Politique de sécurité du système d'information de l'Hospice général – Projet de directives

Avis du 15 avril 2014

Mots clés: mesures d'organisation générales, projet de directives, protection des données personnelles, sécurité de l'information

Contexte: Par courrier du 11 février 2014, le directeur général de l'Hospice général - Institution genevoise d'action sociale (HG), établissement de droit public cantonal au sens de l'art. 3 al. 1 let. c LIPAD, a soumis pour consultation (art. 50 al. 2 let. g LIPAD) au Préposé cantonal à la protection des données et à la transparence (PPDT) un projet de neuf directives relatives à la politique de sécurité de l'information. A en outre été annexé un document intitulé "Politique de sécurité du système d'information".

Ces directives ont pour objectif, à l'ère des moyens de communication électronique, de garantir la sécurité de l'information au sein de l'Hospice général.

Bases juridiques: art. 50 al. 2 let. g LIPAD

Considérations

De manière générale, la protection des données doit garantir que le principe de la proportionnalité sera respecté dans tous les cas, c'est-à-dire que la collecte et le traitement impliqueront le moins de données personnelles possible, et jamais plus que le strict nécessaire ; elle doit par ailleurs garantir à la personne concernée la possibilité de contrôler dans toute la mesure du possible le traitement de ses propres données, pour qu'elle puisse, le cas échéant, s'y opposer. Il est donc impératif que chacun puisse demander aux maîtres de fichiers quelles sont les données le concernant dont ils disposent.

A cet égard, l'Hospice général détient de données sensibles, personnelles et financières nécessitant une garantie de protection adéquate des données et des ressources informatiques.

Confidentialité, intégrité, disponibilité et conformité doivent notamment être assurées, afin de prévenir des conséquences sur les plans organisationnel et financier, sans parler de l'atteinte éventuelle en termes d'image.

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 des textes qui ont été portés 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.

Les dix documents suivants ont été soumis à consultation:

- Politique de sécurité du système d'information

- Directive 1.1: Utilisation des ressources informatiques

- Directive 1.2: Moyens de contrôles de la messagerie
- Directive 1.3: Moyens de contrôles de l'Internet
- Directive 1.4: Gestion de l'exploitation des communications et des réseaux
- Directive 2.1: Classification et contrôle des actifs
- Directive 2.2: Éléments de sécurité liés aux ressources humaines
- Directive 2.3: Sécurité physique et de l'environnement
- Directive 3.1: Gestion de la continuité de l'activité
- Directive 3.2: Conformité, cadre légal et technique

De l'examen effectué, il apparaît que les textes s'inscrivent bien dans le respect des principes relatifs à la protection des données. Ils se positionnent dans la lignée des directives du Collège spécialisé des systèmes d'information du canton de Genève, dont ils tirent visiblement leur essence (directive sur la classification des informations, directive sur les comptes et mots de passe, directive sur les moyens de contrôle relatifs à l'utilisation de la messagerie, directive sur les moyens de contrôle relatifs à la station de travail, directive relative à l'utilisation de la téléphonie, directive sur les moyens de contrôles relatifs à l'utilisation d'Internet, directive sur le partage d'informations couvertes par le secret de fonction).

La structure des textes est à saluer: préambule, documents de référence, champ d'application, mesures de protection, moyens de contrôle sont systématiquement mentionnés. La rédaction est soignée, les titres des différents chapitres clairs.

Cela dit, nous nous permettons ci-après quelques remarques ou suggestions :

Politique de sécurité du système d'information

Le document pose notamment les buts, le champ d'application et l'architecture de la politique de sécurité selon le schéma de la norme ISO 27000.

Il rappelle judicieusement que les ressources informatiques et de télécommunications mises à disposition par l'HG sont destinées à un usage strictement professionnel, conformément à l'art. 23A du règlement d'application de la loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publics médicaux du 24 février 1999 (RS GE B 5 05.01).

La rédaction d'un glossaire nous paraîtrait tout à fait opportune dans ce contexte très spécialisé. A cet égard, ce texte général devrait contenir tous les termes répertoriés dans les neuf directives, ce qui permettrait d'alléger le contenu de ces dernières et de regrouper tous les mots expliqués dans un seul document à vocation générale. Renvoi pourrait être fait à cet égard à l'art. 4 LIPAD pour le surplus, qui contient des définitions pertinentes pour le propos.

Inspiration pourrait être tirée du règlement sur l'organisation et la gouvernance des systèmes d'information et de communication du 26 juin 2013 (ROGSIC; RSGE B 4 23.03). Ce texte, qui n'est pas directement applicable au grand Etat, 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), définit de façon claire et concise le cadre organisationnel des systèmes d'information relatif aux projets informatiques et son 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 ROGSIC 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 ROGSCI 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;

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.

Directive 1.1: Utilisation des ressources informatiques

Une erreur est à signaler à la page 2. Il est fait référence au Règlement concernant la protection des applications et des systèmes informatiques dans l'administration cantonale du 5 avril 2000 (RCPA). Or ce dernier a été abrogé par l'art. 36 let. a ROGSIC.

Le point 8 (smartphones) est particulièrement bien rédigé. Il démontre la réflexion menée par l'HG sur la nécessite de prendre des mesures permettant de mettre en place une gestion sécurisée et efficace des données afin de se mettre en conformité avec la norme ISO 27002.

La définition des données personnelles a été reprise telle quelle de l'art. 4 let. a LIPAD.

Directive 1.2: Moyens de contrôles de la messagerie

Mention du RCPA et glossaire: même remarque que supra.

Remarque d'ordre rédactionnel p. 2: le chiffre marginal 4.4.1 n'a pas lieu d'être, en l'absence de 4.4.2. Idem p. 6 pour le chiffre 6.4.1.

Remarque orthographique p. 3: "l'expéditeur ou l'expéditrice en est avisée".

Directive 1.3: Moyens de contrôles de l'Internet

Mention du RCPA et glossaire: même remarque que supra.

Remarque d'ordre rédactionnel p. 4: le chiffre marginal 6.2.1 n'a pas lieu d'être, en l'absence de 6.2.2. Idem pour le chiffre 6.3.1.

Directive 1.4: Gestion de l'exploitation des communications et des réseaux

Le cadre général semble un peu long et abscons. Il serait souhaitable de le simplifier.

Mention du RCPA et glossaire: même remarque que supra.

Remarque d'ordre rédactionnel p. 3: le chiffre marginal 4.4.1 n'a pas lieu d'être, en l'absence de 4.1.2. Idem p. 4 pour les chiffres 4.5.1, 4.6.1, 5.1.1, 7.1.1, 9.2.1 et 10.5.1.

[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) »*.

Directive 2.1: Classification et contrôle des actifs

Mention du RCPA et glossaire: même remarque que supra.

Le fait de donner des définitions de concepts à la page 2 se conçoit volontiers, étant donné le sujet spécifique de la directive. En revanche, le maintien du glossaire ce justifie d'autant moins à ce stade.

Remarque d'ordre rédactionnel p. 7: le chiffre marginal 5.6.1 n'a pas lieu d'être, en l'absence de 5.6.2.

Directive 2.2: Éléments de sécurité liés aux ressources humaines

Mention du RCPA et glossaire: même remarque que supra.

Remarque d'ordre rédactionnel p. 4: le chiffre marginal 7.1.1 n'a pas lieu d'être, en l'absence de 7.1.2. Idem pour les chiffres 7.2.1 et 7.4.1.

Directive 2.3: Sécurité physique et de l'environnement

Mention du RCPA et glossaire: même remarque que supra.

Directive 3.1: Gestion de la continuité de l'activité

Mention du RCPA et glossaire: même remarque que supra.

Directive 3.2: Conformité, cadre légal et technique

Mention du RCPA et glossaire: même remarque que supra. A cet égard, les définitions mentionnées à la page 3 font en outre double emploi avec le glossaire.

Il convient de préciser, à la page 2, que l'HG est un établissement de droit public cantonal au sens de l'art. 3 al. 1 let. c LIPAD

La référence à l'art. 1 al. 2 let. b LIPAD, s'agissant d'un des buts de la loi, à savoir protéger les droits fondamentaux des personnes physiques ou morales de droit privé quant aux données personnelles les concernant, serait souhaitable.

La directive reprend in extenso le texte de l'art. 37 LIPAD. L'on comprend mal pourquoi il n'en va pas de même des art. 35 (bases légales), 36 (qualité des données personnelles) et 38 (collecte). Ces dispositions reprennent, en la matière, des principes cardinaux tirés de la loi fédérale sur la protection des données du 19 juin 1992 (LPD; RS 235.1). Les intégrer ne serait donc de loin pas inutile.

A la page 3, il conviendrait de préciser que le Préposé cantonal à la protection des données et à la transparence assiste les responsables désignés dans l'accomplissement de leurs tâches (art. 56 al. 3 let. d LIPAD).

Le point 5.1.1 "La politique de sécurité de l'Hospice général doit impérativement respecter la législation en vigueur" est superflu.

Avis du Préposé cantonal

Le Préposé cantonal à la protection des données et à la transparence est d'avis que le projet qui lui a été soumis contient de manière explicite les objectifs poursuivis en matière de sécurité de l'information et des indicateurs mesurables de l'atteinte des objectifs.

La lecture des différents textes semble par ailleurs aisée pour toute collaboratrice et collaborateur de l'Hospice général.

La rédaction de directives constitue certes une mesure nécessaire, sans être toutefois suffisante. En effet, 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 que ces textes doivent s'accompagner d'une politique de sensibilisation à l'égard des collaboratrices et collaborateurs, s'agissant d'un sujet qui comporte des enjeux majeurs.

Pascale Byrne-Sutton	Stéphane Werly
Préposée adjointe	Préposé cantonal