RGPD et institutions publiques genevoises

Extraits et points saillants de l'avis de droit rédigé par l'Etude Capt & Wyss à la demande du PPDT

FICHE INFO DU PPDT

CE QU'IL FAUT RETENIR

Les institutions publiques genevoises sont soumises à la LIPAD, s'agissant du traitement des données personnelles (art. 3 LIPAD). Elles doivent donc respecter les dispositions prévues par cette loi dans tout traitement de données personnelles.

En plus de l'application de la LIPAD, certaines de ces institutions publiques pourraient devoir appliquer les dispositions du RGPD si le traitement de données personnelles opéré entre dans le champ d'application matériel et territorial de ce règlement. Tel est le cas s'agissant du champ d'application territorial, si:

- ***les traitements de données à caractère personnel sont effectués dans le cadre des activités d'un établissement du responsable de traitement sis sur le territoire de l'UE ;***
- ***les traitements de données à caractère personnel sont liés à l'offre de biens ou de services (gratuits ou non) à des personnes se trouvant sur le territoire de l'UE ;***
- ***les traitements sont liés au suivi du comportement de personnes se trouvant sur le territoire de l'UE, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'UE.***

L'APPLICATION DE LA LIPAD

Pour rappel, l'art. 3 LIPAD régit le champ d'application de cette loi. S'agissant de la protection des données, la loi s'applique aux institutions publiques suivantes, sous réserve des alinéas 3 et 5:

"*a) les pouvoirs exécutif, législatif et judiciaire cantonaux, ainsi que leurs administrations et les commissions qui en dépendent;*

b) les communes, ainsi que leurs administrations et les commissions qui en dépendent;

c) les institutions, établissements et corporations de droit public cantonaux et communaux, ainsi que leurs administrations et les commissions qui en dépendent;

d) les groupements formés d'institutions visées aux lettres a à c".

L'APPLICATION EXTRATERRITORIALE DU RGPD

Dans certains cas, il se peut que des institutions publiques doivent également respecter les dispositions du RGPD en vertu de son application extraterritoriale. En effet, même si le règlement s'applique en premier lieu aux traitements de données à caractère personnel effectués sur le territoire de l'UE (application territoriale), les traitements de données à caractère personnel effectués dans un pays tiers sont également soumis au règlement dans les trois cas suivants (application extra-territoriale) :

- les traitements de données à caractère personnel sont effectués dans le cadre des activités d'un établissement du responsable de traitement sis sur le territoire de l'UE ;
- les traitements de données à caractère personnel sont liés à l'offre de biens ou de services (gratuits ou non) à des personnes se trouvant sur le territoire de l'UE ;
- les traitements sont liés au suivi du comportement de personnes se trouvant sur le territoire de l'UE, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'UE.

Les traitements effectués dans le cadre des activités d'un établissement sur le territoire de l'UE

La notion d'« établissement » a été éclaircie par la Cour de justice de l'UE européenne («CJUE»). En substance, une organisation peut être considérée comme établie dès lors qu'elle exerce « toute activité réelle et effective – même minime » – au moyen d'« une installation stable » sur le territoire de l'UE.

Les traitements liés à l'offre de biens ou de services à des personnes dans l'UE

Déterminer si une institution publique offre des biens et des services dans l'UE requiert une analyse au cas par cas; toutefois, un certain nombre d'éléments peuvent être pris en considération. Ils découlent tant des considérants du RGPD que des éléments retenus par la CJUE dans le contexte du droit de la consommation (dont les auteurs considèrent qu'il est possible de s'inspirer, tout en précisant qu'il y a une certaine incertitude sur les critères qui seront finalement retenus dans l'interprétation du RGPD).

Ainsi, l'on peut retenir que sont des indices:

- le fait que l'entité « envisage » que ses activités cibleront des personnes à l'intérieur de l'UE (l'utilisation d'une langue ou monnaie de l'UE, la capacité à passer des commandes dans cette autre langue, ainsi que le fait de faire référence à des utilisateurs ou clients dans l'UE);
- le paiement de sommes d'argent auprès d'un moteur de recherche dans le but de favoriser l'accès à un site Internet aux personnes situées au sein d'un Etat membre (p.ex. « google.de », « google.fr », etc.), ou le fait de désigner nommément les Etats membres ciblés, constituent des preuves manifestes de l'intention de cibler des personnes au sein de l'UE;
- le fait de mentionner des numéros de téléphone présentant un indicatif international, l'utilisation d'un nom de domaine de premier niveau autre que celui de l'Etat dans lequel l'entité est établie (p.ex. « .de », « .fr », « .eu », etc.), la description d'itinéraires depuis les Etats membres vers le lieu où le service est fourni, ainsi que le fait de mentionner une « clientèle internationale composée de clients domiciliés dans différents Etats membres ».

Les traitements liés au suivi d'un comportement qui a lieu au sein de l'UE

Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur Internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit.

Exemples de traitements pouvant être soumis au RGPD, en vertu de son application extraterritoriale :

- Un aéroport fait la promotion de divers services (p.ex. parking, location de véhicules, transport vers les stations de ski, etc.) sur son site Internet, accessible en anglais. Les traitements de données à caractère personnel collectées par le site Internet ou lors de l'usage des services décrits sur le site Internet pourraient être soumis au RGPD.
- Une entreprise de transports publics cible ostensiblement des personnes qui se trouvent dans l'UE en leur permettant d'acheter des abonnements ou des cartes journalières depuis leur lieu de situation. Les traitements de données personnelles liés à aux offres ciblant les personnes de passage pourraient être soumis au RGPD.
- Une commune fait la promotion d'un événement dans un Etat membre de l'UE, pour lequel elle sollicite l'inscription des participants. Le traitement des données à caractère personnel des participants pourrait être soumis au RGPD.
- Une université ou une haute école accueille des étudiants européens dans le cadre d'un programme d'échange avec des Etats membres de l'UE.
- Une entreprise de transports publics exploite des lignes de bus qui desservent des usagers sur le territoire de l'UE. Les traitements de données à caractère personnel qui concernent les usagers sur le territoire de l'UE pourraient être soumis au RGPD, quand bien même lesdits usagers auraient acheté leur abonnement en Suisse.
- Une entité publique collecte des données relatives au comportement d'utilisateurs se trouvant sur le territoire de l'UE visitant son site Internet (p.ex. adresses IP, fréquence de connexion, pages consultées, etc.). Le traitement de ces données devrait être soumis au RGPD.
- Le traitement de données à caractère personnel en lien avec des prestations prévues par un traité international, et dont les ayants droits sont des personnes physiques se trouvant dans l'UE, pourrait éventuellement être soumis au RGPD. Ce cas de figure pourrait notamment concerner l'export des prestations fondées sur la loi fédérale sur l'assurance-vieillesse et survivants. Il s'agit toutefois d'un cas limite, puisqu'il s'agit plutôt de prestations que d'une offre de biens ou de services.

Exemples de traitements non soumis au RGPD:

Il sied de rappeler que les critères de la nationalité ou du lieu de résidence des personnes concernées ne sont pas des critères pertinents, s'agissant de l'application du RGPD. Ce sont uniquement les 3 cas de figure décrits ci-dessus qui sont déterminants.

De plus, le règlement ne s'applique pas, notamment, aux traitements de données à caractère personnel effectués dans le cadre des politiques relatives aux contrôles aux frontières, à l'asile et à l'immigration, ainsi qu'à ceux effectués par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces.

Ainsi, ne sont en principe pas soumises au RGPD les situations suivantes:

- Une entreprise de transports publics exploite des lignes de bus exclusivement en Suisse. Les traitements des données à caractère personnel de citoyens de l'UE qui ont acheté un abonnement en Suisse ne sont en principe pas soumis au RGPD, pour autant qu'ils n'étaient pas ciblés.
- Une entité traite les données à caractère personnel de ses employés ou fonctionnaires qui résident et/ou ont la nationalité d'un Etat membre de l'UE (p.ex. travailleurs frontaliers).
- Une banque cantonale offre ses services à des clients qui résident et/ou ont la nationalité d'un Etat membre de l'UE, sans avoir fait de promotion dans l'UE et sans disposer d'un établissement (y compris un simple représentant) dans l'UE.
- Un hôpital cantonal traite des patients qui résident et/ou ont la nationalité d'un Etat membre de l'UE, sans avoir fait la promotion de ses services dans l'UE.
- L'instruction publique accueille des élèves qui résident et/ou ont la nationalité d'un Etat membre de l'UE, sans avoir fait de promotion sur le territoire de l'UE.
- L'office cantonal de la population et des migrations traite, dans le cadre de sa mission d'intérêt public, les données à caractère personnel concernant des personnes qui résident et/ou ont la nationalité d'un Etat membre de l'UE.

LES OBLIGATIONS DECOULANT DU RGPD, DANS LES GRANDES LIGNES:

- Le respect des principes relatifs au traitement des données personnelles (principes de licéité, de loyauté et de transparence, de limitation des finalités, de minimisation des données, d'exactitude, de limitation de la conservation, d'intégrité et de confidentialité)- art. 5 RGPD
- Bénéficier d'un des motifs justificatifs permettant de traiter des données personnelles - art. 6 RGPD
- Etre attentif aux conditions spécifiques liées au traitement de données sensibles / aux conditions applicables au consentement des enfants – art. 8 et 9 RGPD
- Assurer l'information requise aux personnes concernées – art. 12–14 RGPD
- Mettre en place les droits des personnes concernées – art. 15-22 RGPD
- Respecter les règles en cas de sous-traitance ou de transfert des données dans un Etat tiers – art. 24-27 et 44-49 RGPD
- Tenir un registre des activités de traitement – art. 30 RGPD (cette obligation s'apparente au catalogue des fichiers; pour plus de détails, voir: https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement)
- Assurer la sécurité des données et notifier / communiquer en cas de violation de données à caractère personnel - art. 32 – 34 RGPD
- Mener une analyse d'impact dans les cas prévus par l'art. 35 RGPD
- Désigner un délégué à la protection des données - art. 37 RGPD (à notre sens, il peut s'agir du responsable LIPAD).

REMARQUE FINALE:

La notion de soumission au RGPD ne s'envisage pas de façon globale (toutes les données personnelles collectées et traitées par l'entité visée) mais uniquement en relation avec un traitement de données particulier. Il est ainsi fort possible qu'une institution publique ne soit soumise au RGPD que pour une partie des données qu'elle traite (p.ex. les données récoltées à l'occasion d'un jeu concours visant des personnes physiques se trouvant sur le territoire de l'Union européenne).

Enfin, il sied de rappeler une nouvelle fois que les institutions de droit public sont au premier chef soumises à la LIPAD et à son règlement d'application, le RIPAD. Même en cas d'application du RGPD à certains traitements, la LIPAD restera également applicable.

PPDT - Màj : 28.01.2019

Le Préposé cantonal à la protection des données et à la transparence (PPDT) est une autorité indépendante qui renseigne, conseille et surveille l'application de la LIPAD par les autorités et institutions publiques genevoises. N'hésitez pas à appeler en cas de questions au n° de téléphone 022 546 52 40 ou à adresser un courriel à ppdt@etat.ge.ch.