La nouvelle LIPAD — Comment se préparer à sa mise en œuvre ?

Philipp Fischer et Yvann Barras, le 10 décembre 2024

Le Grand Conseil genevois a adopté le 3 mai 2024 la révision de la LIPAD. Elle a pour but d'aligner la législation genevoise sur les évolutions technologiques et les standards en matière de protection des données apportés par, entre autres, le RGPD et la nouvelle LPD. De ce fait, la systématique de la LIPAD se rapproche de plus en plus du droit fédéral, tout en gardant quelques particularités propres qui sont détaillées dans la présente contribution.

Nota bene : La présente contribution fait partie d'une série de deux contributions consacrées à la nouvelle Loi genevoise sur l'information du public, l'accès aux documents et la protection des données personnelles (nLIPAD) adoptée par le Grand conseil genevois le 3 mai 2024 (cf. www.swissprivacy.law/326 pour un tour d'horizon des nouveautés de la nLIPAD). Cette seconde contribution vise à présenter des pistes de réflexion en vue de sa mise en œuvre au sein des institutions publiques.

I. Introduction

La nLIPAD introduira des changements importants dans la gestion des données personnelles traitées par les institutions publiques genevoises. À ce jour, l'entrée en vigueur de la nLIPAD n'est toutefois pas encore connue, le Conseil d'État genevois devant encore se prononcer après avoir finalisé la révision du Règlement d'application (RIPAD). Malgré cette inconnue, il est impératif pour les institutions publiques de se préparer dès à présent, dans la mesure où la nLIPAD, à la différence de certaines autres législations cantonales, ne prévoit aucun délai transitoire et s'appliquera immédiatement dès son entrée en vigueur, qui devrait probablement intervenir dans la deuxième moitié de l'année 2025.

La mise en œuvre des nouveautés apportées par la nLIPAD constitue la prochaine étape pour les institutions publiques genevoises. La mise en œuvre des nouvelles obligations s'avère complexe, dans la mesure où elles requièrent des compétences interdisciplinaires mêlant des connaissances juridiques, techniques, mais également une compréhension approfondie des enjeux organisationnels. Cette approche transversale peut représenter un défi pour les institutions publiques qui ne disposent pas toujours des ressources humaines, financières ou spécifiques à ce domaine. Afin de les soutenir, nous proposons dans le cadre de la présente contri-

bution une approche méthodologique concrète et adaptée à la nLIPAD, fruit de notre expérience avec des législations similaires dans d'autres cantons.

II. Programme de protection des données — À quoi ça sert ?

La compréhension des législations en matière de protection des données peut, en apparence, sembler théoriquement simple. Leur systématique est raisonnablement similaire, celles-ci étant constituées de principes, qui fondent leur noyau dur, de droits à disposition des personnes concernées, ainsi que d'obligations qui incombent au responsable du traitement. Toutefois, la mise en œuvre de ces législations s'avère en pratique bien plus complexe, et la nLIPAD n'échappe pas à la règle.

La mise en œuvre de la nLIPAD nécessite une adaptation des exigences légales aux particularités de chaque institution publique, tout en intégrant à des questions propres à ses activités et à ses processus internes. Les axes de travail à envisager dans ce cadre sont nombreux, allant de la définition précise des rôles et responsabilités, à l'identification des activités de traitements impliquant des sous-traitants jusqu'à la gestion des risques. C'est la raison pour laquelle un « programme de protection des données » s'impose, non seulement pour assurer une posture de conformité adéquate, mais également pour en faire un levier opérationnel au sein de chaque institution.

De manière générale, un « programme de protection des données » comprend un cadre de gestion structuré et de mesures destinées à guider l'organisation dans sa gestion de la protection des données. Son objectif dépasse la simple recherche de la conformité légale pour viser un équilibre durable entre la protection des droits des personnes concernées et le fonctionnement quotidien de l'organisation. Construit selon un processus itératif, un programme de protection des données permet une adaptation agile face aux évolutions légales, techniques et organisationnelles.

Les bénéfices d'un tel programme sont multiples. Il permet tout d'abord d'assurer autant que possible la conformité légale en intégrant, dans le cas présent, les exigences de la nLIPAD au sein des processus internes, mais également les exigences légales d'autres législations pouvant avoir un lien avec la protection des données. Il renforce également la sécurité des données en identifiant et en traitant les risques de manière ciblée. Par ailleurs, un programme bien structuré facilite considérablement le traitement des demandes des personnes concernées, au travers de procédures claires. Il contribue également à renforcer la confiance des parties prenantes, qu'il s'agisse des collaborateurs ou des citoyens, en démontrant un engagement tangible envers la protection des données. Enfin, le programme aide

généralement l'organisation à mieux se préparer aux situations de crise, notamment en cas de violation de la sécurité des données.

III. Programme de protection des données — Axes de travail

La mise en œuvre d'un programme de protection des données exige une approche structurée dans le cadre duquel chaque composante assure une prise en compte complète des enjeux juridiques, techniques et organisationnels. Un tel programme repose en règle générale sur neuf axes de travail essentiels, chacun répondant à des problématiques spécifiques, pourtant interconnectées les unes aux autres.

Le premier axe concerne *le cadre de gestion*, qui implique l'identification du contexte interne et externe dans lequel évolue l'institution publique, en particulier ses objectifs, ses parties prenantes et les contraintes légales spécifiques applicables. Le cadre de gestion permet de définir les priorités et d'orienter concrètement les actions, qui doivent être formalisées à travers des politiques claires. Le cadre de gestion implique également d'analyser la question des rôles et des responsabilités au sein de l'institution publique, notamment les personnes qui doivent être en charge des questions de la protection des données. Si le conseiller LIPAD joue un rôle essentiel sur ce point, ce dernier ne peut toutefois pas assumer seul l'entier du travail.

Le deuxième axe porte sur *la gestion des activités de traitement*, qui consiste à identifier et documenter les activités de traitement au sein de l'institution publique. Cet exercice passe principalement par la tenue, respectivement l'élaboration, d'un registre des activités de traitement, un outil clé puisqu'il représente le point de départ de tout contrôle par le Préposé à la protection des données, mais également le socle pour la mise en œuvre des droits et des obligations, ainsi que pour l'évaluation des risques (cf. www.swissprivacy.law/294 sur la constitution d'un registre des activités de traitement).

Le troisième axe se concentre sur *la gestion des relations avec les sous-traitants*. Cela passe par l'identification claire des sous-traitants et la formalisation des relations à travers des contrats. Ces derniers doivent inclure des clauses spécifiques relatives à la protection des données, telles que des obligations de confidentialité, des engagements en matière de sécurité et des mécanismes de contrôle (p. ex. droit d'audit).

Le quatrième axe concerne *la gestion des risques*. Elle implique d'identifier, d'apprécier et de traiter les risques associés aux traitements de données personnelles, en tenant compte des différentes menaces. Cette gestion passe par la mise en place d'un plan structuré, incluant

des outils comme des matrices de risque ou des analyses d'impact sur la protection des données pour les traitements présentant des risques élevés.

Le cinquième axe porte sur *la gestion de la sécurité*, fondée sur la mise en œuvre de mesures organisationnelles et techniques adaptées telles que la gestion des accès et des moyens d'authentification ainsi que la classification et le marquage des données. La gestion de la sécurité implique également des réflexions relativement profondes quant à la résilience informatique et à la continuité d'activité en cas de perturbations.

Le sixième axe se concentre sur le *respect des droits des personnes concernées*, tels que le droit d'accès ou de rectification. Cela nécessite la mise en place de procédures claires pour traiter ces demandes dans les délais impartis et de manière efficiente. Chaque institution doit réfléchir à l'instauration d'un canal de communication dédié pour recevoir les demandes des personnes concernées.

Le septième axe porte sur *la gestion des incidents*. Il s'agit de détecter, signaler et répondre aux violations de données. La gestion des incidents implique notamment l'élaboration d'une procédure pour évaluer leur gravité et en informer, si nécessaire, l'autorité et les personnes concernées. Renforcer les capacités de détection et instaurer un plan d'intervention rapide permettront également de limiter les impacts et de garantir le respect des obligations.

Le huitième axe met l'accent sur *la sensibilisation et la formation des collaborateurs* aux enjeux de la protection des données ainsi qu'à la sécurité. Des campagnes régulières et des formations ciblées doivent être organisées pour renforcer la culture de la sécurité et de la protection des données au sein de l'institution publique.

Le neuvième, et dernier axe est dédié à *la gestion de la conformité*, qui consiste à structurer et à documenter dans la durée les actions entreprises pour respecter les obligations. Cela inclut l'élaboration et la mise à jour des documents clés, comme le registre des activités de traitement, et la mise en place d'un processus de revue périodique pour garantir la pertinence et l'actualité des pratiques internes.

IV. Conclusion

La mise en œuvre de la nLIPAD, comme toute autre législation dédiée à la protection des données, constitue un défi majeur pour les institutions publiques genevoises, qui devront s'engager activement dans le travail à fournir. Si le rôle du conseiller LIPAD est essentiel pour coordonner ces efforts, il ne peut à lui seul relever l'ensemble des enjeux. Il sera impératif

pour chaque institution publique d'élaborer une stratégie générale et de mobiliser les ressources nécessaires pour intégrer durablement les nouveautés apportées par la nLIPAD dans ses pratiques quotidiennes. Selon notre expérience, le « programme de protection des données » évoqué ci-dessus constitue un moyen pragmatique et prouvé en pratique pour assurer la mise en conformité à la nLIPAD.

Proposition de citation : Philipp FISCHER / Yvann BARRAS, La nouvelle LIPAD — Comment se préparer à sa mise en œuvre ?, 10 décembre 2024 *in* www.swissprivacy.law/327