Projet de règlement d'application de la loi sur la protection des lanceurs d'alerte au sein de l'Etat (RPLA – B 5 07.01)

Avis du 22 février 2022

Mots clés : protection des données personnelles; anonymat; communication d'informations; moyens d'enquête.

Contexte : En date du 16 février 2022, la Direction des affaires juridiques de la Chancellerie d'Etat (DAJ) a sollicité l'avis du Préposé cantonal à la protection des données et à la transparence dans le cadre d'un projet de règlement d'application de la loi sur la protection des lanceurs d'alerte au sein de l'Etat (RPLA – B 5 07.01). Plusieurs dispositions du projet ont trait au traitement de données personnelles, ainsi qu'à la transmission desdites données.

Bases juridiques : art. 56 al. 3 litt. e LIPAD; art. 23 al. 8 RIPAD

1. Caractéristiques de la demande

Par courrier électronique du 16 février 2022, la Direction des affaires juridiques de la Chancellerie d'Etat (DAJ) a sollicité l'avis du Préposé cantonal à la protection des données et à la transparence dans le cadre d'un projet de règlement d'application de la loi sur la protection des lanceurs d'alerte au sein de l'Etat (RPLA – B 5 07.01).

Il sied de relever que le Préposé cantonal avait d'ores et déjà été consulté dans le cadre de l'élaboration de ce projet et que ses remarques émises les 8 décembre 2021 par courriel et 13 janvier 2022 lors d'une séance de travail ont été prises en considération. Ces remarques visaient essentiellement à ce que les éléments communiqués entre entités dans le cadre de la coordination soient mieux clarifiés, de même que l'accord du lanceur d'alerte à leur communication.

Était joint au courrier électronique du 16 février 2022 un tableau synoptique comportant des commentaires relatifs au projet de règlement. Il y est précisé que « *même si le règlement ne l'indique pas explicitement, il est bien entendu que la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (LIPAD; A 2 08) est applicable, notamment les principes régissant le traitement des données personnelles visés à ses articles 35 à 40* ».

Diverses dispositions du projet de règlement ont trait directement ou indirectement à des questions de protection des données personnelles. Tel est le cas des dispositions suivantes :

Art. 1 al. 2 : *Des informations peuvent être demandées par divers moyens tels que téléphone, courrier électronique, courrier ou lors d'un entretien confidentiel avec le groupe de confiance; les demandes peuvent également être formulées de manière anonyme, notamment par le biais d'une plateforme d'échange externe sécurisée qui garantit l'anonymat.*

La référence à une plateforme d'échange externe sécurisée garantissant l'anonymat se retrouve dans d'autres dispositions, à savoir aux art. 7 al. 2, 24 al. 4 et 34 al. 2.

Art. 3 : *Si l'employeur ainsi qu'une autre entité sont saisis d'un même signalement, il revient à l'employeur de le traiter en priorité.*

Au sujet de cette disposition, le commentaire précise qu'une autre entité saisie en parallèle de l'employeur ne va pas échanger d'informations avec celui-ci en application du principe de la confidentialité.

Art. 4 *Coordination*

Entre l'entité chargée de la protection et celle ayant reçu le signalement (art. 8, al. 6, 2ème phrase, de la loi)

[1] Le dispositif chargé de la protection peut demander à l'entité qui a reçu un signalement d'irrégularités de lui confirmer si des lanceuses et lanceurs d'alertes ou des personnes témoins ont bien un tel statut.

Entre entités saisies d'un signalement

[2] Lorsque le traitement du signalement sort du champ de compétences de l'entité saisie, cette dernière – lorsqu'elle n'est pas l'employeur – propose aux lanceuses et lanceurs d'alerte de le transmettre à une entité plus à même de le traiter. A défaut d'accord, le signalement est classé.

[3] Lorsque les lanceuses et lanceurs d'alerte annoncent qu'ils ont saisi plusieurs entités d'un même signalement – hors employeur –, ces dernières communiquent entre elles – après accord des lanceuses et lanceurs d'alerte – pour déterminer l'entité la plus à même de traiter le signalement.

[4] L'entité désignée comme la plus à même de traiter le signalement informe les lanceuses et lanceurs d'alerte de ce choix et traite le signalement. L'autre ou les autres entités saisies le classent.

[5] Si les lanceuses et lanceurs d'alerte ne donnent pas leur accord à l'échange entre entités saisies d'un même signalement, chaque entité ayant demandé cet accord peut classer le signalement.

S'agissant de l'alinéa 1, il est précisé que l'accord des lanceuses et lanceurs d'alerte ou des personnes témoins n'est pas requis, dès lors que la loi ne l'exige pas pour la confirmation du statut de lanceuse et lanceur d'alerte ou de personnes témoins à l'entité chargée de la protection.

Art. 9 : *Transmission du signalement (art. 5, al. 4 de la loi)*

[1] Lorsque le signalement porte sur des faits susceptibles de constituer un crime ou un délit poursuivi d'office, le groupe de confiance le transmet au Ministère public et en informe les lanceuses et lanceurs d'alerte.

[2] Dans les autres cas que ceux visés à l'alinéa 1, lorsque le traitement du signalement sort du champ de compétences du groupe de confiance, l'article 4, alinéa 2 du présent règlement est applicable.

L'art. 25 al. 2 du projet prévoit une disposition similaire à l'art. 9 al.1 visant un signalement adressé à la référente alerte. Il en va de même de l'art. 36 al.1 concernant le service d'audit interne.

Art. 11 al. 3 : *Le groupe de confiance a accès à tous les renseignements et à toutes les pièces utiles au traitement d'un signalement.*

L'art. 38 al. 3 du projet prévoit la même disposition concernant le service d'audit interne.

Art. 13 : *Fin du traitement*

[1] A l'issue du traitement de l'alerte, le groupe de confiance fait part de ses conclusions à l'employeur.

[2] Les lanceuses et lanceurs d'alerte sont informés de la remise de ces conclusions mais non de leur contenu.

[3] L'employeur informe le groupe de confiance du type de mesures prises suite à la remise desdites conclusions

Au sujet de l'alinéa 3, il est précisé que l'employeur informe le groupe de confiance du type de mesures prises, sans spécifier lesquelles, dans le respect de la protection des données personnelles. Ainsi, il pourra être indiqué s'il s'agit de mesures de gestion, disciplinaires ou encore s'il y a eu une résiliation des rapports de travail.

L'art. 40 du projet de règlement reprend les mêmes dispositions s'agissant de la fin du traitement par le service d'audit interne.

Art. 17 al. 2 : *Les lanceuses et lanceurs d'alerte ou les personnes témoins reçoivent une copie de la recommandation.*

Art. 23 al. 3 : *Les référentes alertes échangent régulièrement entre elles sur leurs pratiques dans le respect de la confidentialité et de la protection des données.*

Art. 29 : *Information relative au traitement du signalement et aux mesures prises*

[1] La hiérarchie ou l'autorité compétente visée à l'article 28 du présent règlement informent les lanceuses et lanceurs d'alerte que leur signalement a été traité mais non des mesures prises.

[2] Lorsque les faits ont été instruits par une autre entité, la hiérarchie ou l'autorité compétente informe cette dernière du type de mesures prises suite à l'instruction par ladite entité.

[3] Les référentes alerte sont également informées du type de mesures prises.

2. Les règles de protection des données personnelles à Genève

La loi sur l'information du public, l'accès aux documents et la protection des données personnelles du 5 octobre 2001 (LIPAD – A 2 08), a fait l'objet d'une révision importante en 2008, par laquelle la protection des données personnelles a été ajoutée au champ d'application matériel de la loi en sus de son volet relatif à la transparence.

Depuis le 1er janvier 2010, date de l'entrée en vigueur de cette modification législative, un autre objectif figure désormais dans le texte légal à son art. 1 al. 2 litt. b : "*protéger les droits fondamentaux des personnes physiques ou morales de droit privé quant aux données personnelles les concernant*".

Par donnée personnelle, il faut comprendre : "*toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable*" (art. 4 litt. a LIPAD).

Les données personnelles sensibles comprennent les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques, syndicales ou culturelles; la santé, la sphère intime ou l'appartenance ethnique; des mesures d'aide sociale; des poursuites ou sanctions pénales ou administratives (art. 4 litt. b LIPAD).

La LIPAD énonce un certain nombre de principes généraux régissant la collecte et le traitement des données personnelles (art. 35 à 40 LIPAD).

- Base légale (art. 35 al. 1 et 2 LIPAD)

  Le traitement de données personnelles ne peut se faire que si l'accomplissement des tâches légales de l'institution publique le rend nécessaire. En outre, la loi stipule que des données personnelles sensibles ou de profils de la personnalité ne peuvent être traités que si une loi définit clairement la tâche considérée et si le traitement en question est absolument indispensable à l'accomplissement de cette tâche ou s'il est nécessaire et intervient avec le consentement explicite, libre et éclairé de la personne concernée.

- Bonne foi (art. 38 LIPAD)

  Il n'est pas permis de collecter des données personnelles sans que la personne concernée en ait connaissance, ni contre son gré. Quiconque trompe la personne

concernée lors de la collecte des données – par exemple en collectant les données sous une fausse identité ou en donnant de fausses indications sur le but du traitement – viole le principe de la bonne foi. Il agit également contrairement à ce principe s'il collecte des données personnelles de manière cachée.

- Proportionnalité (art. 36 LIPAD)

  En vertu du principe de la proportionnalité, seules les données qui sont nécessaires et qui sont aptes à atteindre l'objectif fixé peuvent être traitées. Il convient donc toujours de peser les intérêts en jeu entre le but du traitement et l'atteinte à la vie privée de la personne concernée en se demandant s'il n'existe pas un moyen moins invasif permettant d'atteindre l'objectif poursuivi.

- Finalité (art. 35 al. 1 LIPAD)

  Conformément au principe de finalité, les données collectées ne peuvent être traitées que pour atteindre un but légitime qui a été communiqué lors de leur collecte, qui découle des circonstances ou qui est prévu par la loi. Les données collectées n'ont ensuite pas à être utilisées à d'autres fins, par exemple commerciales.

- Reconnaissabilité de la collecte (art. 38 LIPAD)

  La collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée. Cette exigence de reconnaissabilité constitue une concrétisation du principe de la bonne foi et augmente la transparence d'un traitement de données. Cette disposition implique que, selon le cours ordinaire des choses, la personne concernée doit pouvoir percevoir que des données la concernant sont ou vont éventuellement être collectées (principe de prévisibilité). Elle doit pouvoir connaître ou identifier la ou les finalités du traitement, soit que celles-ci lui sont indiquées à la collecte ou qu'elles découlent des circonstances.

- Exactitude (art. 36 LIPAD)

  Quiconque traite des données personnelles doit s'assurer de l'exactitude de ces dernières. Ce terme signifie également que les données doivent être complètes et aussi actuelles que les circonstances le permettent. La personne concernée peut demander la rectification de données inexactes.

- Sécurité des données (art. 37 LIPAD)

  Le principe de sécurité exige non seulement que les données personnelles soient protégées contre tout traitement illicite et tenues confidentielles, mais également que l'institution en charge de leur traitement s'assure que les données personnelles ne soient pas perdues ou détruites par erreur.

- Destruction des données (art. 40 LIPAD)

  Les institutions publiques détruisent ou rendent anonymes les données personnelles dont elles n'ont plus besoin pour accomplir leurs tâches légales, dans la mesure où ces données ne doivent pas être conservées en vertu d'une autre loi.

L'art. 39 LIPAD traite de la communication des données, en fonction du destinataire.

La communication de données personnelles à une autre institution publique soumise à la loi est possible aux conditions suivantes :

[1] *Sans préjudice, le cas échéant, de son devoir de renseigner les instances hiérarchiques supérieures dont elle dépend, une institution publique ne peut communiquer des données personnelles en son sein ou à une autre institution publique que si, cumulativement :*

a) l'institution requérante démontre que le traitement qu'elle entend faire des données sollicitées satisfait aux exigences prévues aux articles 35 à 38;

b) la communication des données considérées n'est pas contraire à une loi ou un règlement.

[2] L'organe requis est tenu de s'assurer du respect des conditions posées à l'alinéa 1 et, une fois la communication effectuée, d'en informer le responsable sous la surveillance duquel il est placé, à moins que le droit de procéder à cette communication ne résulte déjà explicitement d'une loi ou d'un règlement.

[3] Les institutions publiques communiquent aux autorités judiciaires les données personnelles que celles-ci sollicitent aux fins de trancher les causes dont elles sont saisies ou de remplir les tâches de surveillance dont elles sont investies, sauf si le secret de fonction ou un autre secret protégé par la loi s'y oppose.

3. Appréciation

Comme mentionné ci-dessus, les Préposés ont été consultés lors de l'élaboration du projet, de sorte que leurs remarques, essentiellement liées à des demandes de clarifications relatives à la coordination entre les différents acteurs, ont été intégrées au projet qui leur est soumis aujourd'hui. Ils n'ont dès lors que peu de commentaires à ajouter.

Ils relèvent que l'accord du lanceur d'alerte est nécessaire à la mise en place de toute démarche de coordination (art. 4), sauf pour la vérification du statut du lanceur d'alerte par l'entité chargée de la protection. Cette disposition a le mérite de répondre aux principes de la bonne foi et de la transparence dans la transmission d'informations. S'agissant des éléments transmis, s'ils visent des données personnelles, il convient que les conditions de l'art. 39 LIPAD soient respectés, particulièrement le principe de la proportionnalité.

Les art. 9 al. 1, 25 al. 2 et 36 al. 1 prévoient que lorsque le signalement porte sur des faits susceptibles de constituer un crime ou un délit poursuivi d'office, l'entité qui traite le signalement le transmet au Ministère public et en informe les lanceuses et lanceurs d'alerte. Il s'agit là d'un rappel de l'art. 33 de la loi d'application du code pénal suisse et d'autres lois fédérales en matière pénale, du 27 août 2009 (LaCP – E 4 10). Le fait que la ou le lanceur d'alerte soit informé de cette transmission est à saluer.

Les art. 11 al. 3 et 38 al. 3 prévoient que le groupe de confiance, respectivement le service d'audit interne, ont un accès à « *tous les renseignements et à toutes les pièces utiles au traitement d'un signalement* ». Une telle disposition est naturellement nécessaire à la bonne réalisation de leur mission. La manière dont elle est rédigée permet un accès large à de nombreuses informations dont potentiellement des données personnelles. Ici encore, dans la mise en œuvre pratique de cet article, il conviendra de respecter les principes de protection des données, en particulier celui de la proportionnalité.

S'agissant des communications prévues à la fin du traitement d'une alerte (art. 13, 29 et 40), les Préposés relèvent que les solutions retenues ont le mérite de prévoir une information au lanceur d'alerte tout en protégeant la personnalité (et donc les données personnelles) d'autres personnes potentiellement concernées. En outre, ils saluent le fait que le lanceur d'alerte reçoive une copie de la recommandation des mesures de protection qui le concernent (art. 17 al. 2). En effet, il s'agit là d'une mise en œuvre du droit d'accès à ses données personnelles.

L'art. 23 al. 3, qui prévoit l'échange régulier entre les référentes alerte sur leurs pratiques, précise que cet échange doit intervenir « *dans le respect de la confidentialité et de la protection des données* ». Cette précision est à saluer, car un tel échange de pratiques doit intervenir sans transmission de données personnelles entre les participants. En effet, une description générique des situations sans mention des personnes concernées suffit à mener à bien un échange de pratique.

Finalement, diverses dispositions font référence à une « *plateforme d'échange externe sécurisée qui garantit l'anonymat* ». Les Préposés attirent l'attention des entités recourant à une telle plateforme que, lors de sa mise en place, il conviendra d'être vigilant quant aux aspects techniques (pas de collecte de données personnelles, telles des adresses IP notamment). Il conviendra également de s'assurer que le tiers externe responsable de la plateforme n'ait pas accès à de telles données.

* * * * * *

Les Préposés remercient la Direction des affaires juridiques de la Chancellerie d'Etat de les avoir consultés et se tiennent à disposition pour tout renseignement complémentaire.

Joséphine Boillat
Préposée adjointe

Stéphane Werly
Préposé cantonal