu de la p. 6, ne devrait-on pas préciser plus avant ce que l'on entend par « régulièrement », en ajoutant par exemple lors de chaque mise à jour du dispositif de contrôle interne, chaque année au minimum, etc. ?

En haut de la p. 7, quels sont les critères qui permettent de savoir si une procédure est clairement définie ou non ? Faut-il la soumettre préalablement à la consultation du per-

sonnel concerné, le former sur le contenu a posteriori, l'illustrer à l'aide d'exemples concrets ? De même, s'agissant des « bonnes pratiques », qui les déterminent ? Chaque département et service a-t-il les moyens de définir seuls de telles bonnes pratiques ? Ne faut-il pas élaborer au niveau de la DSIE un tel guide de bonnes pratiques.

A la p. 7, au 8e §, il faut distinguer clairement la problématique de l'archivage des données ou des documents, de celle liée aux prestations en ligne, afin d'éviter tout risque de confusion. En effet, la LIPAD et la Larch posent des contraintes légales fortes qui obligent à gérer le cycle de vie des données, soit à prévoir leur destruction à la fin de leur durée d'utilité pour les services ou, au contraire, leur versement aux Archives d'Etat pour leur conservation sur le long terme. Ecrire qu'il s'agit « d'aspects d'archivage » ne traduit pas la réalité de ces contraintes. Les questions liées à l'AeL sont d'une autre nature.

A la p. 8, au 3e § qui commence par "Cette responsabilité impose... », l'on pourrait rajouter les principes gouvernant la protection des données qui manquent (licéité, bonne foi, proportionnalité, finalité, exactitude et reconnaissabilité pour la personne en cause).

A la p. 8, au 4e §, il est mis l'accent sur un problème effectivement très sensible et important qui relève à la fois des outils mis à disposition par l'Etat de Genève et du contexte d'urgence dans lequel le travail doit être réalisé, parfois à l'extérieur du bureau. Les solutions à apporter à ce problème débordent largement du cadre de la présente directive transversale.

A la p. 8, supprimer l'avant dernier § qui n'a pas sa place dans un document émanant des services.

A la p. 9, au dernier § du point 6 qui commence par : « D'autres entités... » préciser en toutes lettres en lieu de place de « préposé », le « Préposé cantonal à la protection des données et à la transparence » et ajouter « les responsables LIPAD des départements et des services ».

Avis du Préposé cantonal

Le Préposé cantonal se demande si une telle politique ne devrait pas préalablement être l'objet d'un extrait de procès-verbal qui fixe les objectifs et demande sa mise en œuvre par le biais d'une directive transversale.

Le Préposé cantonal à la protection des données et à la transparence est d'avis que le projet de directive transversale, qui répond à l'exigence posée par l'art. 35 du ROGSIC, devrait être beaucoup plus court et simplifié pour que sa lecture par toute collaboratrice et collaborateur de l'Etat de Genève soit plus aisée.

Ce texte devrait en particulier comprendre de façon plus explicite les objectifs poursuivis en matière de sécurité de l'information et des indicateurs mesurables de l'atteinte des objectifs.

Convaincu que la sécurité de l'information est l'affaire de toutes et tous, et qu'elle dépend pour une large part des mesures prises pour sensibiliser chaque personne, le Préposé cantonal considère qu'il importe que la directive transversale comporte des éléments plus précis de ce que recouvre ce volet et qui le prend en charge.

Pascale Byrne-Sutton
Préposée adjointe

Stéphane Werly
Préposé cantonal