Cour des comptes
République et canton de Genève

La sécurité des données personnelles sensibles en Ville de Genève

Rapport n°198

14 octobre 2025

SYNTHÈSE

AUDIT DE CONFORMITÉ

Au service d'une action publique performante

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

Cour des comptes
République et canton de Genève

La Cour des comptes est chargée du contrôle indépendant et autonome des services et départements de l'administration cantonale, du pouvoir judiciaire, des institutions cantonales de droit public, des organismes subventionnés ainsi que des institutions communales. Elle a également pour tâche l'évaluation des politiques publiques et assure la révision des comptes de l'État.

La Cour des comptes vérifie d'office et selon son libre choix la légalité des activités et la régularité des recettes et des dépenses décrites dans les comptes, et s'assure du bon emploi des crédits, fonds et valeurs gérés par les entités visées par ses missions. La Cour des comptes peut également évaluer la pertinence, l'efficacité et l'efficience de l'action de l'État. Elle organise librement son travail et dispose de larges moyens d'investigation. Elle peut notamment requérir la production de documents, procéder à des auditions, à des expertises, se rendre dans les locaux des entités concernées.

Le champ d'application des missions de la Cour des comptes s'étend aux entités suivantes :

- l'administration cantonale comprenant les départements, la chancellerie d'État et leurs services ainsi que les organismes qui leur sont rattachés ou placés sous leur surveillance ;
- les institutions cantonales de droit public ;
- les entités subventionnées ;
- les entités de droit public ou privé dans lesquelles l'État possède une participation majoritaire, à l'exception des entités cotées en bourse ;
- le secrétariat général du Grand Conseil ;
- l'administration du pouvoir judiciaire ;
- les autorités communales, les services et les institutions qui en dépendent, ainsi que les entités intercommunales.

Les rapports de la Cour des comptes sont rendus publics : ils consignent ses observations, les conclusions de ses investigations, les enseignements qu'il faut en tirer et les recommandations conséquentes. La Cour des comptes prévoit en outre de signaler dans ses rapports les cas de réticence et les refus de collaborer survenus au cours de ses missions.

La Cour des comptes publie également un rapport annuel comportant la liste des objets traités, celle de ceux qu'elle a écartés, celle des rapports rendus avec leurs conclusions et recommandations et les suites qui y ont été données. Les rapports restés sans effet ni suite sont également signalés.

Vous pouvez participer à l'amélioration de la gestion de l'État en prenant contact avec la Cour des comptes. Toute personne, de même que les entités comprises dans son périmètre d'action, peuvent communiquer à la Cour des comptes des faits ou des pratiques qui pourraient être utiles à l'accomplissement des tâches de cette autorité.

Prenez contact avec la Cour par téléphone, courrier postal ou électronique.

Cour des comptes
Route de Chêne 54, 1208 Genève | 022 388 77 90 | info@cdc-ge.ch | www.cdc-ge.ch

Contexte général

Au sein des administrations publiques, le nombre de données traitées (collectées, manipulées, stockées, transmises) augmente au rythme des projets de numérisation et les nouvelles capacités techniques induisent toujours plus de menaces à la sécurité des données (notamment capacité d'export et de transfert en masse, utilisation de services *cloud*[1] , essor du télétravail). Tous ces éléments rendent la sécurisation des données lourde et labyrinthique, constituant un véritable défi pour les institutions publiques.

Certaines de ces données à protéger se rapportent à une personne identifiée ou identifiable. On parle alors de données personnelles. Parmi elles, les données personnelles dites **« sensibles »** revêtent une criticité particulière puisqu'elles concernent, par exemple, des informations sur les opinions religieuses, l'origine ethnique, l'état de santé ou encore le passé judiciaire d'un individu.

À Genève, les institutions publiques cantonales, communales et intercommunales sont tenues de protéger ces données. Elles sont en effet soumises à la *Loi sur l'information du public, l'accès aux documents et la protection des données personnelles* (LIPAD) *du 5 octobre 2001*[2] dont l'article 37 pose comme principe général que « l*es données personnelles* ***doivent être protégées*** *contre tout traitement illicite* ***par des mesures organisationnelles et techniques appropriées*** »[3].

Problématique et objectifs de l'audit

Vers la fin de l'année 2023, la Cour a reçu plusieurs alertes dénonçant des accès trop étendus et non contrôlés d'administrateurs informatiques de la Ville de Genève (VdG) à des données personnelles sensibles. Les allégations portaient également sur le fait que le dispositif de sécurité mis en œuvre par la VdG autour des données personnelles ne serait pas conforme aux dispositions de la LIPAD. Ces éléments ont convaincu la Cour de l'opportunité de réaliser un audit de conformité sur cette thématique.

L'objectif de cet audit était d'apprécier dans quelles mesures la VdG a défini et mis en œuvre les mesures organisationnelles[4] et techniques appropriées pour assurer la sécurité des données personnelles.

[1] Il s'agit d'une technologie informatique qui offre des capacités informatiques évolutives et adaptables sous la forme d'un service reposant sur des technologies liées à Internet, souvent offerte par des fournisseurs sous forme de service.
[2] rs/GE A 2 08. Entrée en vigueur le 1er mars 2002 en ce qui concerne l'aspect transparence. La réforme des règles sur la protection des données a été introduite par la loi 9870 du 9 octobre 2008, entrée en vigueur le 1er janvier 2010.
[3] Art. 37, al. 1 LIPAD.
[4] Cela inclut par exemple le *corpus* procédural, l'organisation, la formation des collaborateurs, le contrôle interne ou encore la supervision.

Appréciation générale

Il est important d'indiquer que les travaux de la Cour n'ont pas identifié de cas significatif de violation de la sécurité des données. La Cour a notamment consulté les traces des documents exportés via des clés USB et des téléchargements vers internet sur plusieurs mois. Concernant les allégations d'accès étendus et non contrôlés d'administrateurs informatiques à des données personnelles, la Cour constate que la VdG a pris des mesures pour limiter les accès, assurer la traçabilité des actions réalisées et valider les accès à certains systèmes sensibles. Ainsi, les contrôles mis en place par la VdG sur ces aspects apparaissent comme suffisants au moment de l'audit.

De manière générale, la LIPAD ne définit pas les mesures techniques de sécurité à mettre en place. Elles doivent être déterminées en fonction des risques encourus et du niveau de sécurité voulu par la gouvernance de la VdG. Or, la Cour constate des lacunes en la matière. Si la VdG a implémenté plusieurs dispositifs de sécurité au cours des dernières années, ses efforts se sont principalement concentrés sur les risques cyber (menaces venant de l'extérieur). Par contre, d'autres domaines, comme la prévention de la perte ou fuite de données, ne sont pas pleinement couverts par les mesures en place.

Principaux constats

Une connaissance insuffisante des risques et de leur niveau de couverture

La Ville de Genève n'a pas de vision complète des risques auxquels les données personnelles sensibles sont exposées tout au long de leur cycle de vie. En particulier, les risques liés à l'utilisation de nouvelles technologies (*cloud*, intelligence artificielle), à la perte ou à la fuite de données ou au transfert de données ne sont pas suffisamment identifiés ni analysés. De ce fait, plusieurs aspects de la sécurité des données ne sont pas pris en compte lors des décisions adoptées en termes de gestion des risques.

Par ailleurs, bien que la méthodologie de gestion des risques prévoie que le Conseil administratif définisse une « appétence au risque », celle-ci n'est pas assez précise pour guider les décisions sur les contrôles à mettre en place pour garantir la sécurité des données personnelles.

Une stratégie de contrôle qui n'est pas définie

La VdG ne dispose pas d'une vision d'ensemble des mesures en place et ne peut pas s'assurer de leur caractère approprié sur tout le cycle de vie de la donnée. La Cour relève en particulier que les attentes doivent être clarifiées pour les trois domaines suivants :

a) Premièrement, par la nature des droits informatiques dont ils disposent, les collaborateurs informatiques, en particulier les administrateurs, constituent une zone importante de risque. Bien que la VdG ait déjà pris de nombreuses mesures au fil des années (réduction des privilèges, traçage des activités, validation des demandes d'accès aux serveurs sensibles, etc.), la stratégie de couverture des risques dans ce domaine doit encore être finalisée et formalisée par des procédures écrites.

b) Deuxièmement, pour l'ensemble des collaborateurs traitant des données au sein des services, les pratiques ou usages autorisés (et ceux à proscrire) ne sont pas suffisamment définis. Par exemple, dans les directives et procédures existantes, rien

n'interdit à un collaborateur de copier des données sensibles sur une clé USB non sécurisée ou sur un espace de stockage dans le *cloud*.

c) Enfin, pour les données que la VdG fait traiter par des prestataires externes, le niveau de contrôle global est insuffisant. En effet, les institutions demeurent responsables des données personnelles qu'elles font traiter au même titre que si elle les traitait elle-même [5]. Ainsi, elles doivent prendre les mesures nécessaires, par le biais de clauses contractuelles appropriées, pour assurer la sécurité des données personnelles qu'elles font traiter[6] et contrôler le respect de ces clauses[7]. Les travaux de la Cour révèlent des insuffisances sur définition des clauses ainsi que l'absence de contrôle systématique des prestataires.

Des mesures organisationnelles insuffisantes, notamment au sein des services

Étant donné la nature des prestations rendues, la diversité des métiers en Ville de Genève et la structure décentralisée de l'administration, toutes les problématiques de sécurité ne peuvent être réglées de manière centralisée. Une partie des mesures doit être définie par les services métiers en fonction de leurs spécificités (pratiques de travail). Dès lors, il apparaît nécessaire que chaque département ou service dispose d'un relai local afin d'assumer ce rôle, au plus près des collaborateurs. La Cour note un manque de clarté sur les rôles et responsabilités en lien avec la sécurité des données au sein des services, ce qui induit un niveau de contrôle hétérogène d'un service à l'autre.

Enfin, la Cour constate que certaines notions de base, comme la définition d'une donnée personnelle ou les précautions nécessaires pour leur traitement, ne sont pas toujours connues des collaborateurs. Bien que des formations aient été intégrées au catalogue de formation obligatoire de la VdG, elles restent trop générales et n'abordent pas suffisamment la question de la sécurité des données personnelles. De plus, les collaborateurs « sensibles » ou « à risque » tels que les administrateurs de base de données, les informaticiens ou encore les intervenants externes (nombreux en informatique) ne bénéficient pas de formation renforcée.

Un corpus documentaire incomplet

La Cour constate que le cadre procédural en matière de sécurité des données au sein de la VdG est insuffisant et nécessite une mise à jour pour s'adapter aux avancées technologiques. Les documents de référence et les directives générales adoptées en VdG abordent peu la question de la sécurité des données personnelles. Par exemple, les comportements et pratiques que les collaborateurs doivent adopter lors du traitement, de la transmission ou de la destruction de la donnée ne sont pas abordés. De plus, le *corpus* procédural existant n'inclut pas les technologies récentes comme l'intelligence artificielle, l'utilisation de service de stockage en ligne (*cloud*) ou plus largement, l'utilisation d'internet.

---

[5] Art. 13A, al. 2 du règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (RIPAD) : « *L'institution demeure responsable des données personnelles qu'elle fait traiter au même titre que si elle les traitait elle-même* ».

[6] Art. 37, al. 2 LIPAD : « *Les institutions publiques prennent, par le biais de directives ainsi que de clauses statutaires ou contractuelles appropriées, les mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données personnelles qu'elles traitent ou font traiter* ».

[7] Art. 37, al. 3 LIPAD : « *Les institutions publiques sont tenues de contrôler le respect des directives et clauses visées à l'alinéa 2* ».

Axes d'amélioration proposés

Réaliser une évaluation complète des risques relatifs à la sécurité des données personnelles et clarifier l'appétence au risque

La Cour recommande en premier lieu de réaliser une évaluation complète des risques relatifs à la sécurité des données personnelles en veillant à couvrir les dimensions pertinentes (travail des informaticiens, usage de l'informatique par les métiers, sous-traitance de traitement de données, etc.). Ensuite, la Cour préconise de présenter l'analyse des risques ainsi réalisée au Conseil administratif de la Ville de Genève (CA) afin de s'assurer que l'état actuel des dispositifs de sécurité et le degré d'exposition de l'administration aux risques sont cohérents avec la tolérance au risque du CA. Cette démarche permettra à l'exécutif de la VdG de clarifier son appétence au risque en matière de sécurité des données personnelles.

Définir une stratégie de contrôle couvrant l'ensemble du cycle de vie de la donnée

La Cour recommande de définir une stratégie de contrôle englobant de manière cohérente l'ensemble des domaines évoqués précédemment. Ainsi, il s'agit dans un premier temps de couvrir les risques liés aux pratiques et modes opératoires des équipes informatiques. Ensuite, les risques liés à l'utilisation des outils informatiques par les collaborateurs ainsi que leurs pratiques de travail doivent être couverts. Enfin, il conviendra de renforcer la gestion de la sécurité des données personnelles lors des sous-traitances, notamment en identifiant les prestations impliquant des données personnelles et en s'assurant que des clauses appropriées soient systématiquement intégrées aux contrats. La VdG devra s'assurer que le prestataire respecte ses engagements pendant toute la durée du contrat.

Désigner des personnes relais au sein des services pour renforcer la sécurité des données personnelles

La Cour recommande de désigner des personnes relais au sein des services / départements pour coordonner les aspects liés à la sécurité des données personnelles. Celles-ci devront définir les pratiques autorisées au sein de leur unité organisationnelle et en assurer le suivi. Elles joueront aussi le rôle de référent pour répondre à d'éventuelles interrogations des collaborateurs du service en lien avec la sécurité des données personnelles.

Compléter et actualiser le corpus procédural et renforcer le dispositif de formation

La Cour recommande d'enrichir et de mettre à jour le cadre procédural existant afin de préciser les pratiques, mesures et comportements attendus en matière de sécurité des données personnelles. Ces règles doivent être en adéquation avec le niveau de sécurité cible défini, tenir compte des avancées technologiques et être présentées de manière à faciliter leur compréhension et l'application par les utilisateurs des systèmes d'information (SI).

Enfin, la Cour recommande de définir un plan de formation spécifique à la sécurité des données personnelles prévoyant une sensibilisation renforcée des collaborateurs pouvant accéder à une grande quantité de données (selon une approche basée sur les risques), incluant les prestataires externes.

Tableau récapitulatif des recommandations

Recommandations : 8		Niveau de priorité[8] :	
- Acceptées :	8	Très élevée	-
		Élevée	5
- Refusées :	-	Moyenne	2
		Faible	1

Les huit recommandations adressées aux audités ont toutes été acceptées.

No	Recommandation / Action	Priorité	Responsable	Délai
1	Réaliser une évaluation plus détaillée des risques relatifs à la sécurité des données personnelles	Élevée	Groupe SCI, DSIC, en collaboration avec le DPO	31.12.2026
2	Clarifier l'appétence au risque	Élevée	Groupe SCI, DSIC, en collaboration avec le DPO	31.03.2027
3	Définir une stratégie de contrôle sur la gestion des systèmes d'information par les équipes informatiques	Élevée	RCI DCTN, DSIC, en collaboration avec le DPO	31.12.2026
4	Définir une stratégie de contrôle liée à la sécurité des données au sein des services	Élevée	RCI DCTN, DSIC, en collaboration avec le DPO	31.12.2026
5	Renforcer la sécurité des données dans le cadre des sous-traitances	Élevée	CMAI, en collaboration avec la DSIC et le DPO	31.12.2026
6	Désigner des personnes relais au sein des services pour renforcer la sécurité des données personnelles	Moyenne	CODIR et le DPO	31.12.2026
7	Définir et mettre en œuvre un dispositif de formation et de sensibilisation approprié en lien avec la sécurité des données personnelles	Moyenne	CODIR et le DPO	31.12.2026
8	Compléter et actualiser le *corpus* procédural en matière de la sécurité des données	Faible	DSIC, service des archives, en collaboration avec le DPO	31.12.2026

[8] Le niveau de priorité est déterminé par la Cour des comptes en lien direct avec l'appréciation des risques et en fonction de l'impact positif de la recommandation sur l'amélioration de la gouvernance et les risques à couvrir. Le niveau de priorité de chacune des recommandations est explicité lors de la présentation desdites recommandations.

Dans le cadre de ses missions légales, la Cour des comptes doit effectuer un suivi des recommandations émises aux entités auditées, en distinguant celles ayant été mises en œuvre et celles restées sans effet. À cette fin, elle a invité le Conseil administratif de la Ville de Genève à remplir le tableau ci-dessus qui synthétise les améliorations à apporter, en indiquant le responsable de leur mise en place et leur délai de réalisation. Le niveau de priorité a été défini par la Cour.

Cour des comptes
République et canton de Genève

Vous pouvez participer à l'amélioration de la gestion de l'État en prenant contact avec la Cour des comptes.

Toute personne, de même que les entités comprises dans son périmètre d'action, peuvent communiquer à la Cour des comptes des faits ou des pratiques qui pourraient être utiles à l'accomplissement des tâches de cette autorité.

La Cour des comptes garantit l'anonymat des personnes qui lui transmettent des informations.

Vous pouvez prendre contact avec la Cour des comptes par téléphone, courrier postal ou électronique.

Cour des comptes
Route de Chêne 54, 1208 Genève | 022 388 77 90
info@cdc-ge.ch | www.cdc-ge.ch

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX