Cour des comptes
République et canton de Genève

# La sécurité des données personnelles sensibles en Ville de Genève

## Rapport n°198

## 14 octobre 2025

**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

# Synthèse

## Contexte

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.

# Table des matières

# Liste des principales abréviations utilisées

| | |
|---|---|
| CA | Conseil administratif |
| CFI | Service du contrôle financier |
| CMAI | Centrale municipale d'achat et d'impression |
| CODIR | Comité de direction |
| COMSEC-G | Comité de sécurité - Gouvernance |
| COMSEC-M | Comité de sécurité - Management |
| DCTN | Département de la culture et de la transition numérique |
| DELTRANS | Délégation du Conseil administratif à la transformation numérique |
| DGUSIC | Directive générale relative à l'utilisation des systèmes d'information et de communication |
| DPO | Délégué à la Protection des Données |
| DSIC | Direction des systèmes d'information et de communication |
| ETP | Équivalent temps plein |
| LIPAD | Loi sur l'information du public, l'accès aux documents et la protection des données personnelles |
| nLIPAD | Nouvelle loi sur l'information du public, l'accès aux documents et la protection des données personnelles |
| PPDT | Préposé cantonal à la protection des données et à la transparence |
| PFPDT | Préposé fédéral à la protection des données et à la transparence |
| PSSI | Politique de sécurité des systèmes d'information |
| RCI | Responsables de contrôle interne |
| RIPAD | Règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles |
| RSSI | Responsable de la sécurité informatique |
| SCI | Système de contrôle interne |
| SI | Systèmes d'information |
| SIC | Systèmes d'information et de communication |
| SMSI | Système de management de la sécurité informatique |
| TOM | Guide relatif aux mesures techniques et organisationnelles de la protection des données du préposé fédéral à la protection des données et à la transparence |
| VdG | Ville de Genève |

# Liste des figures et tableaux

# 1. Cadre et contexte de l'audit

Vers la fin de l'année 2023, la Cour a reçu plusieurs signalements de citoyens inquiets d'accès étendus et non contrôlés d'administrateurs informatiques de la Ville de Genève (ci-après « VdG ») à des données personnelles sensibles. Les allégations portaient également sur le fait que le dispositif de sécurité mis en œuvre autour des données personnelles ne serait pas conforme aux dispositions de la Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (ci-après : « LIPAD ») et de son règlement d'application (ci-après : « RIPAD »).

Au-delà des signalements reçus, la protection des données personnelles représente un enjeu important, tant pour l'image des institutions publiques que pour le maintien de la confiance des citoyens envers leur administration. La protection contre l'emploi abusif des données concernant une personne constitue un droit fondamental garanti par la constitution fédérale (art. 13, al. 2) et la constitution cantonale (art. 21, al. 2).

Au sein des institutions publiques, de plus en plus d'outils informatiques sont mis en place pour améliorer aussi bien les prestations aux citoyens que les processus internes. On parle alors de transition numérique. Ce faisant, le nombre de données traitées (collectées, manipulées, stockées, transmises) augmente significativement, y compris en ce qui concerne les données personnelles. Ces dernières se disséminent au travers de systèmes d'information (SI) toujours plus étendus et complexes (architecture décentralisée, utilisation de services *cloud*[9], essor du télétravail, recours à des prestataires externes, possibilité d'extraction et d'export de données en masse en quelques secondes, etc.) rendant leur sécurisation lourde et labyrinthique.

Compte tenu de ce qui précède, la maîtrise des SI et la sécurisation des données constituent des enjeux et des défis importants pour la VdG. Relever de tels défis n'est possible qu'au travers d'un ensemble de mesures organisationnelles et techniques adéquates, sur tout le cycle de vie de la donnée.

La somme de ces éléments a convaincu la Cour de l'opportunité de réaliser un audit sur la sécurité des données personnelles sensibles en VdG.

La présente mission s'accorde avec les compétences de la Cour de s'assurer de la légalité des activités des autorités communales et des services qui en dépendent, ainsi que du bon emploi des fonds publics, dans le respect des principes de la performance publique (art. 35 let. g et art. 40 al. 1 et 2 de la loi sur la surveillance de l'État).

Ainsi, par lettre du 20 février 2025 adressée à la Maire de la commune, la Cour a officiellement informé la VdG de sa décision d'entreprendre un audit de conformité portant sur la sécurité des données personnelles en VdG.

[9] 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.

Deux objectifs sont couverts par l'audit :

- S'assurer que la VdG a défini et mis en œuvre les conditions-cadres et les mesures organisationnelles appropriées afin d'assurer la sécurité des données personnelles sensibles[10] ;
- S'assurer que, sous l'angle technique, la VdG identifie et protège de manière appropriée les données personnelles.

Pour répondre à ces objectifs, la Cour a formulé les quatre questions d'audit suivantes :

1. La VdG a-t-elle défini et implémenté un cadre procédural et organisationnel permettant d'assurer la sécurité des données personnelles ?

2. La VdG dispose-t-elle d'une vision complète et à jour des données personnelles qu'elle traite ou conserve et a-t-elle un inventaire des systèmes informatiques sous-jacents ?

3. Des mesures techniques de sécurité de la donnée personnelle sont-elles correctement définies et implémentées (incluant les données sous-traitées) ?

4. La VdG a-t-elle mis en œuvre une surveillance adéquate concernant les dispositifs techniques de sécurité des données personnelles (incluant les données sous-traitées) ?

Le périmètre de la mission de la Cour s'étend à l'ensemble de l'administration communale avec une focale sur les mesures techniques appliquées aux données personnelles sensibles ainsi que sur les mesures organisationnelles associées[11]. Si la LIPAD fait partie du cadre référentiel de l'audit, la Cour n'a pas réalisé un audit de la conformité à toutes ses dispositions et elle s'est uniquement concentrée sur les aspects liés à la sécurité des données.

Souhaitant être la plus efficace possible dans ses travaux, la Cour examine lors de ses investigations l'ensemble des rapports d'audit préalables effectués par des tiers, tant internes qu'externes, portant sur les mêmes thématiques que le présent rapport. Dans le cas présent, la Cour n'a pas eu connaissance d'audits récents réalisés sur la thématique de la sécurité des données personnelles en VdG[12].

Afin de faciliter la lecture du rapport, le masculin générique est utilisé pour désigner les deux sexes.

[10] Cela inclut par exemple le *corpus* procédural, l'organisation, la formation des collaborateurs, le contrôle interne ou encore la supervision.
[11] Dont le *corpus* procédural, la répartition des rôles et responsabilités, la formation et la sensibilisation des collaborateurs, les flux de remontées d'information et la supervision des dispositifs techniques.
[12] La Cour a consulté les audits récents portés à sa connaissance même s'ils n'abordaient que partiellement la sécurité informatique. Ainsi, des sujets comme la gestion des accès, le paramétrage de logiciel, l'analyse des risques ou encore la gouvernance des SI ont été couverts. Par ailleurs, si certains aspects de la LIPAD ont été revus par un organe de contrôle, les articles liés à la sécurité des données n'ont pas fait l'objet d'une revue approfondie.

# 2. Modalités et déroulement de l'audit

La Cour a réalisé ses travaux entre les mois de mars et juin 2025. Elle a conduit cet audit sur la base de l'analyse des documents remis par la VdG, ainsi qu'en menant une vingtaine d'entretiens avec :

- Des collaborateurs du secrétariat général ;
- Des correspondants LIPAD ;
- Des collaborateurs de la Direction des systèmes d'information et de communication (DSIC) ;
- Des collaborateurs de la gestion des risques et du contrôle interne ;
- Des collaborateurs de services juridiques ;
- Des correspondants informatiques ;
- Des collaborateurs du service du contrôle financier (CFI).

La première étape a consisté en l'analyse de l'ensemble des directives, procédures ou autres consignes existantes en VdG et portées à la connaissance de la Cour en lien avec la sécurité des données et la LIPAD.

La Cour a également procédé à une revue des principales mesures techniques en place, telles que la gestion des accès, la traçabilité et la journalisation des évènements informatiques, la classification des fichiers, la sécurisation des postes utilisateurs ou encore la gestion des accès à hauts privilèges (administrateurs).

La Cour a aussi procédé à l'analyse d'un échantillon de contrats de sous-traitance en lien avec des prestations pouvant induire le traitement[13] de données personnelles sensibles par des prestataires ainsi que les mesures en place pour limiter les risques associés.

Comme prévu par sa base légale, la Cour privilégie avec ses interlocuteurs une démarche constructive et participative visant à la **recherche de solutions améliorant le fonctionnement de l'administration publique**. C'est ainsi que la Cour a pu proposer aux intervenants rencontrés différentes possibilités d'amélioration de leur gestion, dont la faisabilité a pu être évaluée et la mise en œuvre appréciée sous l'angle du **principe de la proportionnalité**.

La Cour a conduit ses travaux conformément à la loi sur la surveillance de l'État, à sa charte éthique et à ses procédures internes. Celles-ci s'inspirent des normes professionnelles en vigueur (notamment les normes ISSAI et les normes internationales d'audit interne) dans la mesure où elles sont applicables et compatibles avec la nature particulière de la mission.

En pratique, la méthodologie de la Cour des comptes est la suivante :

**1ère phase : Planification**
Cette phase consiste à définir et à mobiliser les ressources et les compétences les mieux adaptées à la mission que ce soit auprès des collaborateurs de la Cour des comptes ou auprès de tiers, et à déterminer les outils méthodologiques à utiliser.

[13] L'article 4, lettre e) LIPAD définit le traitement comme « toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données ».

**2ème phase : Préparation de l'audit**
Cette phase consiste à identifier auprès de l'entité auditée quels sont ses bases légales et ses intervenants-clés, à comprendre son organisation et son fonctionnement, à collecter des données chiffrées et à procéder à l'analyse des risques qui lui sont propres. À ce stade, un plan de mission est rédigé avec notamment les objectifs de la mission, les moyens à disposition, les travaux dévolus à chaque intervenant de la Cour et les délais impartis dans le déroulement de la mission.

**3ème phase : Récolte d'informations**
Cette phase consiste à déterminer les sources de l'information pertinente, à savoir quelles sont les personnes-clés à contacter et quelles sont les informations qui sont nécessaires à l'atteinte des objectifs. Ensuite, les collaborateurs de la Cour et/ou les tiers mandatés procèdent à des entretiens et collectent les informations requises.

**4ème phase : Vérification et analyse de l'information**
Cette phase consiste d'une part à s'assurer que les informations récoltées sont fiables, pertinentes, complètes et à jour et d'autre part à les analyser et à les restituer sous la forme de documents de travail.

**5ème phase : Proposition de recommandations**
Cette phase consiste à établir les constatations significatives, à déterminer les risques qui en découlent et enfin à proposer des recommandations afin de rétablir la légalité des opérations, la régularité des comptes ou d'améliorer la structure ou le fonctionnement de l'organisation.

**6ème phase : Rédaction du rapport**
Cette phase consiste à rédiger le rapport conformément aux documents de travail et à la structure adoptée par la Cour des comptes.

**7ème phase : Validation du rapport**
Cette phase consiste à discuter le contenu du rapport avec l'entité auditée, avec pour objectif de passer en revue les éventuelles divergences de fond et de forme et de s'accorder sur les priorités et délais des recommandations.

Ainsi, chaque thème développé dans ce rapport fait l'objet d'une mise en contexte, de constats et de recommandations soumis aux observations de l'audité.

Afin de faciliter le suivi des recommandations, la Cour a placé dans la synthèse un tableau qui résume les améliorations à apporter et dans lequel l'entité auditée a indiqué le responsable de leur mise en place ainsi que leur délai de réalisation.

Sauf exception, la **Cour ne prévoit pas de réagir aux observations de l'audité**. Elle estime qu'il appartient au lecteur de juger de la pertinence des observations formulées eu égard aux constats et recommandations développés par la Cour.

# 3. Contexte général

## 3.1. La base juridique sur la protection des données personnelles à Genève

### 3.1.1 La loi actuelle et ses exigences

La législation vise à prévenir tout traitement[14] abusif des données relatives aux personnes et protéger leur personnalité et sphère privée. Le respect de la vie privée est un droit fondamental ancré dans la Convention européenne des droits de l'homme[15] ainsi que dans les Constitutions suisse[16] et genevoise[17]. Les pouvoirs publics, qui gèrent nombre de données relatives à leurs administrés, sont particulièrement concernés par les exigences qui en découlent. En plus du droit au respect de la sphère privée, la Constitution genevoise prévoit le droit à l'intégrité numérique qui inclut notamment le droit *« d'être protégé contre le traitement abusif des données liées à sa vie numérique »*[18].

À Genève, les institutions publiques cantonales, communales et intercommunales sont soumises à la *Loi sur l'information du public, l'accès aux documents et la protection des données personnelles* (LIPAD) *du 5 octobre 2001*[19] et au *Règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (RIPAD) du 21 décembre 2011*[20]. Ces deux textes sont largement inspirés des règles fédérales en la matière[21].

En matière de sécurité des données, la LIPAD vise à poser des principes généraux : « *Les données personnelles* ***doivent être protégées*** *contre tout traitement* ***illicite par des mesures organisationnelles et techniques appropriées*** »[22]. Pour les communes, le RIPAD n'apporte guère de précisions, sauf l'obligation pour les institutions de tenir à jour un répertoire des personnes ayant accès aux SI contenant des données personnelles[23].

L'accent est également mis sur les éléments suivants :

- **L'importance des directives :** « 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 »[24].

---

[14] La LIPAD définit un traitement comme « *toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données* » (Art. 4, lettre e).
[15] Art. 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 (CEDH, RS 0.101).
[16] Art. de la Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst-féd, RS 101).
[17] Art. 21 de la Constitution de la République et canton de Genève du 14 octobre 2012 (Cst-GE, rs/GE A 2 00).
[18] Art. 21 A Cst-GE.
[19] 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.
[20] rs/GEA 2 08.01. Entré en vigueur le 29 décembre 2011.
[21] Principalement composé des dispositions de la loi fédérale sur la protection des données (LPD, RS 235.1) et de son ordonnance (OPDo, RS 235.11).
[22] Art. 37, al. 1 LIPAD.
[23] Art. 13, al. 3 RIPAD.
[24] Art. 37, al. 2 LIPAD.

- **La responsabilité en cas de recours à des prestations externes :** « Les institutions demeurent responsables des données personnelles qu'elles font traiter au même titre que si elle les traitait elle-même »[25].
- **L'importance de veiller à la correcte application de la loi :** « Des responsables ayant une formation appropriée et les compétences utiles doivent être désignés et des procédures adéquates doivent être mises en place au sein des institutions publiques, pour y garantir une correcte application de la présente loi »[26].

La loi institue aussi la fonction de Préposé cantonal à la protection des données et à la transparence (PPDT) afin de « *garantir une application coordonnée des principes applicables en matière d'information relative aux activités des institutions et de ceux régissant la protection des données personnelles* »[27].

### 3.1.2 Historique et évolution en cours de la législation genevoise

Le cadre législatif genevois actuel trouve son origine dans l'adoption, par le Grand Conseil genevois, le 24 juin 1976, de la loi sur les informations traitées automatiquement par ordinateur (LITAO). Cette loi, entrée en vigueur le 1er mars 1977, aborde pour la première fois la question de la sécurité des données numériques[28].

La LITAO a été abrogée, avec effet au 1er janvier 2010, par une modification de la LIPAD, qui ne contenait jusqu'alors que les dispositions en matière d'information et d'accès aux documents[29]. Bien que la LIPAD ait été modifiée à plusieurs reprises depuis le 1er janvier 2010, le système législatif général de la protection des données est resté le même jusqu'à aujourd'hui.

Les évolutions du cadre juridique international et national[30], ont conduit à une révision importante de la LIPAD, adoptée le 3 mai 2024 par le Grand Conseil (L 13347). La date d'entrée en vigueur de cette nouvelle loi doit encore être fixée par le Conseil d'État et une adaptation du RIPAD sera nécessaire. Cette révision de la LIPAD (« nLIPAD » dans les pages qui suivent) ne prévoit pas de changements fondamentaux en ce qui concerne les mesures techniques et organisationnelles nécessaires à la sécurité des données personnelles. Cependant, elle impose que ces mesures soient mises en œuvre dès la conception des traitements de données et introduit de nouvelles obligations, telles que la réalisation d'analyses d'impact pour les traitements à risque, la tenue d'un registre des traitements et le signalement des violations de sécurité des données au PPDT.

Il est à noter que la Cour a veillé à ce que les constats et recommandations du présent rapport soient cohérents avec les exigences du futur cadre juridique genevois.

---

[25] Art. 13A, al. 2 RIPAD.
[26] Art. 50 alinéa 1 LIPAD du 5 octobre 2001 / RS/GE A 2 08.
[27] Art. 52 LIPAD.
[28] Art. 4 LITAO du 17 décembre 1981 / B 4 35 : « *Les informations enregistrées doivent être protégées contre les risques de falsification, de destruction, de vol, de copie et d'accès illicites* ».
[29] Loi 9870 du 9 octobre 2008. Le projet de loi 9870 déposé par le Conseil d'État prévoyait une loi spécifique sur la protection des données, mais la commission judiciaire et de la police a décidé d'intégrer les dispositions sur la protection des données dans la LIPAD pour ne faire qu'un seul texte législatif comprenant les deux domaines (transparence et protection des données).
[30] En particulier le protocole d'amendement de la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel. Sur ces questions, voir l'exposé des motifs du projet de loi 13347, p. 25-30, https://ge.ch/grandconseil/data/texte/PL13347.pdf.

### 3.1.3 La sécurité des données lors de sous-traitance de données

Il y a une sous-traitance lorsqu'une entité fait appel à la collaboration de tiers pour traiter ses données. Dans de tels cas, les institutions demeurent responsables des données au même titre que si elles les traitaient elles-mêmes[31]. Ainsi, elles doivent prévoir des clauses contractuelles appropriées pour assurer la sécurité des données qu'elles font traiter et elles sont tenues de contrôler le respect des clauses contractuelles par le prestataire[32].

## 3.2. Définition d'une donnée personnelle et d'une donnée personnelle sensible

Selon l'article 4, lettre a) LIPAD, les données personnelles sont définies comme étant « *toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable* ».
Les données personnelles sensibles (art. 4, lettre b) LIPAD) constituent une catégorie particulière de données personnelles et concernent :

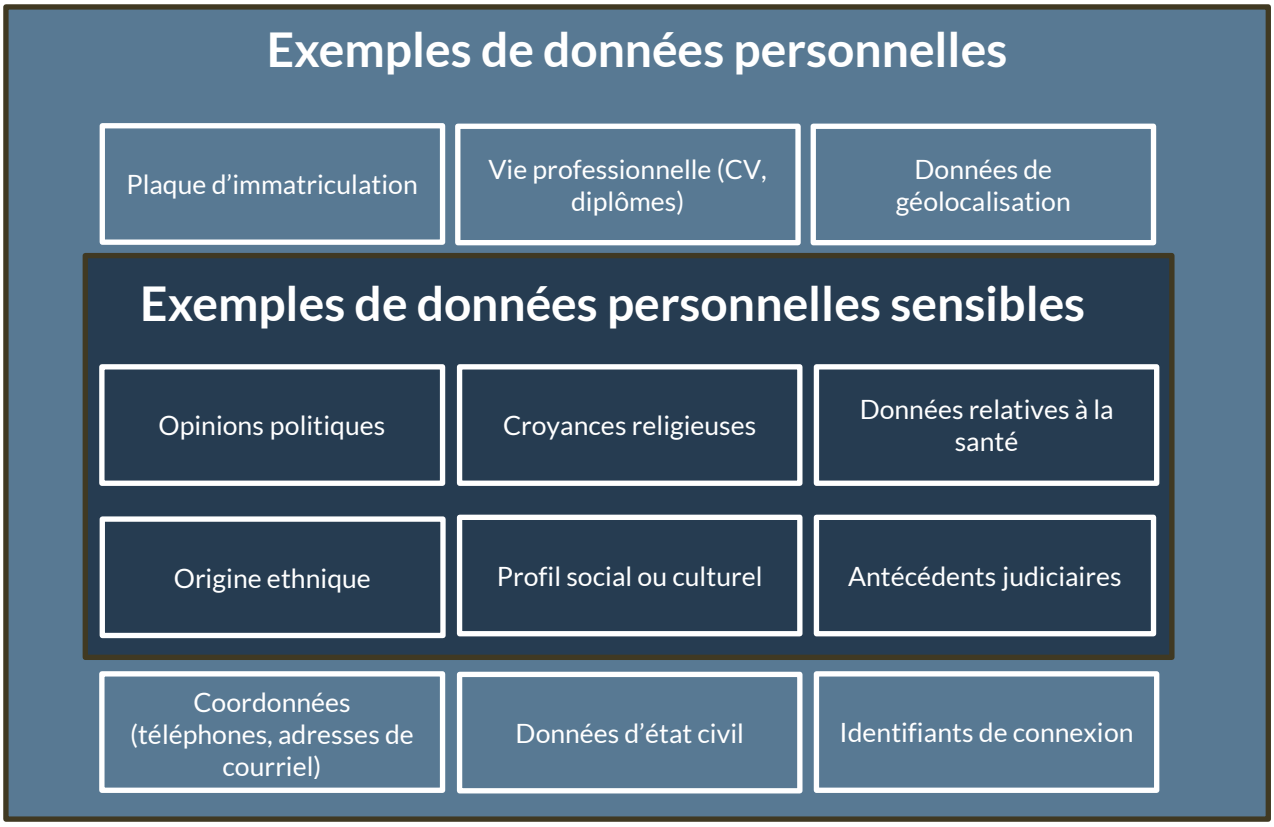
- les opinions ou activités religieuses, philosophiques, politiques, syndicales ou culturelles ;
- la santé, la sphère intime ou l'appartenance ethnique ;
- les mesures d'aide sociale ;
- les informations relatives aux poursuites ou sanctions pénales ou administratives.

Après son entrée en vigueur, la nLIPAD :

- supprimera les opinions ou activités culturelles ;
- remplacera « appartenance ethnique » par « origine raciale ou ethnique » ;
- ajoutera les données génétiques et les données biométriques identifiant une personne physique de façon unique.

[31] Art. 13A, al. 2 RIPAD.
[32] Art. 37, al. 2 et 3 LIPAD. L'article 13A, al. 3 RIPAD prévoit en outre que « *La sous-traitance de données personnelles fait l'objet d'un contrat de droit privé ou de droit public avec le prestataire tiers, prévoyant pour chaque étape du traitement le respect des prescriptions de la loi et du présent règlement ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant* ».

Figure 1 : Exemples de données personnelles et personnelles sensibles




Source : Cour des comptes, 2025

Les données personnelles sensibles revêtent une importance et une criticité particulières pour les citoyens. Ainsi, en toute logique, elles doivent être manipulées avec une précaution accrue et faire l'objet d'une protection renforcée.

Quand il est fait mention dans ce rapport de données personnelles, les données personnelles sensibles sont également concernées, sauf mention contraire explicite.

## 3.3. La sécurité des données d'un point de vue technique

### 3.3.1 Concepts liés à la sécurité des données

Au-delà des aspects juridiques évoqués précédemment, la sécurité des données comprend les processus et outils associés qui protègent les données, en transit (en cours de traitement ou transfert) ou au repos (stockées)[33]. Elle est une composante de la sécurité des SI au sens large. La sécurité des données vise à garantir (1) la disponibilité, (2) l'intégrité et (3) la confidentialité[34] des données.

Par ailleurs, il est important de comprendre la différence entre cybersécurité et sécurité informatique. La cybersécurité est une section limitée de la sécurité informatique. Si ces dernières années, la cybersécurité a pris une part importante dans l'actualité, elle se concentre principalement sur la protection face à des menaces externes, souvent venant d'internet. À l'inverse, la sécurité informatique a pour vocation de couvrir l'ensemble des menaces, incluant les erreurs ou fraudes internes, les risques liés aux prestataires, les risques environnementaux (inondation d'un centre de données par exemple), etc.

Les principaux risques auxquels sont exposées les données sont les suivants :
- Accès à des données personnelles par une personne non autorisée (interne ou externe à l'entité) ;
- Perte de données accidentelle (document perdu dans les transports publics, erreur dans une adresse mail de destination, etc.) ;
- Cyberattaque ayant pour but d'extraire ou de détruire des données ;
- Fuite de données à cause d'un prestataire ;
- Risques liés aux usages des ordinateurs et équipements par les collaborateurs (clé USB non sécurisée, utilisation d'ordinateur personnel, copie de données dans le *cloud* ou dans des outils d'intelligence artificielle) ;
- Risques liés à la sécurisation du poste de travail (possibilité d'installer des virus ou programmes malveillants, possibilité de corruption du poste, manque de blocage ou règle sur les usages interdits).

### 3.3.2 La sécurité des données dans la loi sur la protection des données

Comme évoqué précédemment, les exigences de la LIPAD et du RIPAD se veulent générales et indiquent simplement que les données personnelles doivent être protégées par des mesures appropriées. Pour l'administration cantonale, le RIPAD apporte un certain nombre de précisions, mais cela n'est pas le cas pour les communes.

Si ces exigences peuvent paraître imprécises, l'article 37, alinéa 2 LIPAD indique que les institutions doivent prendre « *par le biais de directives […] les mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données personnelles qu'elles traitent ou font traiter* ». Ainsi, **il appartient à chaque institution de décliner ces exigences** et de définir, par écrit, les mesures attendues, qu'elles soient techniques ou organisationnelles.

[33] Définition inspirée de celle proposée par Gartner (https://www.gartner.com/en/marketing/glossary/data-security), consultée le 27 août 2025.
[34] Ces objectifs sont par ailleurs précisés dans l'article 37, alinéa 2 LIPAD.

De plus, l'article 37, alinéa 1 LIPAD précise que les mesures de sécurité doivent être « appropriées ». Cela induit **la nécessité pour les institutions de préciser le niveau de sécurité global attendu**. La révision de la LIPAD de 2024 (qui n'est pas encore entrée en vigueur au moment où ce rapport est écrit) précise d'ailleurs ce point en indiquant que le caractère approprié des mesures doit être défini en « fonction des risques encourus »[35].

### 3.3.3 Standards et lignes directrices en termes de sécurité de l'information

De manière générale, plusieurs référentiels, guides ou standards (internationaux ou fédéraux) existent et peuvent aider les institutions dans la définition des mesures à implémenter en donnant des bonnes pratiques en termes de sécurité informatique.

La VdG n'ayant pas formellement adopté un standard en particulier, la Cour n'a pas basé son audit sur la revue détaillée des exigences d'un référentiel spécifique. Cependant, elle s'est inspirée en particulier des deux éléments suivants :

- Les normes internationales ISO 27 000[36] ;
- Le « Guide relatif aux mesures techniques et organisationnelles de la protection des données » publié par le préposé fédéral à la protection des données et à la transparence (PFPDT)[37].

Normes ISO 27 000

La norme ISO 27 001[38] spécifie les exigences pour la définition, la mise en œuvre, la maintenance et l'amélioration continue d'un système de management de la sécurité de l'information (ci-après « SMSI »). Le SMSI recense les mesures de sécurité pour garantir la protection des actifs d'une entité contre toute perte, vol ou altération. La norme prévoit une adoption de mesures proportionnées aux risques encourus, ce qui implique une approche proactive de la gestion des risques liés à la sécurité de l'information. L'application de cette norme dépend donc avant tout de l'analyse des risques et des objectifs fixés par l'entité, lui laissant ainsi une marge de manœuvre importante.

La norme ISO 27 002[39], complémentaire à l'ISO 27 001, fournit des lignes directrices pour la gestion de la sécurité de l'information. Elle prévoit des mesures pour plusieurs volets dont, l'évaluation des risques de traitement, les politiques et l'organisation de la sécurité de l'information, la sécurité des ressources humaines, le contrôle d'accès, les relations avec les fournisseurs ou encore la gestion des incidents.

---

[35] Art. 37A, al1 nLIPAD : « *Les institutions publiques doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru* ».
[36] Bien que, dans le cadre de sa politique de sécurité des systèmes d'information (ci-après « PSSI »), la VdG indique s'appuyer sur la famille des normes internationales relatives à la sécurité de l'information (ISO 27 000), elle ne s'engage pas explicitement à les mettre en œuvre.
[37] Préposé fédéral à la protection des données et à la transparence, (2024). Guide relatif aux mesures techniques et organisationnelles de la protection des données, Confédération Suisse. La dernière version disponible est celle du 15 janvier 2024, consultable via le lien suivant : https://www.edoeb.admin.ch/fr/23012024-guide-tom-disponible.
[38] ISO/IEC 27001, (2022). Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences. Genève : International organization of standardization.
[39] ISO/IEC 27002, (2022). Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information. Genève : International organization of standardization.

Guide relatif aux mesures techniques et organisationnelles de la protection des données

Ce guide, aussi appelé TOM, est publié par le PFPDT. Il constitue une introduction aux risques et solutions liés à la protection des données dans les SI actuels. Les thèmes principaux de la protection des données sont présentés sous l'angle des mesures techniques et organisationnelles envisageables, comme le chiffrement, l'anonymisation, l'authentification, etc. Il est conçu comme une aide pour la mise en œuvre de mesures adéquates afin d'assurer une protection optimale et appropriée des données personnelles. À titre d'illustration, il traite la sécurité des supports et celle des postes de travail de la façon suivante :

Figure 2 : Premier exemple de mesures préconisées par le TOM, au sujet de la sécurité des supports

Les données ne sont pas seulement mémorisées sur les serveurs centraux et les ordinateurs personnels. De nombreux supports externes permettent de transférer de l'information entre collaborateurs ou vers l'extérieur sans avoir à passer par le réseau. Des sauvegardes temporaires et limitées sont également possibles sur ces supports.

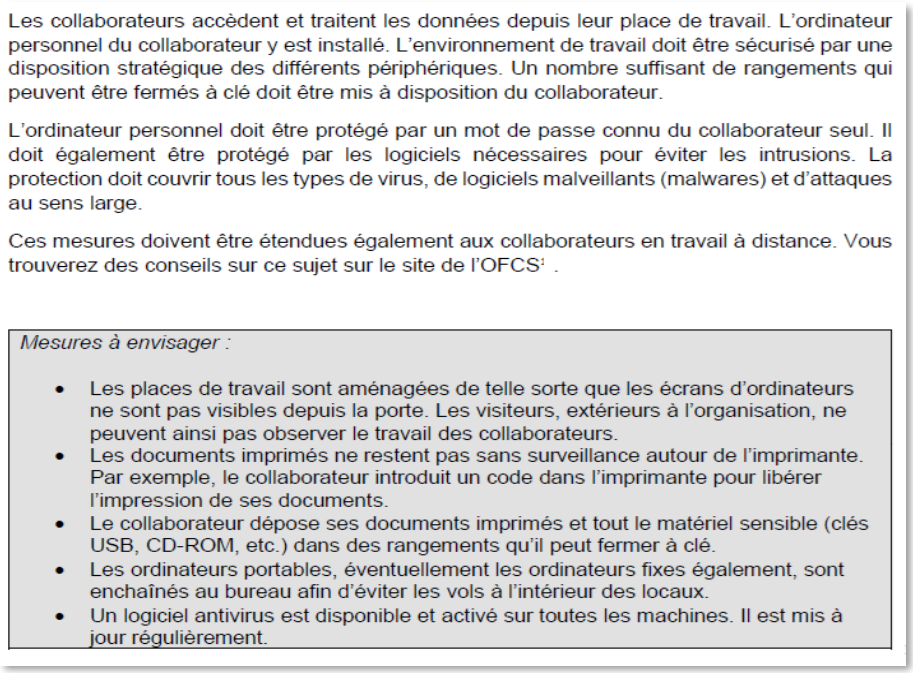
Parmi les supports externes, les clés USB, les disques durs externes, les CD-ROM, etc. ont des fonctions diverses puisqu'ils n'ont pas tous les mêmes propriétés. Certains sont réinscriptibles, comme les clés USB, d'autres ne le sont pas, comme les CD-ROM. Il est possible de stocker une quantité de données toujours plus importante sur un support toujours plus petit. Il faut garder cela à l'esprit pour ne pas sous-estimer les risques liés à ces supports.

*Mesures à envisager :*

- Les collaborateurs sont formés aux dangers d'introduire un support inconnu (clé USB, …) dans son ordinateur.
- Les supports externes contenant des données personnelles sensibles ou des profilages sont chiffrés.
- Les supports externes doivent être mis sous clé.
- Une procédure de destruction des supports est mise en place et les outils nécessaires à cette destruction sont disponibles.
- Une revue régulière de la configuration et des mises à jour est prévue.

Source : extrait du TOM, janvier 2024, page 42.

Figure 3 : Deuxième exemple de mesures préconisées par le TOM, au sujet de la sécurité des places de travail



Les collaborateurs accèdent et traitent les données depuis leur place de travail. L'ordinateur personnel du collaborateur y est installé. L'environnement de travail doit être sécurisé par une disposition stratégique des différents périphériques. Un nombre suffisant de rangements qui peuvent être fermés à clé doit être mis à disposition du collaborateur.

L'ordinateur personnel doit être protégé par un mot de passe connu du collaborateur seul. Il doit également être protégé par les logiciels nécessaires pour éviter les intrusions. La protection doit couvrir tous les types de virus, de logiciels malveillants (malwares) et d'attaques au sens large.

Ces mesures doivent être étendues également aux collaborateurs en travail à distance. Vous trouverez des conseils sur ce sujet sur le site de l'OFCS[1] .

*Mesures à envisager :*

- Les places de travail sont aménagées de telle sorte que les écrans d'ordinateurs ne sont pas visibles depuis la porte. Les visiteurs, extérieurs à l'organisation, ne peuvent ainsi pas observer le travail des collaborateurs.
- Les documents imprimés ne restent pas sans surveillance autour de l'imprimante. Par exemple, le collaborateur introduit un code dans l'imprimante pour libérer l'impression de ses documents.
- Le collaborateur dépose ses documents imprimés et tout le matériel sensible (clés USB, CD-ROM, etc.) dans des rangements qu'il peut fermer à clé.
- Les ordinateurs portables, éventuellement les ordinateurs fixes également, sont enchaînés au bureau afin d'éviter les vols à l'intérieur des locaux.
- Un logiciel antivirus est disponible et activé sur toutes les machines. Il est mis à jour régulièrement.

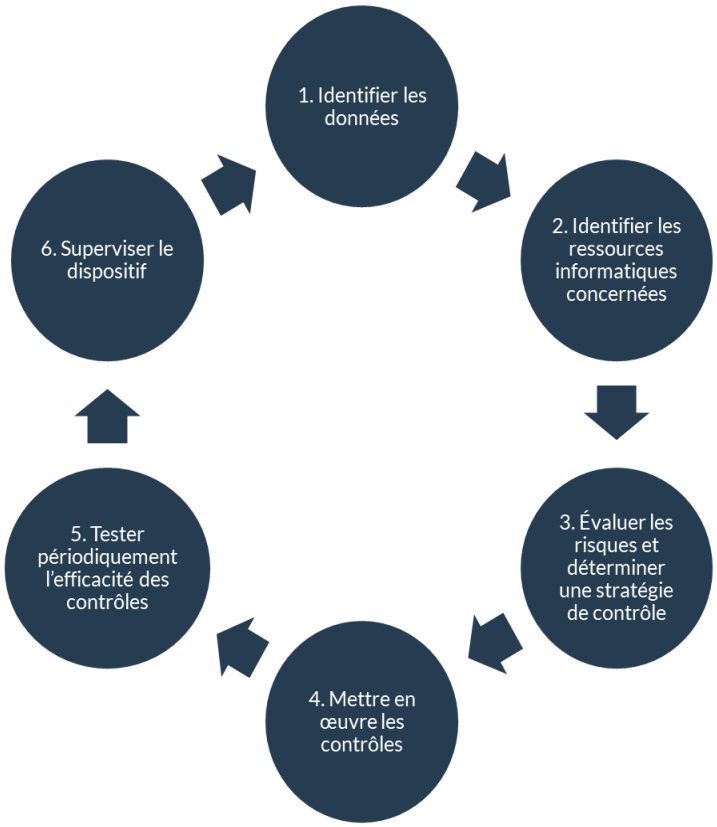
Source : extrait du TOM, janvier 2024, page 34.

Ce guide est par ailleurs cité en référence par le PPDT dans sa « fiche info » du 29 janvier 2019 sur les aspects juridiques et pratiques de la sécurité des données.

### 3.3.4 La logique de mise en œuvre de la sécurité des données

De manière générale, la plupart des méthodologies de gestion de la sécurité des données ont la même approche quant à la logique de définition, de mise en œuvre et de supervision des dispositifs de sécurité. Elle peut se résumer au travers du schéma ci-dessous :

Figure 4 : La logique de gestion de la sécurité des données




Source : Cour des comptes, 2025

### 3.3.5 Des mesures organisationnelles et techniques (contrôles)

En préambule, il convient de souligner que, dans ce rapport, **le terme « contrôle » fait référence à l'ensemble « *des mesures organisationnelles et techniques* »** au sens de l'article 37, alinéa 2 LIPAD. Cela comprend, par exemple :

- la définition d'une consigne (exemple : les collaborateurs ne sont pas autorisés à télécharger des données personnelles sensibles vers une plateforme de stockage *cloud*) ;
- la mise en place de mesures techniques (exemple : l'accès à une plateforme de stockage *cloud* est bloqué techniquement) ;
- la définition d'une pratique de travail (exemples : les tests informatiques sont faits sur des données synthétiques ou anonymisées[40], les collaborateurs ne doivent pas laisser de documents confidentiels sur leur bureau le soir) ;

[40] Il s'agit d'une bonne pratique à mettre en place pour que les collaborateurs de l'informatique ou des externes n'accèdent qu'aux données qui leur sont nécessaires dans la réalisation de leur tâche (il s'agit du principe du « *need-to-know* »).

- la mise en place de mesures détectives (exemple : si un collaborateur transfère de manière inhabituelle une grande quantité de fichiers classés comme confidentiels vers l'extérieur, une alerte est envoyée à son responsable ou à l'équipe de sécurité informatique) ;
- des processus de revue (exemple : un juriste revoit les contrats avant qu'ils ne soient signés pour s'assurer de choses particulières) ;
- des mécanismes de supervision (exemple : quelqu'un est en charge de vérifier que les données sont bien chiffrées ou que les prestataires respectent bien les exigences contractuelles).

De manière générale, la distinction peut être faite entre les mesures techniques et organisationnelles. Les mesures techniques se rapportent directement aux outils et contraintes mécaniques existants dans les SI (anonymisation, chiffrement, authentification renforcée, blocage technique, etc.). Les mesures organisationnelles couvrent un périmètre plus large et se rapportent plutôt à l'environnement autour du SI, à ses utilisateurs et à la manière dont il est utilisé (règles et procédures internes, registre des traitements et des activités, sensibilisation, supervision, etc.).

## 3.4. La sécurité des données personnelles en VdG

### 3.4.1 La nature des données traitées en VdG

Les services de l'administration municipale sont amenés à traiter des données personnelles à travers les nombreuses prestations délivrées à la population. Par exemple[41]:

- des données telles que le nom, prénom, adresse personnelle, numéro de carte d'identité ;
- des données sensibles telles que la liste des infractions, des plaintes et le statut de sans-papiers (par le service de la police municipale), des informations liées à la santé (capacité de travail), au casier judiciaire (par la section ressources humaines du service juridique), des informations liées aux procédures civiles, pénales et administratives (par le service de l'État civil) ou encore les informations liées aux allocations de prestation sociale diverses perçues par les familles (par le service de la petite enfance)[42].

### 3.4.2 Historique de la sécurisation des données en VdG

Depuis 2012, la VdG a engagé plusieurs démarches pour appliquer les dispositions légales sur la protection des données personnelles, à commencer par l'adoption de la Directive d'application de la LIPAD. En 2020, la Politique de sécurité des systèmes d'information (PSSI) est adoptée et s'accompagne de la mise en place d'une gouvernance propre aux questions liées à la sécurité de l'information, avec des comités dédiés.

En 2024, la VdG a réalisé une analyse visant à identifier d'éventuels écarts avec les nouvelles exigences de la nLIPAD. Un groupe de travail dédié a ainsi défini un plan d'action

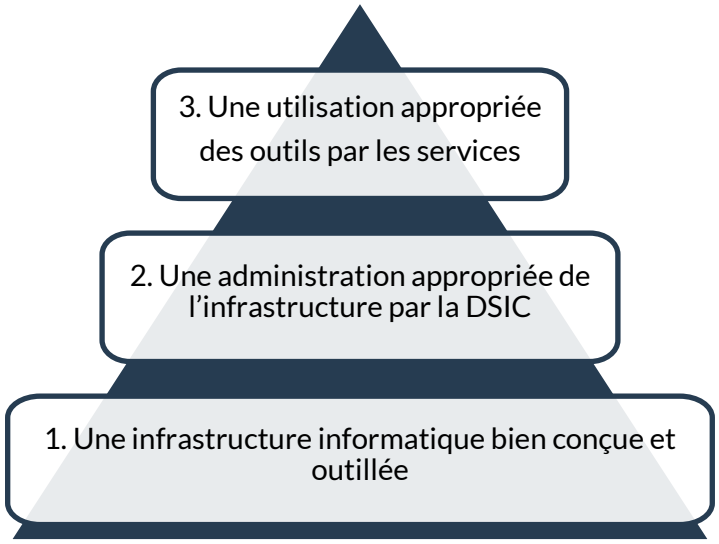
[41] Ces exemples sont tirés du catalogue de données gérées par le Préposé cantonal à la protection des données et à la transparence, sur la base des informations transmises par la VdG (http://outil.ge.ch/chacatfich/#/catalog/institution/228/302).
[42] Cette liste provient du registre des activités de traitement remis annuellement au PPDT. Il s'agit de quelques exemples d'informations collectées/traitées par les services de la VdG.

listant les évolutions nécessaires. Au moment de la rédaction de ce rapport, le plan d'action a été validé et est en cours de mise en œuvre par la VdG. L'un des points centraux est le recrutement d'un collaborateur spécialisé et dédié à la protection des données personnelles.

### 3.4.3 Des risques liés aux informaticiens et aux utilisateurs des systèmes

D'un point de vue opérationnel, l'objectif de sécurité des données repose sur deux éléments complémentaires : d'une part, la plateforme informatique doit être adéquatement sécurisée via des outils et des processus de gestion appropriés, d'autre part, les collaborateurs, simples utilisateurs de l'informatique, doivent adopter des habitudes de travail permettant de limiter les risques liés aux données.

Figure 5 : Les attentes en matière de sécurité des données

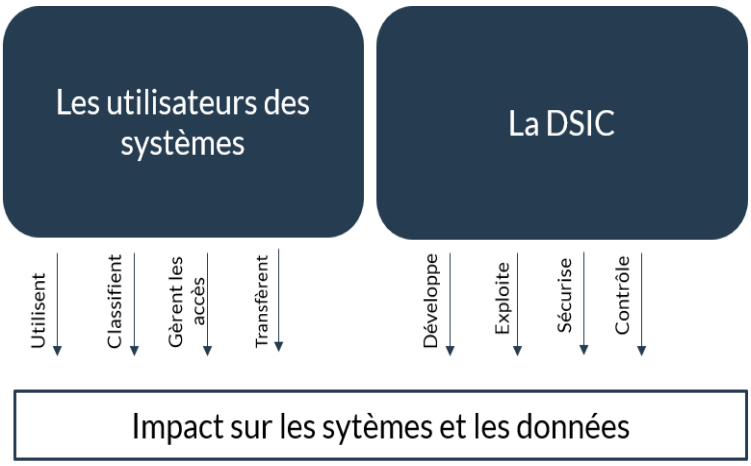



Source : Cour des comptes, 2025

La Direction des systèmes d'information et de communication (DSIC) doit garantir la sécurité des données lors des processus de gestion de la plateforme informatique (gestion de la salle serveur, des systèmes d'exploitation, des bases de données, des cyberattaques, des ordinateurs, etc.). Ses activités sont régies par la PSSI et les directives et procédures internes à la DSIC.

Au sein des services métiers, les utilisateurs des SI jouent un rôle important, souvent sans le savoir, dans la sécurité des données. En effet, ils interviennent dans la classification et le stockage des fichiers, leur transmission en interne ou vers l'extérieur (aussi bien par courriel ou via des plateformes de partage, des clés USB, etc.), l'impression et le stockage d'information sur papier. Plus largement, leur utilisation des outils modernes et d'internet de manière générale (réseaux sociaux, solutions *cloud*, etc.) peut avoir un impact significatif sur la sécurité des données personnelles.

Figure 6 : Les différentes activités ayant un impact sur les données




Source : Cour des comptes, 2025

### 3.4.4 L'organisation décentralisée de la VdG

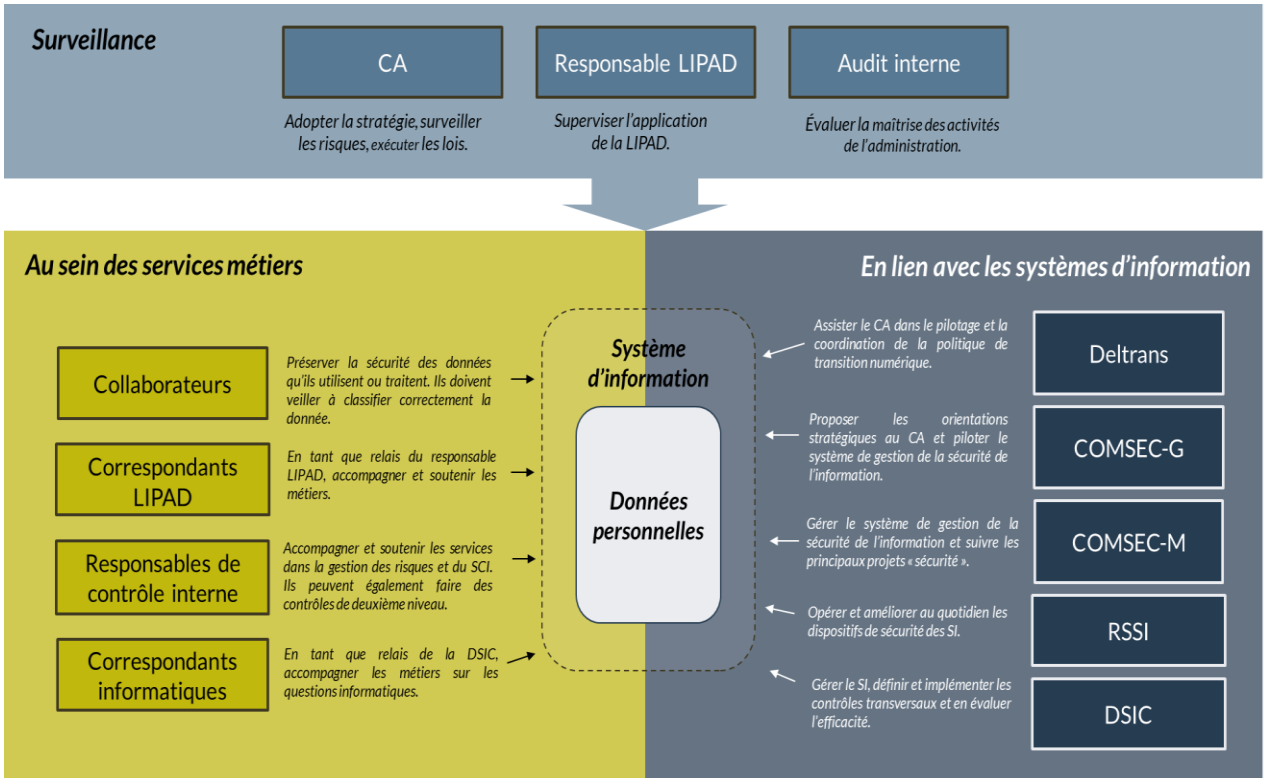
La VdG compte près de 4'000 collaborateurs qui travaillent au sein d'une quarantaine de services répartis dans cinq départements. De manière générale, l'administration municipale fonctionne de façon décentralisée : des directives transversales donnent des lignes directrices, mais les départements et les services disposent d'une grande marge de manœuvre pour définir le cadre de travail le plus approprié à leurs besoins et à leurs enjeux respectifs.

La définition de règles communes applicables à l'ensemble des collaborateurs de la VdG n'est pas aisée, étant donné la grande diversité de missions et de services qu'elle offre.

### 3.4.5 Les rôles des acteurs en VdG

De nombreux acteurs sont concernés par la sécurité des données personnelles, soit parce que leur métier les amène à traiter des données, soit parce qu'ils contribuent à la gestion ou à la sécurisation des SI. La figure 7 ci-dessous présente de manière synthétique les différents acteurs et leurs responsabilités dans la sécurité des données en VdG.

Figure 7 : Rôles et responsabilités en lien avec la sécurité des données personnelles




Source : Cour des comptes, 2025

Ci-dessous, le tableau 1 reprend les rôles et les responsabilités prévus par le *corpus* procédural de la VdG en matière de sécurité de la donnée personnelle.

Tableau 1 : Rôles et responsabilités appliqués aux étapes de gestion de la sécurité des données

| Étapes | Rôles et responsabilités |
|---|---|
| Définition d'une stratégie de sécurité de la donnée personnelle | La **DSIC**[43] **et en particulier le responsable de la sécurité informatique (RSSI)**[44] préparent des propositions en lien avec la stratégie de sécurité de l'information (incluant les données personnelles) et les soumet au **Comité de Sécurité – Gouvernance** (COMSEC-G). Ce dernier s'assure de la cohérence de la stratégie de sécurité avec la stratégie globale de l'administration. Les axes stratégiques ainsi définis sont proposés au **CA**.<br><br>Le **CA** a la responsabilité d'adopter la stratégie en veillant au fait qu'elle soit proportionnelle aux risques encourus. |
| Définition des contrôles | La **DSIC** a la responsabilité de définir les mesures de sécurité informatique transversales. La PSSI précise que toutes les directives générales, instructions de service et instructions transversales relatives à la sécurité de l'information doivent être rédigées et régulièrement mises à jour par le **RSSI,** en particulier.<br><br>En parallèle, les **directions de services** sont responsables de mettre en place, documenter et maintenir le système de contrôle interne (SCI) relatif à leurs activités et prestations de manière générale. Pour les sujets en lien avec la sécurité des données, ils sont en particulier chargés d'identifier les données personnelles qu'ils traitent et de gérer les accès aux applications ainsi que la sécurité physique de leurs espaces de travail. |
| Mise en œuvre des contrôles | La **DSIC** (principalement le RSSI) a la responsabilité de déployer les mesures de sécurité et de suivre leur implémentation.<br><br>Par ailleurs, le *corpus* procédural attribue aux **utilisateurs des SI** la responsabilité permanente d'assurer la sécurité des données qu'ils traitent. Ils doivent également veiller à classifier correctement les données en fonction de leur niveau de sensibilité. |
| Évaluation et tests de l'efficacité des contrôles | La PSSI prévoit que l'efficacité des contrôles liés à la sécurité informatique doit faire l'objet d'une évaluation régulière par la **DSIC**. Par ailleurs, les **responsables de contrôle interne** (RCI) ont pour mission de suivre l'efficacité et le bon fonctionnement du SCI de manière générale. |
| Surveillance de l'application de la loi | La directive générale relative à l'application de la LIPAD confie **au responsable LIPAD** de la VdG, la responsabilité de superviser la mise en œuvre de la loi au sein de l'administration municipale. La directive prévoit également, de manière facultative, la nomination **de conseillers à l'information** qui agissent comme des relais du **responsable LIPAD** dans leur service ou département.<br><br>Enfin, la directive générale sur le SCI prévoit que le CFI, en tant que service d'audit interne, pourrait être amené à revoir la sécurité des données en lien avec sa responsabilité d'évaluer la maîtrise des activités de l'administration. |

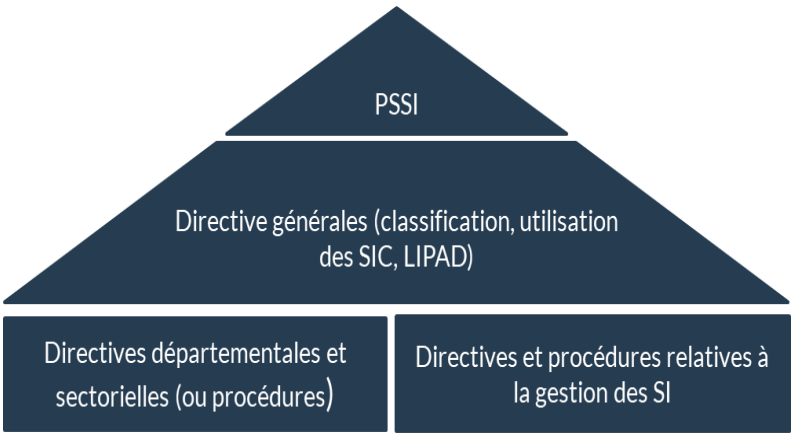
Analyse : Cour des comptes, 2025

[43] La DSIC compte 102.5 ETP en 2025.
[44] Les tâches du RSSI représentent 2 ETP en 2025 (un responsable de la sécurité informatique et un ingénieur sécurité).

### 3.4.6 Règles et procédures internes

Concernant la sécurité des données, les principales règles applicables en VdG sont définies au sein de trois directives transversales : celle sur la classification de l'information, celle sur l'utilisation des SIC et celle sur la LIPAD. La VdG s'est également dotée d'une politique de sécurité des systèmes d'information (PSSI). De plus, chaque département ou service peut définir des règles spécifiques (par exemple, dans leurs manuels de contrôle interne).

Figure 8 : La structure du *corpus* procédural




Source : Cour des comptes, 2025

**Politique de sécurité des systèmes d'information**

Le Conseil administratif de la VdG a validé une politique de sécurité des systèmes d'information (PSSI) le 4 mars 2020. Elle a pour vocation de poser un cadre, en fixant les objectifs, le périmètre, les règles ainsi que les responsabilités nécessaires à sa mise en œuvre. La PSSI aborde les sujets clés devant permettre la protection des données sensibles, comme la gestion des risques, des ressources humaines nécessaires, des actifs informatiques ou encore la sécurité des échanges d'information et la traçabilité. Le document liste les règles et mesures générales de sécurité des SI sans toutefois détailler les mesures techniques à mettre en œuvre. Il est précisé que la PSSI doit être complétée par des directives et suivie de plans d'action spécifiques. Le document indique également que l'efficacité des mesures de protection techniques, organisationnelles et légales doit être régulièrement contrôlée et mesurée, notamment par la DSIC. Enfin, la PSSI établit que les collaborateurs doivent être sensibilisés ou formés à la sécurité et aux risques pesant sur les SI en adéquation avec les fonctions qui leur sont attribuées.

**Directive générale relative à l'utilisation des systèmes d'information et de communication (DGUSIC)**

Il existe également une directive générale relative à l'utilisation des SIC, dont la dernière modification date du 1er avril 2019, laquelle prévoit notamment des mesures de chiffrement systématiques par la DSIC pour les données qui sortent de l'administration municipale. Enfin, le chiffrement des courriels échangés en interne et contenant des informations confidentielles est recommandé, mais pas systématique.

### Directive générale relative à l'application de la LIPAD

La VdG s'est dotée d'une directive générale relative à l'application de la LIPAD en date du 31 octobre 2012. Elle se focalise sur le volet transparence de la loi et précise les modalités d'accès et de consultation des données personnelles, par les citoyens. La directive indique également que la DSIC doit prendre les dispositions nécessaires pour assurer en tout temps la disponibilité, l'intégrité et la confidentialité des données personnelles figurant sur les serveurs de la VdG. Elle indique aussi que chaque institution doit adopter les « *mesures commandées par les circonstances* » pour que les données personnelles en sa possession ne puissent être consultées, manipulées, complétées ou effacées que par les personnes exclusivement habilitées.

### Directive générale relative à la classification et la protection de l'information numérique

Une autre directive transversale portant sur la classification et la protection des données numériques définit les principes et les règles d'accès des données. Validée par le CA de la VdG à l'automne 2024, elle prévoit trois niveaux de confidentialité (public, restreint, confidentiel) attribués par l'utilisateur. Pour les informations classées confidentielles, la seule mesure de sécurité exigée est la mise en place d'un filigrane « confidentiel » sur le document. La directive évoque aussi la « possibilité » pour l'utilisateur de chiffrer un courriel.

Figure 9 : Niveaux de confidentialité de la donnée prévus par la directive générale sur la classification et la protection de l'information numérique

| Niveau | Description | Exemples | Bon usage |
|---|---|---|---|
| C1 - Public | Concerne toute information non confidentielle dont la diffusion non contrôlée ne cause pas préjudice à la Ville ou au-x tiers qu'elle concerne. | Publication site internet ;<br>Communiqués de presse ;<br>Fiche d'une œuvre sur un site de collection ;<br>Lettre d'information ;<br>Information à la population<br>Règlements de la Ville publiés sur Internet. | Je peux librement diffuser l'information. |
| C2 – Restreint VDG | **Label par défaut**, concerne toute information non confidentielle mais dont la diffusion non contrôlée ou sans respect du secret de fonction pourrait causer des dommages à la Ville ou au-x tiers dont la Ville est responsable des données. | Directives et communications internes ;<br>Données personnelles (hors sensibles) ;<br>Factures entrantes, bons de paiement, factures sortantes ;<br>Contrats (prestataires, partenariats etc.) ;<br>Organigrammes détaillés ;<br>Inventaires (mobilier, fournitures etc.). | Je ne dois pas diffuser l'information en dehors de la Ville de Genève hors mesure justificative (prestation avec une autre institution, contrat formel avec une entreprise, prestation pour un citoyen ou une citoyenne etc.) |
| C3 – Confidentiel | Information **sensible** dont la diffusion en dehors d'un cercle restreint de personnes habilitées et hors secret de fonction pourrait porter préjudice à la Ville ou au-x tiers dont la Ville est responsable des données. | Ressources humaines (certificats médicaux, gestion de carrière, évaluation etc.) ;<br>Documents relevant du secret de fonction ;<br>Projets d'appel d'offres ;<br>Rapports de police ;<br>Petite enfance (listes inscriptions crèches, informations relatives à des mineurs),<br>Information sur l'aide sociale de citoyen-ne ;<br>Documents couverts par le secret des affaires | Je ne dois pas diffuser l'information en dehors du cercle de confidentialité de celle-ci, généralement quelques personnes. |

Source : Directive générale sur la classification et la protection de l'information numérique, VdG, 2024, p.7.

**Autres directives**

D'autres directives ou règlements portant sur des questions plus spécifiques ont également été adoptés (vidéosurveillance, assermentations, gestion des autorisations SAP, modalités d'accès aux données personnelles dans les structures d'accueil de la petite enfance, instruments de gestion des documents).

### 3.4.7 La gouvernance de la sécurité

La gouvernance de la sécurité des SI en VdG est assurée par plusieurs instances.

Au quotidien, la sécurité des données est traitée par le RSSI.

À un niveau **stratégique**, le COMSEC-G (« Comité de Sécurité – Gouvernance »)[45] s'assure que la stratégie de sécurité est alignée avec la stratégie globale de l'administration municipale. Il propose au CA les axes stratégiques à inscrire dans le cadre du plan informatique stratégique quadriennal. Il se réunit deux fois par an. Les éléments à portée stratégique sont validés par la CA.

De manière générale, la gestion de la sécurité des données est intégrée dans la gouvernance de la sécurité des SI. Les différents projets et initiatives s'inscrivent dans la démarche de transformation numérique de la VdG. Cette dernière est encadrée par un plan directeur pluriannuel. Le CA, par l'intermédiaire de sa Délégation à la transition numérique[46] **(DelTrans**), s'assure que les projets numériques soient cohérents avec le programme de législature et supervise la répartition des crédits financiers entre les différents portefeuilles de projets.

Enfin, d'un point de vue **opérationnel**, l'organe de gestion de la sécurité est le COMSEC-M (« Comité de Sécurité – Management ») [47]. Il est organisé et animé par le RSSI. Il s'assure du bon fonctionnement des dispositifs et suit les principaux projets. Il se réunit chaque trimestre.

### 3.4.8 Un renforcement récent des mesures techniques en place en VdG

La Cour note que la VdG a, au cours des dernières années, renforcé ses dispositifs de sécurité de l'information. Par exemple, la VdG dispose maintenant d'un outil accompagnant le processus de classification des documents (évoqué précédemment). Un centre de sécurité opérationnelle à également était implémenté. Il permet de mieux suivre les éventuels évènements malicieux sur l'infrastructure informatique et de réagir rapidement. La Cour peut également citer le projet de revue des droits d'accès qui est aussi en cours.

[45] Ce comité est composé du secrétaire général de l'administration municipale, du chef de service juridique de la VdG, du directeur du département de rattachement de la DSIC, du directeur de la DSIC, du gestionnaire des risques de la VdG et du RSSI.
[46] La délégation est notamment composée du maire de la VdG, du magistrat et du directeur en charge du département de tutelle de la DSIC, du directeur de la DSIC. Des collaborateurs sont conviés sur invitation en fonction des sujets à l'ordre du jour.
[47] Il est composé du directeur de la DSIC, des adjoints d'unité de la DSIC, des conseillers de direction de la DSIC et du gestionnaire des risques de la VdG. Il se réunit sur une base trimestrielle.

### 3.4.9 La gestion des risques

L'article 221, alinéa 3, de la constitution de la République et canton de Genève (Cst-GE, A 2 00) prévoit que les communes doivent instituer un organe de contrôle interne.

L'article 125 de la loi sur l'administration des communes (LAC, B 6 05,) précise les exigences liées à l'institution d'un système de contrôle interne (SCI) et donne à l'organe exécutif (soit le CA) la responsabilité d'adopter un tel système. Ce SCI doit :
*« a) assurer la qualité des prestations fournies par une entité dans le respect des lois, règlements, directives et autres normes en vigueur ;*
*b) assurer la qualité des processus visant à fournir ces prestations ;*
*c) gérer les risques découlant de l'activité de l'entité. »*[48]

En VdG, la directive générale relative au SCI entrée en vigueur en 2015, cadre les composantes clés de la gestion des risques, en particulier l'identification, l'évaluation et la validation des risques. Elle précise que les services doivent identifier et évaluer les risques généraux de gestion relatifs à leurs missions et leurs activités, au moins une fois par an. Ils établissent également des plans d'action pour couvrir les risques identifiés, lorsque cela se révèle nécessaire. Les responsables du contrôle interne (RCI) des départements et le gestionnaire de risques accompagnent les chefs de service dans ce processus.

Les inventaires et les cartographies des risques sont validés par les chefs de service et les directions de département. De plus, les risques évalués comme « élevés » sont suivis par le Comité de direction (CODIR)[49] semestriellement. Le CA supervise l'ensemble du dispositif ainsi que les risques institutionnels et critiques.

Ce processus de gestion des risques s'applique à l'ensemble des risques en VdG et donc également à ceux liés à la sécurité des données personnelles.

## 3.5. Limitation du périmètre d'intervention

La Cour tient à rappeler que le présent audit se concentre sur la sécurité des données personnelles et l'application de l'article 37 de la LIPAD. Ainsi, la Cour n'a pas revu en détail les autres aspects de la loi, notamment ceux liés à la vidéosurveillance (article 42 LIPAD), à l'exhaustivité du catalogue de fichier (article 43 LIPAD) ou au rôle de surveillance du PPDT (chapitre II, LIPAD).

Par ailleurs, les travaux de la Cour ont consisté à identifier les mesures mises en œuvre par la VdG et à apprécier leur cohérence avec les objectifs fixés. À l'inverse, les procédures d'audit réalisées par la Cour ne permettent pas de garantir l'efficacité opérationnelle des dispositifs ou contrôles en place. À titre d'illustration, la Cour n'a pas essayé d'exfiltrer des données sensibles pour voir si les mesures en place auraient pu l'en empêcher.

[48] Art. 125 de la LAC.
[49] Le secrétaire général, le secrétaire général adjoint, les directeurs de départements, le directeur des ressources humaines et le directeur des finances forment le CODIR.

# 4. Constats et recommandations

À titre préliminaire, il est important de préciser que les travaux de la Cour n'ont pas identifié de cas significatifs 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, les travaux de la Cour ont permis d'établir qu'avant son intervention, des mesures ont été prises par la VdG pour réduire le nombre d'accès étendus, assurer la traçabilité des actions réalisées et mettre en place des processus de validation d'accès. Ainsi, le cadre de contrôle sur ces aspects apparaît suffisant au moment de notre intervention.

D'autres allégations portaient sur le fait que le dispositif de sécurité mis en œuvre autour des données personnelles ne serait pas conforme aux dispositions de la loi. Les constats présentés ci-dessous traitent précisément de ce sujet.

## 4.1. Constat 1 : les risques liés à la sécurité des données personnelles ne sont pas suffisamment connus, analysés et remontés

### Quel est le constat de la Cour ?

La VDG **ne dispose pas d'une vision complète des risques liés à la sécurité des données personnelles**. Le niveau actuel de maîtrise des risques, résultant des contrôles en place, n'est que partiellement connu et remonté au CA au travers des processus de gestion des risques existants. En effet, plusieurs dimensions de la sécurité des données (détaillées ci-après) ne sont pas prises en compte.

De plus, **l'appétence au risque de la VdG concernant la sécurité des données personnelles n'est pas suffisamment claire** pour guider les efforts à mener en la matière**.** Or, sans décision sur le niveau de risque acceptable en termes de sécurité des données personnelles, le caractère approprié des mesures en place ne peut pas être apprécié.

Une évaluation complète des risques encourus et une définition claire de l'appétence au risque sont deux éléments de base indispensables pour définir des mesures organisationnelles et techniques appropriées (au sens de l'article 37, al. 1 LIPAD).

### Pourquoi ce constat est-il important ?

L'article 37, alinéa 1 LIPAD indique que les « *données personnelles doivent être protégées contre tout traitement illicite par des mesures organisationnelles et techniques* ***appropriées*** ». Or, ni la LIPAD, ni le RIPAD en ce qui concerne les communes ou même d'éventuelles consignes du PPDT n'indiquent clairement les mesures techniques à implémenter. Seule l'exigence d'une approche proportionnelle aux risques est sous-entendue par la loi

actuelle. La modification de la nLIPAD prévoira expressément, après son entrée en vigueur, que la sécurité adéquate doit être définie par rapport aux risques encourus[50].

Dès lors, **il est nécessaire de (1) connaître les risques auxquels la VdG est exposée et de (2) définir un niveau de sécurité cible** (en fonction de l'appétence au risque). Sans ces éléments, la VdG ne peut ni concevoir ni implémenter une stratégie de contrôle appropriée (voir le constat 2). De plus, une remontée, d'information incomplète ou inexacte quant à l'exposition réelle aux risques pourrait mener à des décisions inadaptées ou empêcher la mise en œuvre de mesures correctrices en temps opportuns.

## Ce qui appuie le constat de la Cour

Le constat de la Cour s'appuie principalement sur les éléments suivants :

- L'appétence au risque du CA en matière de sécurité n'est pas précisément définie ;
- Les risques liés à la sécurité des données personnelles ne sont que partiellement identifiés et évalués (ainsi que l'efficacité des contrôles y afférents) ;
- Il n'existe pas de diagnostic ou d'audit quant au respect des dispositions de la LIPAD en matière de sécurité des données.

La Cour présente ci-dessous chacun de ces aspects plus en détail.

**De l'appétence au risque**

L'appétence au risque est définie comme le type et le niveau de risque global qu'une organisation est prête à accepter dans le cadre de la mise en œuvre de stratégie et de ses objectifs[51]. Dans le contexte de la VdG, l'appétence au risque traduit la tolérance au risque que le CA souhaite voir adopter par l'administration et qui, en retour, influence sa culture du risque, son mode de fonctionnement et les décisions prises.

La méthodologie de gestion des risques en VdG ne prévoit qu'un seul niveau d'appétence qui s'applique à l'ensemble des risques au sein de l'administration : seuls les risques ayant un niveau « modéré » ou inférieur sont acceptables. Les risques identifiés comme « élevés » ou « critiques » doivent faire l'objet de mesures appropriées de réduction, de partage ou d'évitement. La Cour relève que, lorsqu'on parle de sécurité des données personnelles, cette approche générale n'est pas suffisamment précise pour donner un cap clair à l'implémentation d'un ensemble de mesures de sécurité et pour permettre un pilotage éclairé et guider les décisions.

À titre d'exemples, durant sa revue sur le terrain, la Cour a constaté qu'environ un tiers des collaborateurs (ceux disposant d'un ordinateur portable) sont administrateurs de leur poste informatique[52] ou qu'il est possible de transférer une grande quantité de données

[50] Art.37A, al. 1 LIPAD : « *Les institutions publiques doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru* ».
[51] Définition issue des normes internationales d'audit interne, Institute of Internal auditors, janvier 2024.
[52] Le fait d'être administrateur induit de nombreux risques en termes de sécurité informatique. Mitiger ces risques est souvent difficile et coûteux. Les bonnes pratiques préconisent de limiter ce droit au strict minimum, selon le principe du « moindre privilège ».

sans blocage ni alerte à la sécurité[53] aussi bien par clé USB que par des exports vers des sites de stockage en ligne (tels que Google Drive ou Microsoft OneDrive). Si la Cour ne se positionne pas quant au caractère approprié ou non de telles pratiques, elle soulève que l'absence de contrôle sur ces éléments semble démontrer une acceptation tacite du niveau de risque actuel auquel est exposé la VdG. Or, l'acceptation de cette exposition au risque ne devrait pas être tacite, mais clairement formalisée afin de garantir un pilotage éclairé.

**De l'évaluation des risques**

Chaque département et service de la VdG a la charge d'identifier et d'évaluer les risques propres à son activité. La finalité de cet exercice est d'identifier les risques dont le niveau est trop élevé (supérieur à l'appétence définie) afin que des mesures correctives (ou de mitigation) soient mises en œuvre pour réduire le risque à un niveau acceptable.

La Cour, sur la base de la revue des inventaires de risque et des rapports annuels sur les risques des dernières années, a constaté que les risques liés à la sécurité des données ne sont que partiellement identifiés et évalués. En particulier :

- le risque de perte ou de fuite de donnée personnelle (accidentelle ou malicieuse) ;
- les risques liés à la sécurité des données personnelles dans le cadre des sous-traitances (voir constat n°3) ;
- les risques liés à la communication ou au transfert de données personnelles quel que soit le support (courriel, clé USB, FTP[54], etc.) ;
- les risques liés aux accès des développeurs et des administrateurs informatiques à des données personnelles ;
- les risques liés à la sécurisation des postes utilisateurs ;
- les risques liés au fait de laisser des documents papier contenant des informations sensibles dans des locaux non sécurisés ;
- les risques liés aux accès en masse à des données sensibles.

De plus, la VdG ne dispose pas d'un répertoire des personnes ayant accès aux SI contenant des données personnelles. Outre le fait qu'il s'agisse d'une exigence du RIPAD[55], l'absence d'un tel répertoire ne permet pas d'avoir une vision claire sur l'étendue des accès attribués. Or, la correcte limitation des accès est un des éléments de base de la sécurité des données.

Enfin, une évaluation partielle des risques liés à la sécurité des données personnelles nuit à la capacité de la VdG : (1) de s'assurer de maîtriser ces risques dans les limites de l'appétence qu'elle s'est fixée, et (2) à prendre les mesures correctives nécessaires si besoin.

**De l'absence de diagnostic**

Le caractère approprié des mesures techniques et organisationnelles relatives à la sécurité des données (au sens de l'article 37 LIPAD) n'a jamais fait l'objet d'un diagnostic, d'une analyse détaillée ou d'un audit.

---

[53] À noter tout de même que des traces des évènements informatiques (« logs ») seront récupérables dans les outils de sécurité informatique, en cas d'investigation.
[54] FTP signifie « Protocole de Transfert de Fichiers » (File Transfer Protocol en anglais). C'est un protocole standard utilisé pour transférer des fichiers entre un ordinateur client et un serveur sur un réseau. En termes simples, il permet de copier des fichiers d'un ordinateur vers un autre.
[55] Art.13 (3) : « *Les institutions publiques tiennent à jour un répertoire des personnes ayant accès aux systèmes d'information contenant des données personnelles* ».

## Recommandation n° 1 :

Priorité : Élevée [56]

## Réaliser une évaluation plus détaillée des risques relatifs à la sécurité des données personnelles

La Cour recommande de réaliser une évaluation complète des risques relatifs à la sécurité des données personnelles en veillant à couvrir les dimensions suivantes :

- les risques liés aux pratiques de la DSIC (en particulier celles des administrateurs, des développeurs, des intervenants sur les environnements informatiques hors production[57]) ;
- les risques liés aux pratiques de travail des collaborateurs au sein des métiers et la manipulation des données (réception, transfert, traitement, suppression) ;
- les risques relatifs à la sécurité des postes de travail (ordinateur, accès aux services en ligne, protection physique des informations) ;
- les risques relatifs aux sous-traitances de traitement de données.

**Modalités possibles :**

- Identifier et formaliser l'ensemble des risques inhérents/bruts liés à la sécurité des données personnelles[58] ;
- Identifier les contrôles existants et évaluer leur efficacité ;
- Identifier également les risques pour lesquels la VdG n'a pas ou pas encore de contrôles suffisants ;
- Possiblement, prévoir un accompagnement des services par la DSIC ou se faire aider par une société externe.

**Livrables :**

- Diagnostic ou analyse des risques et des contrôles en lien avec la sécurité des données personnelles ;
- Mise à jour des inventaires des risques et contrôles.

**Avantages attendus :**

- Meilleure connaissance des risques auxquels la VdG est exposée ;
- Les contrôles (ou leur absence) sont évalués et le niveau de protection est communiqué de manière transparente aux instances appropriées ;
- La VdG dispose d'une analyse permettant d'identifier les zones où l'exposition au risque est supérieure à l'appétence (à définir) et de prioriser les efforts de remédiation ;
- La VdG dispose d'une analyse suffisante pour superviser les dispositifs en place ;
- Améliorer le niveau d'information remonté aux instances de gouvernance leur permettant d'exercer un pilotage éclairé (en lien avec la recommandation suivante).

[56] La priorité de cette recommandation est élevée, car une évaluation complète des risques est un prérequis nécessaire à la mise en œuvre de mesures appropriées au sens de la loi.
[57] Il s'agit principalement des environnements informatiques de « développement » et de « test ».
[58] En intégrant au minimum ceux listés dans la section « De l'évaluation des risques » de ce rapport.

*Recommandation 1 :* ☒ *acceptée* ☐ *refusée*

**Position de la Ville de Genève :**
Les niveaux de maturité des dispositifs de gestion des risques et de contrôle interne de la Ville de Genève ont fait l'objet, en 2025, de deux audits. Les niveaux de maturité ont été estimés, respectivement, à 2,6 et 2,5 sur une échelle de 3.

Les risques en lien avec la thématique traitée dans ce rapport figurent également dans certains inventaires des risques de la Ville mais pas de manière systématique.
Une revue spécifique à la sécurité des données personnelles sera donc réalisée dont la finalité sera l'établissement d'une matrice transversale de risques et de contrôles à mettre en œuvre dans les services.

Délai : 31.12.2026
Responsables : Groupe SCI, DSIC, en collaboration avec le DPO

Néanmoins, la Ville souhaite préciser que certains exemples utilisés par la Cour pour illustrer ces risques mériteraient d'être nuancés au regard des projets de remédiation déjà réalisés ou en cours comme l'élimination des droits d'administration des ordinateurs portables (déjà en place pour les conseillers municipaux), le déploiement généralisé et sécurisé de MS One Drive remplaçant les solutions privées comme Google Drive ou K-Drive ou encore la récolte systématique des traces de des périphériques de stockage connectés sur port USB.

## Recommandation n° 2 : Clarifier l'appétence au risque

Priorité : Élevée[59]

La Cour recommande de présenter l'analyse des risques (réalisée en recommandation n°1) au 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 sa tolérance au risque. Cette démarche permettra à l'exécutif de la VdG de clarifier son appétence au risque en matière de sécurité des données personnelles.

**Modalités possibles :**

- Préparer une synthèse des principaux risques, incluant des exemples concrets (via des scénarios par exemple) ;
- Présenter en particulier les risques liés aux usages ou aux pratiques pour lesquels la VdG a peu ou pas de mesure de protection ;
- Pour ces derniers, s'assurer que des mesures compensatoires soient convenues ou que le risque résiduel soit explicitement accepté par le CA.

**Livrables :**

- Analyse des risques communiquée au CA ;
- Validation formelle des risques évalués en dehors de la zone d'appétence (acceptation) définie et formalisation d'un plan d'action le cas échéant.

**Avantages attendus :**

- Le degré d'exposition de la VdG et les risques sont mieux connus ;
- Permettre à la DSIC de disposer d'un cap clair sur les mesures et le niveau de contrôle à implémenter ;
- Les risques résiduels sont approuvés à un niveau approprié de gouvernance[60] ;
- Un plan d'action est décidé en fonction des priorités fixées par le CA.

*Recommandation 2 :* ☒ *acceptée* ☐ *refusée*

**Position de la Ville de Genève :**
Cette recommandation sera traitée sur la base des travaux en lien avec la recommandation 1.

Délai : 31.03.2027
Responsables : Groupe SCI, DSIC, en collaboration avec le DPO

[59] La priorité de cette recommandation est élevée car il s'agit de fixer le cap et le niveau de sécurité attendus par le CA. Ces éléments permettront de guider l'ensemble des actions à venir.
[60] Les compétences en termes de validation des risques sont définies dans la méthodologie de gestion des risques de la VdG.

## 4.2. Constat 2 : la stratégie de contrôle autour des données personnelles n'est pas définie

### Quel est le constat de la Cour ?

La VdG n'a pas défini de stratégie de contrôle[61] transversale et homogène afin de garantir un niveau de sécurité approprié sur tout le cycle de vie de la donnée. De manière générale, la VdG ne dispose pas d'une vision d'ensemble sur les mesures en place et ne peut pas s'assurer de leur caractère approprié.

En effet, bien que plusieurs contrôles aient été implémentés pour assurer la sécurité des données, notamment **au sein de la DSIC**, ils ne sont (1) pas systématiquement documentés et (2) se concentrent principalement sur les risques cyber (menaces ou attaques venant de l'extérieur) sans couvrir les autres dimensions de la sécurité des données.

Par ailleurs, pour couvrir le risque dans sa globalité et ne pas se limiter aux simples processus informatiques, la stratégie de contrôle doit s'étendre **aux pratiques de travail des collaborateurs dans les services** et à l'utilisation qu'ils font des outils informatiques. En particulier, leur capacité à extraire des données, les stocker et les communiquer de manière sécurisée. Là aussi, bien que des mesures soient en place, la Cour note l'absence d'une stratégie complète et documentée.

Enfin, il existe peu de contrôle de second niveau ou de supervision visant à s'assurer que les principaux dispositifs en lien avec la sécurité des données fonctionnent de manière appropriée.

### Pourquoi ce constat est-il important ?

La définition d'une stratégie de contrôle est un élément clé pour s'assurer de couvrir les risques de manière appropriée. Elle permet de définir un niveau de contrôle attendu et uniforme sur tout le cycle de vie de la donnée.

En outre, la définition des contrôles et leur formalisation sont des éléments de base du contrôle interne qui permettront la mise en œuvre et le renforcement d'autres processus tels que l'évaluation des risques, la supervision du dispositif de sécurité établi ainsi que le pilotage.

Une stratégie de contrôle permet de définir une feuille de route et de guider les efforts et les investissements à venir en matière de sécurité des données. Une stratégie de contrôle alignée avec l'appétence au risque, permet de garantir de répondre avec efficience aux attentes du CA tout en donnant un cap pour l'implémentation de mesures techniques et organisationnelles appropriées.

Enfin, lorsque la mise en œuvre de mesures techniques ou organisationnelles est décidée, il est important que sa correcte implémentation et son bon fonctionnement au fil du temps

[61] Par « stratégie de contrôle », la Cour entend une vision globale, même sommaire, des mesures (ou contrôles) organisationnelles et techniques à implémenter.

soient testés et confirmés par une personne indépendante de celle en charge de sa réalisation.

## Ce qui appuie le constat de la Cour

Tout d'abord, la Cour rappelle que le terme « contrôle » désigne ici l'ensemble « *des mesures organisationnelles et techniques appropriées* » au sens de l'article 37, alinéa 2 LIPAD (pour plus de détail, voir point 3.3.2 du présent rapport).

**Concernant les contrôles liés à la gestion du système d'information par les équipes informatiques**

En premier lieu, la Cour note que la DSIC et son responsable de la sécurité informatique ont mis en place plusieurs mesures visant principalement à renforcer la cybersécurité. Si la Cour salue cet important travail, il est important de préciser que ces efforts ont pour but premier de lutter contre les menaces venant de l'extérieur. À l'inverse, la priorité n'a, pour l'instant, pas été donnée à la mise en œuvre de mesures visant à garantir la confidentialité des données personnelles au sens large.

En particulier, la Cour a constaté **l'absence de contrôle concernant la perte de données** (appelé DLP pour *Data Loss Prevention*, en anglais). Il s'agit d'un ensemble de pratiques et d'outils visant à détecter, dissuader ou empêcher que des données sensibles soient exfiltrées de manière accidentelle ou malveillante.

De manière plus générale, la Cour note que **les risques suivants, relatifs à la sécurité des données personnelles, ne font pas l'objet de contrôles suffisants** :

- le risque d'accès à des données personnelles depuis des environnements autres que la « production ». La production est l'environnement informatique normal de travail, qui peut contenir des données sensibles. Seuls les utilisateurs dûment habilités peuvent y accéder. À l'inverse, les autres environnements informatiques, souvent moins sécurisés, ne devraient pas accueillir de données sensibles d'après les bonnes pratiques. Lors d'entretiens avec la DSIC, il a été confirmé que les environnements de TEST et de DEV sont parfois « rafraîchis[62] » avec des données de production, afin de réaliser des tests au plus proche des conditions réelles. Or, il n'existe pas de processus systématique d'anonymisation ou de suppression des données sensibles pour ces copies. Ainsi, des données sensibles peuvent se retrouver sur des environnements pour lesquels le niveau de contrôle général est inférieur à celui mis en œuvre pour l'environnement de production (la gestion des accès est différente, des externes peuvent y accéder dans le cadre des projets, etc.).
- le risque lié à la possibilité que des collaborateurs externes accèdent à des données sensibles, dans le cadre de projets ou de contrats de maintenance applicative.
- les risques liés aux administrateurs disposant de hauts privilèges sur les différents outils et systèmes. Pour l'instant, l'essentiel des mesures en place se limitent à la traçabilité des actions réalisées, même si, pour les systèmes les plus sensibles des mesures complémentaires peuvent exister.

[62] Processus visant à copier des données réelles et à jour, depuis l'environnement de production, vers un autre environnement informatique. Cela est utile pour réaliser des tests en conditions réelles. Cependant, cela induit plusieurs risques.

**Concernant les pratiques de travail au sein des services et l'utilisation des outils informatiques**

Au-delà de la gestion des SI, **la sécurité des données personnelles passe aussi par un usage approprié des outils** par les collaborateurs et des pratiques de travail permettant de réduire le risque. À cet égard, la Cour a noté :

- en consultant un échantillon de documents de référence du contrôle interne de services, l'absence de règles ou de consignes relatives au traitement des données personnelles et à la préservation de leur sécurité ;
- de manière générale, il y a **peu ou pas de règles établies quant aux comportements à adopter lors de la manipulation, le transfert ou la destruction de données personnelles sensibles**. En effet, le cadre procédural n'est pas à jour et est incomplet (voir le constat 5 pour plus de détails). À titre d'exemple, il n'existe pas de consigne particulière pour limiter les risques liés à l'utilisation de clé USB et de plateformes de stockage en ligne (*cloud*) ainsi qu'au transfert de données par courriel. Il n'existe pas non plus de règle visant à limiter la présence de documents confidentiels dans les bureaux (souvent appelé « politique du bureau propre »), notamment le soir et les week-ends, quand les locaux sont accessibles aux agents d'entretiens et de sécurité (souvent de sociétés externes), par exemple.

**De l'importance de connaître ses données et leur propagation**

Afin de pouvoir définir une stratégie de contrôle appropriée et proportionnelle au risque, il paraît essentiel de concentrer les efforts sur les données sensibles, contrairement aux données publiques. La Cour soulève ici l'importance de disposer d'une vision claire sur les données sensibles et leur propagation dans l'infrastructure informatique afin de les protéger sur l'ensemble du cycle de vie. La Cour note qu'en l'état, la VdG ne dispose pas d'une vision complète et à jour sur les données sensibles qu'elle détient. La Cour salue toutefois la mise en place récente d'une procédure de classification des fichiers (accompagnée d'un outil informatique convaincant) qui permettra, à moyen terme, d'évaluer le volume de documents confidentiels existants.

**De l'absence de contrôle de second niveau**

Il ressort des discussions avec différents interlocuteurs clés qu'aucun contrôle de second niveau n'est en place sur les mesures liées à la sécurité des données. Par exemple, les plans de contrôle actuels des responsables de contrôle interne se concentrent principalement sur des aspects financiers.

Pour rappel, les contrôles de second niveau ont pour but de porter un regard indépendant sur l'efficacité opérationnelle des mesures décidées (en se concentrant uniquement sur les principales) et le respect des directives et procédures.

Exemples théoriques de contrôles de premier niveau et de contrôles de second niveau correspondants :

| | |
|---|---|
| Les personnes en charge des achats de prestation doivent insérer une clause relative à la sécurité des données dans tous les contrats | Le département juridique fait une revue de certains contrats à risque pour s'assurer que la clause soit présente et appropriée |
| Les collaborateurs doivent classifier tous les fichiers qu'ils manipulent en fonction de la sensibilité des informations | Le responsable de service vérifie deux fois par an que la classification est bien faite dans le dossier partagé de son équipe (par échantillonnage) |
| Le prestataire qui traite des données sensibles s'engage à chiffrer les données dans son infrastructure informatique | Un collaborateur de la VdG s'assure que les données sont effectivement chiffrées |
| Les collaborateurs s'assurent de ne pas laisser de documents confidentiels sur leurs bureaux lorsqu'ils quittent le travail | Une fois par an, quelqu'un visite un bâtiment, ou un étage d'un bâtiment, après 18h et contrôle la présence de document. |

**Conclusion**

Aujourd'hui, **peu de contrôles pour limiter le risque de sécurité des données ont été implémentés par la VdG.** La Cour note tout de même que la VdG dispose d'un outil de collection et de stockage de *logs* (traces des évènements informatiques) permettant de retracer la plupart des actions des utilisateurs. Toutefois, cet outil n'est utilisé qu'en cas d'investigation ou de diagnostic des infrastructures techniques. Il n'y a pas d'approche systématique de détection de comportement anormal ou de pratiques inadéquates. La Cour rappelle tout de même que la mise en place d'une telle démarche nécessite des efforts humains à anticiper.

## Recommandations de la Cour

### Recommandation n° 3 :

| Priorité : | Élevée[63] |
|---|---|

### Définir une stratégie de contrôle de la gestion des systèmes d'information par les équipes informatiques

La Cour recommande de définir **une stratégie de contrôle couvrant les risques liés aux pratiques et modes opératoires des équipes informatiques (DSIC)**. Cela inclut également la sécurisation des postes de travail pour limiter les risques liés à la sécurité des données personnelles.

**Modalités possibles :**

- En se basant sur une liste formalisée des risques de sécurité de la donnée personnelle, définir et formaliser les contrôles attendus sur tout le cycle de vie de la donnée.
- Une bonne stratégie de contrôle comprend souvent des consignes (*soft controls*), de la sensibilisation, la mise en place de mesures techniques, des contrôles préventifs (bloquants ou non) et d'autres détectifs. Elle comprend également la mise en place de contrôles de second niveau afin de s'assurer de la correcte mise en œuvre des contrôles clés et de leur efficacité opérationnelle.
- Prévoir les éléments nécessaires à sa mise en œuvre :
  - définir un plan de déploiement et des priorités sur plusieurs années (feuille de route) ;
  - définir les rôles et responsabilités quant à la mise en œuvre de ce plan et son suivi.

**Livrables :**

- Formalisation d'une (ou plusieurs) matrice(s) de contrôles cibles ;
- Formalisation et validation d'un plan de déploiement et des priorités sur plusieurs années ;
- Formalisation des rôles et responsabilités relatives à la mise en œuvre de ce(s) plan(s) et des modalités de suivi à travers le temps.

**Avantages attendus :**

- Renforcement de la mise en œuvre de l'article 37 LIPAD ;
- Standardisation du niveau de contrôle attendu, en cohérence avec les risques encourus et l'appétence au risque définie ;
- Transparence sur les forces et les faiblesses en termes de sécurité des données personnelles ;
- Clarification des pratiques autorisées et mise en œuvre de contrôles appropriés.

[63] La priorité de cette recommandation est élevée car la définition d'une stratégie de contrôle en fonction des risques encourus permettra d'avoir une meilleure couverture et maîtrise des risques encourus en lien avec la gestion des SI.

*Recommandation 3 :* ☒ *acceptée* ☐ *refusée*

**Position de la Ville de Genève :**
Cette recommandation sera traitée sur la base des travaux en lien avec la recommandation 1.

Délai : 31.12.2026
Responsables : RCI DCTN, DSIC, en collaboration avec le DPO

## Recommandation n° 4 :
## Définir une stratégie de contrôle liée à la sécurité des données au sein des services

Priorité : Élevée[64]

La Cour recommande de définir une stratégie de contrôle pour maîtriser les risques sur la sécurité des données personnelles **en lien avec l'usage des SI par les collaborateurs et leurs pratiques de travail**.

**Quelle est la différence avec la recommandation précédente ?**

La recommandation précédente a pour but de renforcer les processus informatiques opérés au quotidien par des informaticiens (gestion des serveurs, des développements, des projets informatiques, etc.).

La présente recommandation vise à renforcer la sécurité des données lorsqu'elles sont traitées par les utilisateurs des systèmes. Il s'agit d'une population plus hétérogène avec des pratiques de travail diverses et variées.

**Modalités possibles :**

- En se basant sur une liste formalisée des risques de sécurité de la donnée personnelle, définir et formaliser les contrôles attendus lors de l'accès, du traitement, de la sauvegarde ou du transfert de données personnelles par les services.
- Une bonne stratégie de contrôle comprend souvent des consignes (*soft controls*), de la sensibilisation, la mise en place de mesures techniques, des contrôles préventifs (bloquants ou non) et d'autres détectifs. Elle comprend également la mise en place de contrôle de second niveau afin de s'assurer de la correcte mise en œuvre des contrôles clés et leur efficacité opérationnelle
- Prévoir les éléments nécessaires à sa mise en œuvre :
  - Connaître l'étendue des données sensibles traitées par le service, de leurs emplacements dans les systèmes et de ceux qui y accèdent ;

[64] La priorité de cette recommandation est élevée car la définition d'une stratégie de contrôle en fonction des risques encourus permettra d'avoir une meilleure couverture et maîtrise des risques encourus en lien avec l'usage des SI.

- Concevoir un plan de déploiement et des priorités sur plusieurs années (feuille de route) ;
- Définir les rôles et la responsabilité quant à la mise en œuvre de ce plan et sa supervision.

**Livrables :**

- Formalisation d'une (ou plusieurs) matrice(s) de contrôles cibles ;
- Formalisation d'un plan de déploiement et des priorités sur plusieurs années qui doit être validé au niveau approprié de gouvernance ;
- Formalisation des rôles et responsabilités relatives à la mise en œuvre de ce(s) plan(s) et des modalités de suivi à travers le temps.

**Avantages attendus :**

- Renforcement de la mise en œuvre de l'article 37 LIPAD ;
- Définition d'un niveau standard de contrôle attendu, homogène et cohérent avec les risques encourus et l'appétence au risque ;
- Transparence sur les forces et les faiblesses en termes de sécurité des données personnelles ;
- Clarification des usages autorisés et mise en œuvre de contrôles appropriés.

*Recommandation 4 :* ☒ *acceptée* ☐ *refusée*

**Position de la Ville de Genève :**
Cette recommandation sera traitée sur la base des travaux en lien avec la recommandation 1.

Délai : 31.12.2026
Responsables : RCI DCTN, DSIC, en collaboration avec le DPO

## 4.3. Constat 3 : une gestion insuffisante de la sécurité des données personnelles dans le cadre des sous-traitances

### Quel est le constat de la Cour ?

La Cour note que, de manière générale, **les risques liés à la sécurité des données dans le cadre des sous-traitances ne sont pas suffisamment couverts** par des mesures appropriées. En effet, avec les dispositifs actuellement en place, il est difficile pour la VdG de garantir la préservation de la sécurité des données personnelles dont le traitement est sous-traité :

- dès la conception des contrats, l'intégration de clauses relatives à la sécurité des données suffisante n'est pas systématique ;
- durant toute la durée de la relation contractuelle, la VdG n'a pas mis en place de dispositif suffisant visant à s'assurer du respect des dispositions par le prestataire.

### Pourquoi ce constat est-il important ?

Les cas où la VdG recourt à des prestations externes sont nombreux et il n'est pas rare que des données personnelles soient concernées par la prestation, notamment quand les contrats portent sur des services de maintenance informatique ou de l'infrastructure[65].

Obligation légale et réglementaire

Il s'agit tout d'abord d'une obligation légale et réglementaire. En effet, **les institutions demeurent responsables des données personnelles qu'elles font traiter** au même titre que si elle les traitait elle-même [66]. 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[67]. Enfin, elles sont **tenues de contrôler le respect des clauses**[68] .

Nécessité d'avoir un niveau de sécurité minimum

Le niveau de maîtrise du risque de la violation de la sécurité des données peut varier d'un prestataire à l'autre et la VdG doit **s'assurer, d'un point de vue contractuel et opérationnel, qu'un niveau de contrôle minimum soit en place**. De plus, elle doit s'assurer que le niveau de sécurité du prestataire est au moins équivalent aux exigences que la VdG s'impose à elle-même.

Au-delà de la protection contractuelle qui est un prérequis indispensable, la VdG doit **s'assurer de la mise en œuvre effective des mesures** prévues au contrat. En effet, une fuite

[65] Par exemple, des collaborateurs d'une société qui édite un logiciel de gestion utilisé par la VdG se connectent à distance à l'application pour la faire évoluer. Les accès dont ils disposent leur permettent de consulter (ou extraire) des données personnelles sensibles, en grande quantité.
[66] Art. 13A, al. 2 RIPAD : « *L'institution demeure responsable des données personnelles qu'elle fait traiter au même titre que si elle les traitait elle-même* ».
[67] 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* ».
[68] Art. 37, al. 3 LIPAD : « *Les institutions publiques sont tenues de contrôler le respect des directives et clauses visées à l'alinéa 2* ».

de données chez un prestataire impacterait significativement l'image de la VdG, nuirait aux citoyens concernés et questionnerait la responsabilité de la VdG, même si un contrat approprié est en place.

## Ce qui appuie le constat de la Cour

La Cour note l'absence d'un cadre procédural et organisationnel approprié permettant de gérer les sous-traitances impliquant le traitement de données personnelles.

En premier lieu, il n'existe pas d'inventaire des prestations concernées, ce qui rend difficile tout contrôle.

Pour ce qui est de la **préparation des contrats**, les mesures de contrôle minimales suivantes ne sont définies dans aucune directive : obligation d'avoir un contrat écrit même si le montant est inférieur à 50'000 F lorsque des données sensibles sont traitées, clauses à intégrer aux contrats, étape de validation des contrats concernés par des spécialistes en sécurité des données, exigences techniques à intégrer aux contrats, etc. La Cour a revu un échantillon de contrats de prestations informatiques et note une hétérogénéité dans l'intégration et la teneur des clauses (bien que dans la plupart des cas, une clause de confidentialité était, à minima, en place).

Enfin, il n'existe pas de processus pour **contrôler le respect des clauses contractuelles** définies avec les sous-traitants. Pour tous les cas que la Cour a examinés, aucune démarche de contrôle active de la VdG n'a été engagée afin d'avoir une assurance raisonnable que les clauses prévues sont bien mises en œuvre.

## Recommandation n° 5 : Renforcer la sécurité des données dans le cadre des sous-traitances

Priorité : Élevée[69]

La Cour recommande de renforcer le cadre de gestion de la sécurité des données personnelles lors des sous-traitances selon les axes suivants :

- Mieux identifier les prestations impliquant des données personnelles ;
- S'assurer que des contrats soient systématiquement rédigés et que des clauses appropriées soient incluses ;
- Mettre en place un processus visant à s'assurer du respect de ces clauses par le prestataire.

**Modalités possibles :**

- Renforcer le processus achat en intégrant des points de contrôles spécifiques en matière de sécurité des données ;
- Rendre obligatoire l'existence d'un contrat écrit pour les prestations concernées, quel qu'en soit le montant ;
- Définir des clauses minimales devant être intégrées dans les contrats concernés ;
- Définir un processus (et les rôles et responsabilités relatives) de contrôle des prestataires clés tel qu'attendu par l'article 37, alinéa 3 LIPAD[70].

**Livrables :**

- Formalisation des clauses minimales à intégrer ;
- Mise à jour des procédures d'achats pour intégrer l'obligation d'un contrat écrit ;
- Validation d'un processus de contrôle.

**Avantages attendus :**

- Le risque de sécurité des données dans le cadre des sous-traitances est mieux connu et géré ;
- Renforcement de la conformité avec les exigences de la LIPAD y relatives.

*Recommandation 5 :* ☒ *acceptée* ☐ *refusée*

**Position de la Ville de Genève :**
Un travail important a débuté avec la DSIC afin de définir des clauses adaptées aux marchés informatiques. Ces clauses sont déjà intégrées à ces marchés et seront revues et validées avec le DPO. La CMAI définira en outre en collaboration avec la DSIC et le DPO les prestations qui devraient faire l'objet d'un contrat obligatoire indépendamment du montant ainsi que les mesures de contrôles nécessaires.

Délai : 31.12.2026
Responsables : CMAI, DSIC, en collaboration avec le DPO

[69] La priorité de cette recommandation est élevée car il s'agit d'une exigence de la LIPAD. De plus, le recours à des sous-traitants étant de plus en plus fréquent, notamment en informatique, il est important de cadrer ces pratiques.

[70] Art. 37, al. 3 LIPAD : « *Les institutions publiques sont tenues de contrôler le respect des directives et clauses visées à l'alinéa 2. S'il implique l'exploitation de ressources informatiques et le traitement de données personnelles, ce contrôle doit s'exercer conformément à des procédures spécifiques que les instances mentionnées à l'article 50, alinéa 2, doivent adopter à cette fin, après consultation du préposé cantonal.* »

## 4.4. Constat 4 : des mesures organisationnelles insuffisantes au sein des services

### Quel est le constat de la Cour ?

La Cour note que l'organisation au sein des départements et des services ne permet pas de garantir la sécurité des données personnelles sensibles, notamment sur les aspects suivants :

- Les rôles et responsabilités concernant la mise en œuvre des mesures organisationnelles et techniques de sécurité (au sens de l'article 37 LIPAD) ne sont pas clairement établis et personne ne semble en charge d'y veiller ;
- Il n'existe pas de processus visant à s'assurer que d'éventuelles violations de la sécurité des données personnelles sont identifiées et remontées ;
- Les mécanismes de formation et de sensibilisation sur la sécurité de données personnelles sensibles au sein de l'institution apparaissent comme insuffisants.

### Pourquoi ce constat est-il important ?

**Des rôles et responsabilités insuffisamment arrêtés au sein des services**

La sécurité des données est une problématique éminemment transversale. Si des dispositifs techniques peuvent être mis en place par la DSIC, une partie des mesures doivent être mises en œuvre par les services métiers (pratiques de travail). Étant donné la nature des prestations rendues, la diversité des métiers en VdG et la structure décentralisée de l'administration, il apparaît difficile d'établir une fonction centrale qui aurait la responsabilité de s'assurer de la sécurité des données au sein des processus métiers. 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 pour mieux prendre en compte toutes les spécificités de leur rôle. La Cour note que le manque de clarté actuel sur les rôles et responsabilités autour de la sécurité induit un niveau de contrôle hétérogène d'un service à l'autre.

**De l'absence d'un processus de traitement des violations de sécurité**

Il est important de pouvoir identifier les éventuelles violations à la sécurité des données pour les analyser et les traiter de manière appropriée. Il est également utile d'étudier si ces violations ont été possibles en raison d'éventuelles faiblesses dans les dispositifs de contrôle et de renforcer ces derniers le cas échéant. Ce processus est d'autant plus important qu'il s'agit d'une exigence de la nouvelle mouture de la LIPAD.

Constatant en cours de mission qu'un plan d'action était en cours de rédaction et que l'importance de ce sujet était correctement identifiée par la VdG, la Cour renonce à émettre une recommandation sur ce sujet. La VdG devra cependant déployer ce plan d'action au plus tard lors de l'entrée en vigueur de la nLIPAD.

**De l'insuffisance du dispositif de sensibilisation et de formation**

Les bonnes pratiques informatiques considèrent toujours que « la sécurité est la responsabilité de tous » dans une organisation. En effet, quelles que soient les mesures techniques mises en œuvre, un usage inadapté des outils, par négligence ou manque de connaissance, peut rapidement avoir un impact négatif de grande ampleur. Avec les nouvelles technologies, la vitesse de transmission ou d'extraction et la quantité de données concernées peuvent vite devenir problématiques. Ainsi, chaque utilisateur des SI doit être sensibilisé afin de comprendre les enjeux, mais aussi les pratiques autorisées et celles qui sont interdites.

## Ce qui appuie le constat de la Cour

**De l'insuffisance de l'organisation en place au sein des services**

La Cour a cherché à comprendre les rôles et responsabilités, au sein des services, en ce qui concerne la sécurité des données personnelles. Elle constate que si certains services ont désigné des conseillers LIPAD, ces derniers n'ont peu ou pas de responsabilité sur ce sujet et leur fonction n'est pas systématiquement définie et comprise (absence de fiche de poste, de formation appropriée[71], etc.). Il n'existe pas non plus de registre qui répertorie les conseillers qui ont été désignés en VdG.

La Cour constate également que les autres interlocuteurs clés au sein des services (correspondants informatiques, responsables de contrôle interne ou collaborateurs des services juridiques) n'interviennent pas formellement sur les questions en lien avec la sécurité des données et ne se sentent pas investis d'une responsabilité directe pour superviser le respect des exigences légales en la matière.

Il ressort que les rôles ou responsabilités en lien avec la sécurité des données au sein des services ne sont pas clairement définis.

**De l'absence d'un processus de traitement des violations de sécurité**

Actuellement, aucun processus d'identification et de traitement des violations n'est en place. La définition même d'une violation n'est pas établie. Ce faisant plusieurs questions centrales restent sans réponses : quelles sont les natures de données concernées ? À partir de quelle quantité de données, une alerte doit-elle être lancée ? Selon quels critères d'appréciation ? Ensuite, les rôles et responsabilités quant à l'identification, le signalement, l'évaluation de l'impact d'une violation de sécurité ou encore un éventuel plan de communication ou de crise sont encore à définir. Le plan d'action sur lequel travaille la VdG devra répondre à ces questions.

[71] Pour rappel, d'après l'article 2 de la Directive générale relative à la LIPAD : « *chaque conseiller-ère doit suivre une formation spécifique dans le domaine de la protection des données et la transparence, et mettre régulièrement à jour ses connaissances en la matière.* »

**De l'insuffisance du dispositif de sensibilisation et de formation**

Les différents entretiens menés par la Cour montrent que certaines notions de base (telle que la définition d'une donnée personnelle ou les précautions attendues pour leur traitement) ne sont pas toujours connues des collaborateurs. Plusieurs formations ont récemment été mises en place, mais elles sont générales et se focalisent sur la sécurité des SI. Si la Cour salue cette initiative, elle note tout de même que les formations ne vont pas assez loin sur les sujets liés à la sécurité des données personnelles et les usages autorisés. De plus, les supports de formation ne sont pas systématiquement adaptés aux spécificités de la VdG.

Par ailleurs, les collaborateurs « sensibles » ou « à risque » tels que les collaborateurs traitant de grandes quantités de données sensibles ou les administrateurs informatiques (qui pourraient accéder à des données grâce à leurs accès à hauts privilèges) ne bénéficient pas de formation renforcée.

Enfin, les dispositifs de formation actuels ne s'appliquent pas aux ressources externes, alors que certaines accèdent ou manipulent des données sensibles. La Cour constate, par ailleurs, que les formations existantes ne font pas l'objet d'un suivi spécifique visant à s'assurer de leur efficacité ou de leur bon déploiement, ni d'ajuster les actions de sensibilisation en fonction des résultats obtenus.

## Recommandation n° 6 : Désigner des personnes relais au sein des services pour renforcer la sécurité des données personnelles

Priorité : Moyenne[72]

La Cour recommande de désigner des personnes relais au sein des services afin de coordonner les aspects liés à la sécurité des données personnelles. Elles seront chargées de définir les pratiques autorisées et de contrôler leur mise en œuvre au sein des services. 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.

**Modalités possibles :**

- Identifier des personnes relais au sein de chaque service et tenir un registre des personnes désignées ;
- Définir et formaliser leur rôle en lien avec la sécurité des données personnelles (cahier des charges) ;
- S'appuyer sur une fonction déjà existante et la renforcer (les correspondants LIPAD, les correspondants informatiques, les responsables de contrôle interne, ou les managers/cadres par exemple) ;
- S'assurer que les personnes concernées bénéficient d'une formation appropriée.

**Livrables :**

- Mise en œuvre d'un registre des personnes concernées (potentiellement, maintenu par le futur délégué à la protection des données (DPO) ;
- Les cahiers des charges des personnes concernées sont mis à jour ;
- Matrice de rôle et responsabilité définie et approuvée ;
- Définition d'un plan de mise en œuvre approuvé.

**Avantages attendus :**

- Les responsabilités sont clarifiées ;
- Les collaborateurs disposent d'un relai au sein des services ;
- La sécurité est renforcée grâce à un contact de proximité qui s'assure de la mise en œuvre des bonnes pratiques dans les activités du quotidien.

[72] La priorité de cette recommandation est moyenne, car la désignation de personnes relais au sein des services est nécessaire pour renforcer la mise en œuvre de la stratégie de contrôle qui sera décidée et mieux soutenir l'administration au quotidien.

*Recommandation 6 :* ☒ *acceptée* ☐ *refusée*

**Position de la Ville de Genève :**
La modification des cahiers des charges des personnes concernées devra être initiée par le DPO pour assurer une harmonisation du contenu (cela figure dans son cahier des charges), étant précisé que celui-ci devra être le même dans chaque service.

La DRH peut intervenir en soutien mais son intervention sera limitée à l'évaluation des cahiers des charges modifiés. Il est relevé que de telles responsabilités supplémentaires pourront avoir un impact sur la classe de traitement des postes concernés. Il conviendra donc d'en tenir compte.

Délai : 31.12.2026
Responsables : CODIR et le DPO

| Priorité | Moyenne[73] |
|---|---|

## Recommandation n° 7 : Définir et mettre en œuvre un dispositif de formation et de sensibilisation approprié en lien avec la sécurité des données personnelles

La Cour recommande de définir un plan de formation spécifique à la sécurité des données personnelles. Celui-ci doit **prévoir une sensibilisation renforcée des collaborateurs pouvant accéder à une grande quantité de données** (selon une approche basée sur les risques), incluant les ressources externes.

**Modalités possibles :**

- Poursuivre le développement des initiatives de sensibilisation obligatoires pour tous les collaborateurs ;
- Identifier les fonctions et collaborateurs traitants ou pouvant accéder à une quantité significative de données sensibles (critères à définir), aussi bien à l'informatique que dans les métiers et définir un processus de formation renforcé pour cette population ;
- S'assurer qu'un suivi documenté des participations soit en place ;
- Veiller à ce que les collaborateurs externes travaillant pour la VdG soient inclus lorsque cela est pertinent (par exemple, si l'intervention implique un traitement de données personnelles sensibles).

**Livrables :**

- Liste des fonctions / personnes concernées et critères de sélection ;
- Plan de formation et modalité de suivi.

**Avantages attendus :**

- Une meilleure sensibilisation des collaborateurs ;
- Les efforts de formations supplémentaires sont concentrés sur des fonctions plus risquées ;
- La VdG peut démontrer la mise en œuvre de mesures organisationnelles appropriées au sens de la LIPAD.

*Recommandation 7 :* ☒ *acceptée* ☐ *refusée*

**Position de la Ville de Genève :**
La DRH poursuivra les initiatives déjà entreprises en matière de formation, sur la base de ce qui sera prévu par le DPO.

Délai : 31.12.2026
Responsables : CODIR et le DPO

[73] La priorité de cette recommandation est moyenne, car la sécurité des données ne peut être garantie que si l'ensemble des collaborateurs adoptent des pratiques de travail appropriées, notamment en ce qui concerne la classification, le stockage et le transfert de données personnelles.

## 4.5. Constat 5 : les directives et procédures en lien avec sécurité des données sont incomplètes

La Cour constate que le cadre procédural en place 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. Les règles et la documentation existantes ne fournissent pas une base suffisante pour établir un dispositif de sécurité adéquat pour les données gérées par l'administration. En effet, plusieurs aspects importants de la sécurité des données ne sont pas traités tels que, par exemple, les comportements et pratiques que les collaborateurs doivent adopter lors du traitement, de la transmission ou de la destruction de la donnée. 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.

Les documents de référence actuels sont difficiles à appréhender pour les utilisateurs des SI, lesquels soulignent le besoin d'un cadre de référence plus accessible et plus simple à mettre un œuvre.

### Pourquoi ce constat est-il important ?

Pour rappel, l'adoption d'un cadre procédural adéquat est une obligation légale en vertu de l'article 37, alinéa 2 LIPAD, qui précise que les institutions publiques doivent prendre « *les mesures nécessaires pour assurer la [sécurité] des données personnelles* », « *par le biais de directives* ». Ainsi, il est attendu que les mesures organisationnelles et techniques soient déclinées dans des directives internes[74]. Au vu du caractère incomplet et obsolète du cadre procédural en place, la VdG n'est pas en mesure de respecter pleinement cette exigence légale. Par ailleurs, un cadre procédural complet et qui fixe clairement les responsabilités permettrait de limiter les risques auxquels la VdG s'expose en cas de survenance d'un litige portant sur le respect des dispositions légales sur les données personnelles.

D'un point de vue opérationnel, l'avènement de l'informatique et l'expansion rapide de nouveaux outils numériques ont considérablement facilité la collecte et la circulation des données. L'arrivée de ces possibilités techniques s'est accompagnée de nouveaux risques qui peuvent survenir plus facilement et concerner un volume de données de plus en plus important. Dans ce contexte, il est crucial de définir des règles claires concernant les usages et les pratiques autorisés, en particulier lorsque la mise en place de contrôles techniques est trop complexe ou trop coûteuse.

De plus, le fait que les procédures existantes n'aient pas été mises à jour en fonction des avancées technologiques[75] entraîne le risque de voir se développer des pratiques hétérogènes en lien avec l'usage d'outils de plus en plus risqués et qui impliquent un

[74] L'article 37, alinéa 2, prévoit que « *les institutions publiques doivent prendre, par le biais de directives et de clauses statutaires ou contractuelles appropriées, les mesures nécessaires pour garantir la disponibilité, l'intégrité et la confidentialité des données personnelles qu'elles traitent ou font traiter* ».
[75] La nLIPAD précise à son article 37, alinéa 2, que les mesures organisationnelles et techniques doivent être appropriées au regard notamment de l'état de la technique.

volume de données croissant sans même que l'usager des SI en soit conscient. Par exemple, lorsqu'un collaborateur utilise un simple outil de traduction en ligne, le texte à traduire est automatiquement envoyé à une entreprise externe. Il est donc impératif que l'utilisateur soit vigilant à ne pas saisir de données personnelles, à plus forte raison sensibles. Dans ce contexte, il est important pour une entité comme la VdG de rester informée des évolutions technologiques et des meilleures pratiques afin de disposer d'un cadre procédural à même de prévenir les risques liés à l'utilisation des outils numériques, tout en accompagnant les utilisateurs.

## Ce qui appuie le constat de la Cour

**Une directive générale d'application de la LIPAD qui se focalise essentiellement sur l'application du volet transparence de la loi**

La directive générale relative à la LIPAD se concentre principalement sur la mise en œuvre du volet de transparence de la loi, notamment le recensement des fichiers et le traitement des demandes d'accès. Elle n'aborde que de manière succincte la sécurité des données en indiquant que chaque entité doit prendre toutes les mesures nécessaires pour que les données personnelles qu'elle détient ne soient accessibles, manipulées, complétées ou supprimées que par des personnes dûment autorisées, conformément à la loi. Elle précise aussi que la DSIC doit mettre en place les mesures requises pour garantir en permanence la sécurité des données personnelles stockées sur les serveurs de la VdG. Ainsi, la directive évoque de manière générale la sécurité des serveurs de la VdG, mais n'aborde pas la sécurité durant tout le cycle de vie (lors des transferts, en cas de stockage sur le *cloud*, ou ailleurs que sur un serveur de la VdG, par exemple).

**Une politique de sécurité des systèmes d'information qui n'a pas été déclinée dans des procédures opérationnelles**

La politique de sécurité des systèmes d'information (PSSI) adoptée en 2020 définit les règles et mesures générales en matière de sécurité. Bien qu'il fût prévu qu'elle soit déclinée en procédures opérationnelles, notamment pour cadrer les pratiques de travail au sein de la DSIC, cela n'a pas encore été mis en œuvre. Ainsi, de nombreux concepts importants liés à la sécurité de l'information y sont mentionnés sans être développés dans une documentation de référence, par exemple :

- L'utilisation des équipements mobiles.
- Les règles et modalités de gestion des accès aux SI.
- La gestion et la traçabilité des activités et des accès aux SI.
- La gestion des fournisseurs et de la sous-traitance en matière de sécurité des données.
- Le référentiel des processus, standards de configuration, procédures, modes opératoires et listes de contrôle qui régissent les activités de sécurité informatique à réaliser par les équipes techniques de la DSIC.

La Cour a constaté que plusieurs documents prévus par la PSSI n'ont toujours pas été rédigés, près de cinq ans après son adoption. Parmi les documents manquants, figurent la directive sur l'usage des technologies en *cloud*, la directive sur la gestion des accès aux SI, le règlement concernant l'usage des appareils personnels ou encore le règlement relatif aux usages acceptables dans les SI.

La Cour note tout de même que, sur certains de ces aspects, la DSIC a mis en œuvre des mesures de contrôle, mais qu'elle n'a pas formalisé ces éléments dans un ensemble de procédures.

**Un encadrement insuffisant des activités et des usages métiers**

La Cour constate un manque de règles et directives claires pour régir les activités et pratiques des usagers des SI lors de la manipulation, du transfert ou de la destruction de données personnelles.

Plus particulièrement, il n'existe pas de règles concernant plusieurs aspects essentiels de la sécurité de l'information. Par exemple, aucun document de référence ne précise les méthodes de gestion des accès ni les procédures autorisées pour le transfert de données sensibles. Cette observation s'étend également aux pratiques acceptées pour le transfert et la sortie de données, à l'utilisation des plateformes *cloud*, aux rôles et responsabilités liés à la gestion des accès aux fichiers, à l'organisation des espaces de travail, à l'intégration de l'intelligence artificielle (IA), à l'utilisation de solutions de messagerie instantanée et à la durée de conservation des données personnelles.

Par exemple, la directive générale relative à l'utilisation des SI et de communication (DGUSIC), adoptée en 2019, présente plusieurs insuffisances. Elle contient peu de règles pour encadrer les pratiques des utilisateurs sur les activités du quotidien comme l'envoi de données vers l'extérieur, leur stockage sur des solutions *cloud* (pratique observée), leur impression, leur destruction, etc. Plus particulièrement, aucune mesure pour prévenir la fuite et la perte de données n'est évoquée. De plus, la directive n'est pas à jour concernant les avancées technologiques récentes. Elle aborde ainsi l'utilisation des disques durs externes (ce qui est rare en 2025) sans évoquer l'utilisation de solutions basées sur le *cloud* ou l'utilisation d'outils d'intelligence artificielle (qui sont d'actualité et présentent des risques accrus). Par ailleurs, cette directive est considérée comme complexe et inadaptée par de nombreux collaborateurs. Elle ne constitue pas un référentiel pratique et accessible sur lequel les usagers des SI peuvent s'appuyer lors du traitement ou du transfert des données personnelles.

Un autre exemple est la récente directive générale sur la classification et la protection de l'information numérique, adoptée en 2024. Actuellement, seules deux mesures sont proposées pour la donnée confidentielle : l'utilisation d'un filigrane "confidentiel" et la possibilité, à bien plaire, de chiffrer les courriels qui en contiennent. Aucune mesure n'est prévue pour les documents non confidentiels (même si ceux-ci peuvent contenir des données personnelles). De plus, la directive prévoit d'accompagner les utilisateurs avec des annexes explicatives sur les comportements appropriés selon les applications (comme la messagerie ou le traitement de texte), mais ces documents n'ont pas encore tous été rédigés. Enfin, bien que le périmètre d'application de la directive s'étende à toutes les données détenues par l'administration, les mesures prévues ne s'appliquent qu'aux documents PDF et à ceux issus de l'environnement 365, en excluant d'autres formats, tels que des fichiers ZIP, des bases de données, des images/vidéos ou des documents TXT.

| Priorité : | Faible[76] |
|---|---|

## Recommandation n° 8 : Compléter et actualiser le *corpus* procédural en matière de la sécurité des données

La Cour recommande d'enrichir et de mettre à jour le cadre procédural existant. Plus précisément, il est nécessaire d'intégrer dans la documentation officielle, qu'il s'agisse de règlements, de directives, de procédures ou d'autres formats, 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 par la VdG, tenir compte des avancées technologiques et être présentées de manière à faciliter leur compréhension et leur utilisation par les usagers des SI.

**Modalités possibles :**
*Cette recommandation porte sur la mise à jour des documents de référence régissant la sécurité des données. A minima, cela implique de :*

- Compléter la DGUSIC pour un meilleur encadrement de l'usage des outils tels que l'IA, l'utilisation du *cloud*, les outils de traduction en ligne, les réseaux sociaux, etc. ;
- Décliner la PSSI en procédures opérationnelles telles que prévues par le document ;
- S'assurer que d'éventuels nouveaux contrôles ou nouvelles règles, découlant des recommandations 2, 3 et 4 soient intégrés dans les directives ou procédures pertinentes.

**Livrables :**

- Mise à jour de la DGUSIC ;
- Déclinaison de la PSSI en procédures opérationnelles (ou validation d'une feuille de route pour y parvenir progressivement).

**Avantages attendus :**

- Meilleure conformité aux exigences légales et au cadre interne ;
- Réduction des risques de fuite ou de perte de données sensibles ;
- Meilleure sensibilisation des usagers des SI et uniformisation des pratiques ;
- Formalisation du niveau de sécurité attendu en VdG.

*Recommandation 8 :* ☒ *acceptée* ☐ *refusée*

**Position de la Ville de Genève :**

Cette recommandation fera partie du plan d'action nLIPAD qui sera piloté par le nouveau DPO de la DSG en coordination avec le RSSI de la DSIC et le service des archives.

La DGUSIC est en cours de révision pour tenir compte des nouveaux usages suite au déploiement de MS Office 365 et à la nouvelle charte d'utilisation de l'IA. Les annexes de la directive de classification évolueront en fonctions des nouveaux outils et moyens de traitement qui seront mis en œuvre (notamment OneDrive).

Délai : 31.12.2026
Responsables : DSIC, service des archives, en collaboration avec le DPO

[76] La priorité de cette recommandation est faible, car la mise en à jour du cadre procédural ne devrait être que la documentation de pratiques établies. Cependant, la Cour soulève l'importance de disposer de procédures à jour auxquelles il est possible de se référer.

# 5. Synthèse des recommandations et feuille de route

## 5.1. L'approche théorique proposée par la Cour

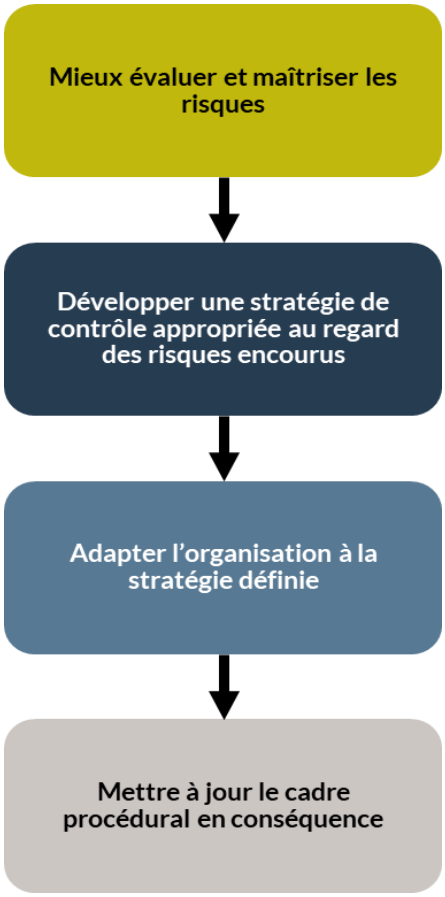
La logique de l'approche proposée par la Cour peut être résumée par la figure ci-contre.

Si le raisonnement théorique repose sur un séquencement d'étapes dépendantes les unes des autres, la Cour rappelle qu'il n'est pas nécessaire d'attendre la fin d'une étape avant de passer à la suivante.

Par exemple, il est fondamental de réfléchir aux rôles et responsabilités le plus tôt possible dans la mise en œuvre des recommandations de ce présent rapport.

La page suivante propose une répartition des différentes recommandations au sein d'une feuille de route schématique.

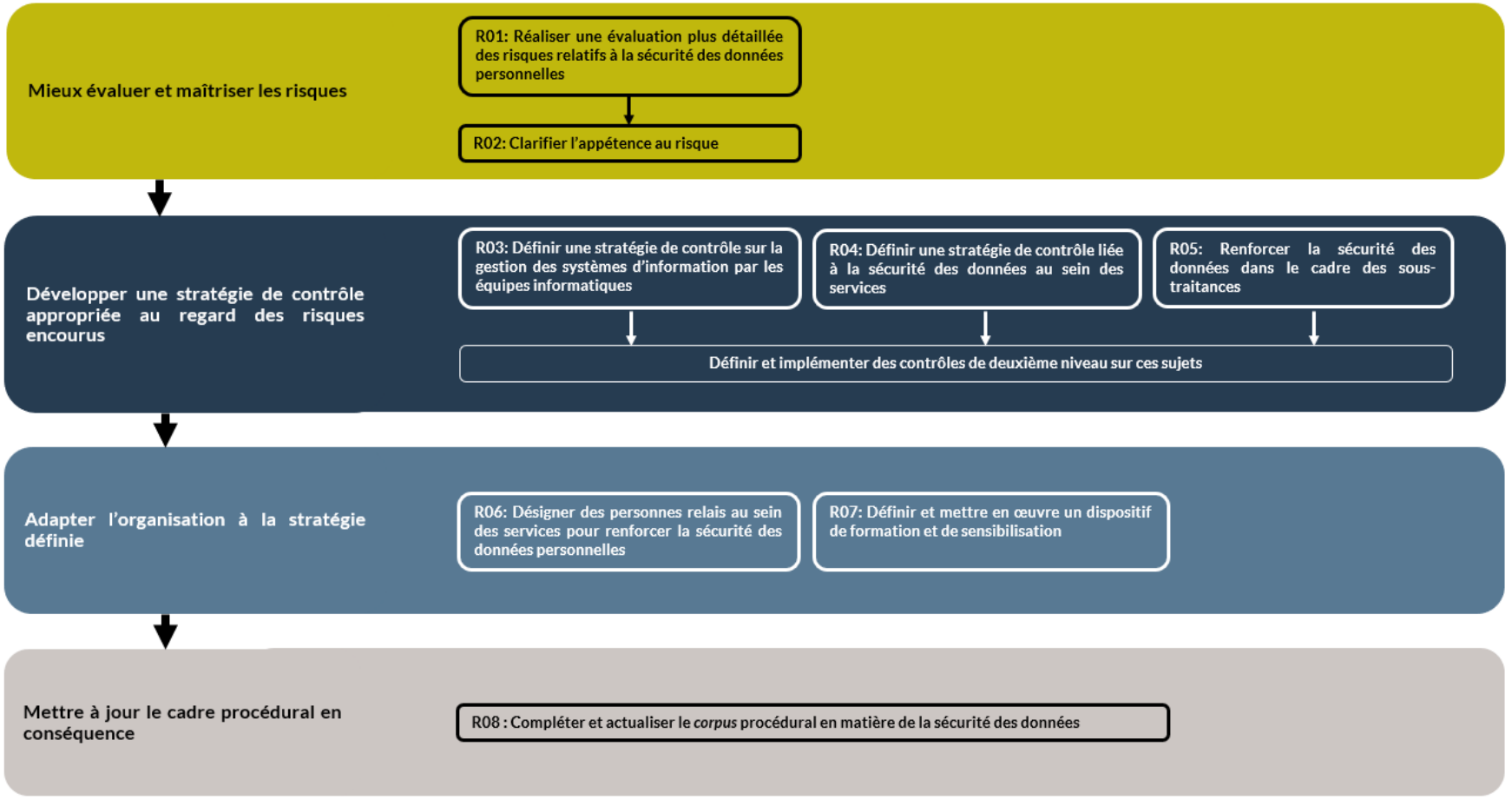
Figure 10 : Vue synthétique de la logique des recommandations




Source : Cour des comptes, 2025

## 5.2. La répartition des recommandations sous forme de feuille de route

Figure 11 : Logique d'implémentation des recommandations proposée par la Cour




Source : Cour des comptes, 2025

## 5.3. Remarque conclusive

Cet audit s'est concentré sur les aspects opérationnels relatifs **à la définition et à la mise en œuvre de mesures de sécurité** de la donnée personnelle sensible. Si les rôles et responsabilités y afférents ont été en partie couverts durant l'audit, la Cour n'a toutefois pas revu en détail **l'organisation globale, ni les mécanismes de surveillance** du dispositif. La Cour encourage la VdG à repenser les rôles et responsabilités des différentes fonctions et leurs interactions en lien avec la sécurité des données personnelles.

# 6. Degré de priorité des recommandations

Le degré de priorité de mise en œuvre des recommandations permet de hiérarchiser les recommandations de la Cour par priorité et de mettre en avant de façon explicite ce qui est important.

La Cour a fixé quatre degrés de priorité :
- Très élevé
- Élevé
- Moyen
- Faible

Cette hiérarchisation est réalisée en fonction de six critères, mobilisés en fonction des objectifs de la mission :
- Favoriser l'atteinte de l'objectif de la politique publique ;
- Amélioration des prestations délivrées ;
- Amélioration de la performance des processus ;
- Amélioration de la gouvernance ;
- Risques à couvrir ;
- Maîtrise des coûts.

Les critères utilisés dans le cadre de la présente mission sont détaillés dans la synthèse au chapitre « *tableau récapitulatif des recommandations* ».

# 7. Bibliographie

ISO/IEC 27001, (2022). *Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences.* Genève : International organization of standardization.

ISO/IEC 27002, (2022). *Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information.* Genève : International organization of standardization.

Préposé cantonal à la protection des données et à la transparence (2019). Fiche info – Sécurité des données - aspects juridiques et pratiques de la sécurité des données, État de Genève.

Préposé cantonal à la protection des données et à la transparence, « Catalogue des fichiers» [En ligne] (disponible à l'adresse) : http://outil.ge.ch/chacatfich/#/catalog/institution/228/302).

Préposé fédéral à la protection des données et à la transparence, (2024). Guide relatif aux mesures techniques et organisationnelles de la protection des données, Confédération Suisse.

Site officiel de Gartner, « Définition de la sécurité de la donnée » [En ligne] (disponible à l'adresse : https://www.gartner.com/en/marketing/glossary/data-security).

# 8. Remerciements

La Cour remercie la Ville de Genève et ses collaborateurs pour leur accueil, la qualité des échanges et les discussions constructives.

L'audit a été terminé en octobre 2025. Le rapport complet a été transmis à la Ville de Genève le 4 septembre 2025, pour observations. Les observations des audités ont été dûment reproduites dans le rapport.

La synthèse a été rédigée après réception des observations de l'audité.

Genève, le 14 octobre 2025

| | | |
|---|---|---|
| Sophie FORSTER CARBONNIER | Fabien MANGILLI | Frédéric VARONE |
| Magistrate titulaire | Magistrat titulaire | Magistrat suppléant |

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