GUIDE PRATIQUE RGPD

A L'ATTENTION DES INSTITUTIONS PUBLIQUES GENEVOISES

Table des matières

Introduction

Le présent guide pratique, rédigé par l'Etude CAPT & WYSS à la demande du *Préposé cantonal à la protection des données et à la transparence*, a pour vocation de donner aux institutions publiques genevoises soumises à la LIPAD un aperçu de l'impact éventuel du RGPD sur la marche de leurs activités courantes et de leur prodiguer quelques conseils généraux.

Il a pour but de permettre à ces institutions de déterminer, pour chaque traitement de données, si une application extraterritoriale du RGPD doit être *prima facie* envisagée.

Ce guide ne remplace toutefois pas un conseil juridique spécifique pour une situation donnée, par principe individuelle, et ne saurait engager la responsabilité de ses rédacteurs.

***

Le Règlement 2016/679/UE du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données ; « RGPD ») est entré en vigueur le 25 mai 2016, et s'applique depuis le 25 mai 2018.

Contrairement à la Directive européenne 95/46/CE qu'il a abrogée, le RGPD s'applique à certains traitements de données personnelles effectués hors du territoire de l'Union européenne (« UE »), que ce soit par des personnes morales de droit privé ou de droit public.

Le but du présent document est d'aider les entités de droit public à déterminer si des traitements de données personnelles qu'elles effectuent entrent dans le champ d'application du RGPD, et de présenter de manière sommaire les principes généraux de protection des données édictés par le règlement.

Champ d'application matériel et notions générales

Champ d'application matériel

Le RGPD s'applique au traitement de données à caractère personnel, automatisé en tout ou partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier (art. 2 § 1 RGPD).

Les données à caractère personnel

Notion de données à caractère personnel

Le règlement s'applique aux « données à caractère personnel », c'est-à-dire à toute information se rapportant à une personne physique identifiée ou identifiable (art. 4 § 1 RGPD). En revanche, il ne s'applique ni aux données anonymes, ni à celles qui concernent des personnes morales ou des personnes physiques décédées.

En d'autres termes, l'application du règlement est subordonnée à la possibilité d'identifier la personne concernée par une/des donnée(s), notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique,

économique, culturelle ou sociale (art. 4 § 1 RGPD). Savoir si une personne physique est identifiable dépendra des moyens raisonnablement susceptibles d'être utilisés pour l'identifier, notamment du coût de l'identification et du temps nécessaire à celle-ci, en tenant compte des technologies disponibles et de leur évolution. La conception de la notion de donnée à caractère personnel adoptée par le législateur européen est donc particulièrement large. A titre exemplatif, une adresse IP, des témoins de connexion (*cookies*) ou encore des tags RFID (par exemple des cartes de contrôle d'accès utilisant cette technologie) peuvent constituer des données à caractère personnel, dans la mesure où des données disponibles auprès de tiers (p.ex. fournisseurs d'accès Internet s'agissant de l'adresse IP) permettent d'identifier la personne concernée.

Le champ d'application du règlement englobe toutes les formes que peut prendre l'information, indépendamment du message véhiculé. Il peut notamment s'agir de caractères alphanumériques, d'images ou de sons, relevant de la vie privée ou professionnelle de la personne concernée, ainsi que de certains aspects de sa vie publique.

Exemple de données à caractère personnel pouvant être soumises au RGPD :

- Une entité publique collecte les adresses du domicile des personnes ayant utilisé ses prestations. Etant donné que ces adresses peuvent permettre d'identifier les personnes concernées, il s'agit de données à caractère personnel au sens du RGPD.

Exemple de données anonymes qui ne sont pas soumises au RGPD :

- Une entité publique ne collecte que les codes postaux des personnes ayant utilisé ses prestations. Dans la mesure où les codes postaux ne permettent pas d'identifier les personnes concernées, il ne s'agit pas de données à caractères personnel mais de données anonymes, et leur traitement n'est en tout état de cause pas soumis au RGPD.

Les données pseudonymisées

La pseudonymisation consiste à faire en sorte que des données à caractère personnel ne puissent plus être attribuées à une personne précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractères personnel ne soient pas attribuées à la personne concernée.

Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires doivent être considérées comme des informations concernant une personne physique identifiable, c'est-à-dire comme des données à caractère personnel au sens du RGPD. Leur traitement est donc soumis au règlement.

Exemple de pseudonymisation soumise au RGPD:

- Une entité publique transmet des données à caractère personnel à une autre entité, à des fins statistiques ou de contrôle. Le fichier transmis contient le numéro identifiant, le montant du loyer et le montant du revenu annuel de chaque personne concernée, à l'exclusion de toute autre information. Les données contenues dans le fichier transmis sont pseudonymisées étant donné que le numéro identifiant permet d'attribuer les données aux personnes concernées en ayant recours aux informations supplémentaires détenues par l'entité qui a transmis le fichier.

Les données anonymes ou anonymisées

Comme nous l'avons vu, le traitement de données anonymes n'est pas soumis au RGPD.

Les données peuvent être anonymes dès leur collecte. Tel est le cas lorsque la collecte porte exclusivement sur des informations qui ne permettent pas d'identifier les personnes concernées, telles que le code postal ou l'âge, par exemple à des fins statistiques.

Il est également possible d'anonymiser des données à caractère personnel (qui ne sont alors plus des données à caractère personnel) afin que leur traitement ne soit plus soumis au RGPD. Pour rendre des données anonymes, il faut en retirer suffisamment d'éléments pour que la personne concernée ne puisse plus être identifiée. Plus précisément, les données doivent être traitées de façon à ne plus pouvoir être utilisées pour identifier une personne physique en recourant à l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par un tiers. Un facteur important est que le traitement doit être irréversible.

Exemple de données anonymes dont le traitement n'est pas soumis au RGPD :

- Une entreprise de transports publics collecte, à des fins statistiques, les codes postaux des usagers, et enregistre ces données dans un fichier qui ne mentionne pas leur nom, leur adresse précise ou tout autre information permettant de les identifier, et sans possibilité de faire le lien avec de telles informations (p.ex. au moyen d'un identifiant). Le traitement des codes postaux à partir du fichier précité n'est en tout état pas soumis au RGPD (ce ne sont pas des données à caractère personnel au sens du RGPD).

Exemples de données non anonymes dont le traitement peut être soumis au RGPD :

- Une entreprise de transports publics collecte, à des fins statistiques, les adresses des usagers, et enregistre ces données dans un fichier qui ne mentionne pas leur nom ou tout autre information permettant de les identifier, et sans possibilité de faire le lien avec de telles informations (p.ex. au moyen d'un identifiant). Etant donné qu'un usager peut, dans certains cas, être identifié par sa seule adresse, il s'agit de données à caractère personnel dont le traitement pourrait être soumis au RGPD.
- Une commune collecte les adresse IP des utilisateurs de son site Internet. Les utilisateurs pouvant être identifiés par leur seule adresse IP, notamment par recoupement avec d'autres informations détenues par des tiers ou par son fournisseur d'accès, il s'agit de données à caractère personnel dont le traitement pourrait être soumis au RGPD.

Exemple d'anonymisation de données à caractère personnel :

- Une commune collecte des données concernant l'utilisation de son site Internet, soit l'adresse IP des utilisateurs, la date et l'heure à laquelle ils ont consulté le site et la durée de la connexion, à l'exclusion de toute autre information (traitement soumis au RGPD). Une fois les adresses IP définitivement effacées, les seules données relatives aux dates et aux durées de connexion peuvent être considérées comme des données anonymes de sorte que leur traitement ultérieur n'est pas soumis au RGPD.

Le traitement de données à caractère personnel

Un traitement de données à caractère personnel n'est soumis au RGPD que s'il est automatisé en tout ou partie, ou si les données sur lesquelles il porte sont contenues ou appelées à figurer dans un fichier.

La notion de « traitement » désigne toute opération appliquée à des données. Cela inclut naturellement la collecte, l'enregistrement, l'organisation, la structuration, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition de données à caractère personnel, mais aussi la simple conservation ainsi que l'effacement ou la destruction (art. 4 § 2 RGPD).

Le traitement automatisé en tout ou partie

La notion de « traitement automatisé en tout ou partie » fait essentiellement référence au traitement informatique des données à caractère personnel, y compris leur simple conservation ou

archivage sur un support de stockage, que celui-ci soit ou non connecté au système d'information (la simple possibilité d'exploiter les données archivées au moyen d'une machine suffit).

Les données appelées à figurer dans un fichier

Quant à la notion de « fichier », elle désigne tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique (art. 4 § 6 RGPD). Un document physique (*i.e.* papier ou tout autre support non numérique) contenant une liste de personnes ou des dossiers physiques les concernant organisés de manière structurée (p.ex. par ordre alphabétique) constitue donc un fichier au sens RGPD, de sorte que le traitement des données à caractère personnel destinées à y figurer (y compris et dès leur collecte) peut être soumis au règlement.

A notre sens, considérer qu'un ensemble de documents ou de dossiers physiques constituent un fichier au sens du RGPD suppose que l'on puisse savoir si cet ensemble contient des données concernant une personne ou un groupe de personnes déterminés en fonction de certains critères, sans avoir à consulter l'ensemble des documents.

En revanche, le traitement de données à caractère personnel disséminées dans un ensemble de documents ou dossiers physiques sans qu'il soit possible d'effectuer une recherche en fonction de certains critères n'est en principe pas soumis au RGPD. Il en va de même d'un document physique isolé destiné à la destruction à brève échéance sans que les données à caractère personnel qu'il contient ne soient conservées sur un autre support (p.ex. notes de réunion, courrier reçu destiné à la destruction, etc.).

Exemples de traitements de données à caractère personnel pouvant être soumis au RGPD :

- Une entité publique enregistre des documents contenant des données à caractère personnel dans son système informatique. Considérant qu'il est possible d'effectuer une recherche des données concernant une personne déterminée, par exemple à partir de son nom, et ce indépendamment de la structure de la base de données contenant les documents (ou de l'absence de structure de celle-ci), le traitement de ces données peut être soumis au RGPD.
- Une entité publique tient une liste des participants à un projet sur un document physique. Etant donné que ce document permet d'identifier les personnes participant au projet, le traitement de leurs données à caractère personnel peut être soumis au RGPD.

Exemple de traitement de données à caractère personnel non soumis au RGPD :

- Une entité publique dispose d'un dossier physique relatif à un projet dans lequel apparaissent, sur divers documents, des noms de participants et personnes concernées par le projet. Dans la mesure où il n'est pas possible d'extraire la liste des personnes concernées ou de rechercher une personne déterminée de manière systématique, la conservation ou la consultation de ces données dans le dossier physique du projet ne sont en principe pas des traitements de données à caractère personnel soumis au RGPD.

Le champ d'application matériel en résumé

Il faut retenir que les notions de « traitement », de « données à caractère personnel » et de « fichier » sont définies de manière très large par le règlement, de sorte que celui-ci peut trouver à s'appliquer dans la plupart des situations où des données peuvent être associées à des personnes physiques. Il suffit en effet que le traitement soit informatisé ou, s'agissant de documents ou dossiers physiques, qu'il soit possible d'accéder aux données à caractère personnel selon des critères déterminés, ce qui est généralement le cas lorsque ceux-ci sont classés de manière systématique.

A notre sens, les seuls traitements qui échappent au champ d'application matériel du règlement sont ceux qui portent sur de données à caractère personnel contenues dans un document physique destiné à la destruction, ou disséminées dans un ensemble de documents physiques sans qu'il soit possible d'y accéder selon des critères déterminés (le système de classement étant fondé sur des critères qui n'entretiennent absolument aucun lien avec les personnes dont les données sont disséminées dans lesdits documents).

Champ d'application territorial du RGPD

Application extraterritoriale

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

Le RGPD s'applique aux traitements des données à caractère personnel effectués dans le cadre des activités d'un établissement sur le territoire de l'UE, que le traitement ait lieu ou non dans l'UE.

La notion d'« établissement » a été éclaircie par la Cour de justice de l'UE européenne (« CJUE ») dans l'affaire de 2015 *Weltimmo c. NAIH*[1]. La Cour a considéré que la notion d'établissement était une notion large et souple, qui ne devait pas dépendre de la forme juridique de l'établissement. 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. La présence d'un seul représentant peut être suffisante.

[1] C-230/14.

Exemple de traitement pouvant être soumis au RGPD :

- 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.

Exemple de traitement non soumis au RGPD :

- 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 (Il en irait différement si les usagers avaient acheté leur abonnement sur un site Internet ciblant spécifiquement des personnes se trouvant sur le territoire de l'UE ; *cf. infra* « Les traitements liés à l'offre de biens ou de services à des personnes dans l'UE »).

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

Les traitements de données à caractère personnel effectués par des entités qui ne disposent pas d'un établissement dans l'UE peuvent également être soumis au RGPD lorsque ces traitements sont liés à l'offre de biens ou de services à des personnes qui se trouvent sur le territoire de l'UE, qu'un paiement soit ou non exigé desdites personnes (art. 3 § 2 let. a RGPD).

La simple accessibilité à un site Internet à partir de l'UE n'est pas suffisante pour que le traitement des données collectées soit soumis au RGPD, quand bien même des personnes physiques qui utilisent ce site Internet seraient résidents ou nationaux d'un Etat membre de l'UE. Il doit être apparent que l'entité « envisage » que ses activités cibleront des personnes à l'intérieur de l'UE. Aux fins de déterminer si tel est le cas, des critères tels que 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 entreront en considération.

La CJUE s'est penchée sur la question de savoir dans quels cas une offre de biens et services pouvait être considérée comme « tournée vers » des États membres de l'UE dans le contexte du droit de la consommation[2]. Ses commentaires sont susceptibles de faciliter l'interprétation des dispositions équivalentes du RGPD. Outre les considérations énoncées ci-dessus, la CJUE a estimé que 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 État membre (p.ex. « google.de », « google.fr », etc.), ou le fait de désigner nommément les États membres ciblés, constituent des preuves manifestes de l'intention de cibler des personnes au sein de l'UE. D'autres facteurs, susceptibles d'être combinés les uns aux autres, peuvent mener à considérer qu'une entité cible des personnes au sein de l'UE, parmi lesquels la « nature internationale » de l'activité en question (p.ex. certaines activités de tourisme), 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'État dans lequel l'entité est établie (p.ex. « .de », « .fr », « .eu », etc.), la description d'itinéraires depuis les États membres vers le

[2] Dans le contexte de l'application du Règlement Bruxelles I (44/2001/CE) « concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale ».

lieu où le service est fourni, ainsi que le fait de mentionner une « clientèle internationale composée de clients domiciliés dans différents États membres ». La CJUE a précisé que cette liste de critères est « non exhaustive » et que la question doit être tranchée au cas par cas[3]. Il faut également garder à l'esprit que cette jurisprudence a été rendue dans le contexte du droit de la consommation, de sorte que la CJUE pourrait établir d'autres critères s'agissant de l'application du RGPD.

Exemples de traitements pouvant être soumis au RGPD :

- 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.
- A notre sens, 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, selon nous, d'un cas limite puisqu'il s'agit plutôt de *prestations* que d'une offre de biens ou de services.

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

Les traitements de données à caractère personnel effectués par des entités qui ne disposent pas d'un établissement dans l'UE peuvent enfin être soumis au RGPD lorsque ces 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 (art. 3 § 2 let. b RGPD).

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.

[3] *Pammer c. Reederei Karl Schlüter GmbH & Co*, et *Hotel Alpenhof c. Heller* (Affaires jointes C-585/08 et C-144/09).

Exemples de traitement pouvant être soumis au RGPD :

- 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.
- Une université ou une haute école offre des cours ouverts en lignes (MOOC) et collecte et analyse des données personnelles, par exemple concernant les cours suivis ou les résultats de tests en ligne, lorsque la personne considérée se trouve sur le territoire de l'UE. Dans ce cas de figure, le traitement peut être soumis au RGPD tant en vertu d'une offre de services à des personnes dans l'UE qu'en vertu du suivi d'un comportement qui a lieu au sein de l'UE.

Absence de pertinence de la nationalité et du lieu de résidence des personnes concernées

De manière générale, le règlement protège les personnes physiques indépendamment de leur nationalité ou de leur lieu de résidence. Pour que le règlement s'applique à un traitement effectué hors de l'UE, il est à la fois nécessaire et suffisant que celui-ci soit effectué dans le cadre des activités d'un établissement au sein de l'UE, ou qu'il soit en lien avec l'offre de biens ou de services à des personnes se trouvant sur le territoire de l'UE ou avec le suivi du comportement de ces personnes. A défaut, le traitement effectué hors de l'UE n'est pas soumis au RGPD, quand bien même il porterait sur des données qui concernent des citoyens de l'UE.

Exemples de traitements non soumis au RGPD :

- 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.

Traitement de données à caractère personnel exclu

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 (art. 2 § 1 lit. b et d RGPD).

> Exemple de traitement de données à caractère personnel exclu du champ d'application du RGPD :
>
> - L'office cantonal de la population 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 principes généraux du RGPD

Les principes relatifs au traitement des données à caractère personnel

Lorsque le traitement de données à caractère personnel est soumis au règlement, celles-ci doivent être[4] :

- traitées de manière licite, loyale et transparente au regard de la personne concernée (principes de licéité, de loyauté et de transparence) ;
- collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (principe de limitation des finalités) ;
- adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de minimisation des données) ;
- exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (principe d'exactitude) ;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de limitation de la conservation) ;
- traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (principes d'intégrité et de confidentialité).

La licéité du traitement

Un traitement de données à caractère personnel n'est licite que s'il repose sur un motif justificatif, soit notamment si[5] :

- la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

[4] Cf. art. 5 § 1 RPGD.
[5] Cf. art. 6 § 1 let. a), b), d) et f) RPGD.

- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée, notamment lorsque la personne concernée est un enfant. Ce dernier point ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

S'agissant des traitements effectués par des personnes morales de droit public, les deux motifs justificatifs suivants revêtent, à notre sens, une importance toute particulière[6] :

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

En outre, les institutions publiques genevoises doivent garder à l'esprit que l'art. 35 LIPAD exige qu'un traitement de données personnelles soit nécessaire à l'accomplissement de leurs tâches légales.

Le consentement de la personne concernée[7]

Le RGPD définit le consentement comme étant toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement. Le consentement ne peut pas être implicite ou tacite, ce qui signifie qu'il ne suffit pas que le traitement soit reconnaissable pour la personne concernée et que celle-ci ne s'y soit pas opposé.

Il incombe au responsable du traitement de prouver que la personne concernée a donné son consentement (art. 7 § 1 RGPD). Le recueil du consentement doit être présenté sous une forme qui le distingue clairement de toute autre question, de manière compréhensible et aisément accessible, et formulé en des termes clairs et simples (art. 7 § 2 RGPD). En outre, la personne concernée a le droit de retirer son consentement à tout moment sous une forme qui doit être aussi simple et accessible que celle utilisée pour donner son consentement (art. 7 § 3 RGPD).

Concrètement, il est exclu que le recueil du consentement soit noyé dans des conditions générales ou dans tout autre document portant également sur d'autres questions. Pour être valable, il nécessite un comportement actif de la personne concernée. A titre exemplatif, la personne concernée peut être invitée à cocher des cases pour chaque finalité de traitement à laquelle elle consent, sur la page d'un site Internet ou sur un document *ad hoc*, lesquels devront dans tous les cas être clairement distincts des autres conditions d'utilisation du service.

Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat (art. 7 § 4 RGPD). En d'autres termes, pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas le motif justificatif pour un traitement lorsqu'il existe un déséquilibre manifeste entre la personne concernée et l'entité qui traite ses données, en particulier lorsque celle-ci est une autorité publique et qu'il est improbable

---

[6] Cf. art. 6 § 1 let. c) et e) RPGD.

[7] Il convient de relever, au vu de l'application de l'art. 35 LIPAD aux institutions publiques genevoises, que le RGPD trouve également application ou non, qu'il est fort improbable que le consentement ait un rôle central à jouer pour légitimer un traitement de données personnelles par les institutions publiques genevoises. Est réservé l'art. 35 al. 2 LIPAD, dans le cadre du traitement de données personnelles sensibles.

que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière. Le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné pour les traitements qui sont absolument nécessaires à la fourniture d'une prestation et ceux qui ne le sont pas (p.ex. traitement à des fins statistiques ou promotionnelles). Il en va de même lorsque l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution.

Ainsi, une entité publique ne devrait pas subordonner la fourniture d'une prestation au fait que la personne concernée consente à ce que ladite entité puisse effectuer des traitements de ses données à caractère personnel qui ne sont pas strictement nécessaire à la fourniture de la prestation fournie. De manière générale, on peut considérer que le consentement a été donné librement lorsque la personne concernée ne s'expose à aucun préjudice d'aucune sorte en refusant de le donner.

Exemple de recueil de consentement qui n'est pas valablement donné :

- Une université qui offre des cours ouverts en ligne (MOOC) subordonne la fourniture de cette prestation au fait que les utilisateurs consentent, en cochant une case au moment de leur inscription, à ce que leurs données à caractère personnel soient traitées aux fins de leur permettre d'accéder à la plateforme pour suivre les cours, leur communiquer des informations utiles en lien avec leur cursus, les évaluer en vue de la délivrance d'un certificat ou diplôme, ainsi qu'à des fins statistiques. Dans la mesure où le traitement des données à caractère personnel à des fins statistiques n'est pas absolument nécessaire à la fourniture des cours ouverts en ligne, le consentement à un tel traitement aurait dû être recueilli de manière distincte pour cette finalité particulière, et ce sans qu'un éventuel refus à cet égard n'expose les personnes concernées à un quelconque préjudice. Le consentement donné en cochant une case unique pour toutes les finalités annoncées n'est donc pas libre, de sorte qu'il ne constitue pas un motif justificatif pour le traitement des données des utilisateurs à des fins statistiques.

Les traitements nécessaires à l'exécution d'un contrat

Un traitement de données à caractère personnel est en principe considéré comme licite lorsqu'il est nécessaire dans le cadre d'un contrat ou de l'intention de conclure un contrat.

Exemple de traitements nécessaires dans le cadre de l'exécution d'un contrat ou de l'intention de conclure un contrat :

- Une entité publique traite des données à caractère personnel concernant des employés d'entreprises qui lui fournissent des biens ou services. Les traitements de données à caractère personnel qui sont strictement nécessaires à la bonne exécution des prestations convenues sont en principe licites, sans qu'il soit nécessaire de recueillir le consentement des personnes concernées. A titre exemplatif, on pense aux données à caractère personnel contenues dans des courriels ou des documents contractuels, ou toute autre communication ou document nécessaire à l'exécution des prestations.
- Dans le cadre d'une procédure d'appel d'offres, une entité publique traite des données à caractère personnel qui lui ont été transmises par les soumissionnaires (p.ex. nom de l'architecte d'un projet, etc.). Les traitements de données à caractère personnel qui sont strictement nécessaires au bon déroulement de la procédure de soumission sont en principe licites, sans qu'il soit nécessaire de recueillir le consentement des personnes concernées.

Les traitements liés au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public

Selon le règlement, pour qu'un traitement soit justifié par une obligation légale à laquelle le responsable du traitement est soumis ou par l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, le traitement en cause devrait avoir un fondement dans le droit de l'Union ou dans le droit d'un État membre[8].

A notre sens, dans le cadre de l'application extraterritoriale du règlement, celui-ci devrait être interprété en ce sens qu'un traitement de données à caractère personnel est en principe justifié s'il est strictement nécessaire au respect d'une obligation ou à l'exécution d'une mission d'intérêt public prévues par une base légale du pays tiers.

Exemple de traitement nécessaire au respect d'une obligation ou à l'exécution d'une mission d'intérêt public prévues par une base légale :

- Une entreprise de transports publics traite des données à caractère personnel concernant les titulaires d'un abonnement de transport. Les traitements strictement nécessaires à des fins de contrôle sont en principe justifiés, sans qu'il soit nécessaire de recueillir le consentement des personnes concernées.
- Une université traite des données à caractère personnel concernant les étudiants. Le traitement des résultats des évaluations des étudiants dans une base de données est nécessaire à l'exécution de la mission d'intérêt public de l'université et est, dans cette stricte mesure, justifié, sans qu'il soit nécessaire de recueillir le consentement des étudiants concernés.

[8] Cf. consid. 45 RGPD.

Le traitement des données sensibles

Des catégories particulières de données personnelles, également dénommées « données sensibles[9] », obéissent à un régime juridique plus protecteur. Il s'agit des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques, des données biométriques traitées aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique[10].

La liste des motifs susceptibles de justifier le traitement de données sensibles est plus limitative que celle relative aux autres données à caractère personnel.

Le traitement de données sensibles est justifié, notamment, s'il est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée (art. 9 § 2 let. g RGPD). A notre sens, dans le cadre de l'application extraterritoriale du RGPD, cette disposition peut être interprétée en ce sens que le traitement est justifié s'il est nécessaire à la poursuite d'un but d'intérêt public important et qu'il est prévu par une base légale formelle.

S'agissant des autres motifs justificatifs, nous nous bornerons ici à mentionner les suivants[11] :

- la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques ;
- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
- le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées ;
- le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ;
- le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle.

Sous-traitance

Le règlement autorise la sous-traitance. Le responsable du traitement demeure toutefois responsable du respect des principes de licéité, loyauté, transparence, limitation des finalités, minimisation des données, exactitude, limitation de la conservation, intégrité et confidentialité (art. 5 § 2 RGPD).

---

[9] Cf. consid. 10 RGPD.
[10] Art. 9 RGPD.
[11] Cf. art. 9 § 2 RGPD.

Il incombe ainsi au responsable du traitement de définir la nature et les catégories de données que le sous-traitant va collecter pour le compte du responsable du traitement, les finalités poursuivies par le traitement délégué, la durée de conservation des données, les traitements effectués, les destinataires (personnes ayant accès aux données) mais également les exigences de sécurité à mettre en œuvre par le sous-traitant.

Il incombe au responsable du traitement de choisir des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement et garantisse la protection des droits des personnes concernés (art. 28 § 1 RGPD).

La relation avec le sous-traitant doit être formalisée dans un contrat écrit qui contient des clauses précises quant à la protection des données personnelles, notamment la répartition des tâches et obligations émanant du RGPD (le contrat doit régler, notamment mais pas exclusivement, la ou les finalités du traitement, la durée de conservation des données, la typologie des données traitées et des personnes concernées, les engagements du sous-traitant, la mise en œuvre et le maintien d'une documentation précise concernant les mesures de protection et de confidentialité, les modalités de notification des violations de données ou encore le *disaster recovery plan*).

En cas de violation de la protection des données chez le sous-traitant, le responsable du traitement doit être en mesure de démontrer qu'il a fait preuve de toute la diligence requise par les circonstances (sensibilité des données, par exemple) et notamment dans le choix, l'encadrement et la surveillance du sous-traitant. A défaut, sa responsabilité pourrait être engagée aux côtés de celle du sous-traitant.

S'agissant des institutions publiques genevoises, il est rappelé qu'elles doivent en tout état et en sus se soumettre, en matière de sous-traitance, aux exigences de l'art. 13a RIPAD (p.ex. encadrement contractuel obligatoire, respect des prescriptions de la LIPAD par le sous-traitant, possibilité d'effectuer un audit sur le site du sous-traitant, etc.).

Exemple de circonstances dans lesquelles une violation de la protection des données par le sous-traitant est de nature à engager la responsabilité du responsable du traitement

- Une institution publique genevoise sous-traite tout ou partie du traitement de données personnelles soumises au RGPD sans avoir fixé par contrat, les obligations du sous-traitant relatives au respect des dispositions du Règlement.

A noter qu'une telle situation constitue par ailleurs une violation de la LIPAD et de l'art. 13a RIPAD.

Les failles de sécurité (*data breach*)

La notion de « violation de données à caractère personnel » désigne une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données (art. 4 § 12 RGPD).

En cas de violation de données à caractère personnel, le responsable du traitement a l'obligation de notifier la violation en question à l'autorité de contrôle compétente, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernée (art. 33 § 1 RGPD).

A notre sens, cette disposition revêt une importance particulière considérant qu'elle permet de diminuer la gravité de l'atteinte subie par les personnes concernées en cas de violation de leurs données, cas échéant de leurs données sensibles.

Aussi, si une entité publique s'estime soumise au RGPD, la mise en place d'une procédure adéquate nous paraît absolument nécessaire.

Droit des personnes concernées

Le responsable du traitement de données à caractère personnel doit être en mesure de garantir les droits suivants aux personnes concernées[12] :

- droit d'information et d'accès aux données personnelles ;
- droit de rectification et d'effacement (ou « droit à l'oubli ») des données personnelles ;
- droit à la limitation du traitement de données personnelles ;
- droit à la portabilité des données personnelles si les conditions de l'art. 20 RGPD sont remplies;
- droit d'opposition à un traitement de données personnelles ;
- droit de ne pas faire l'objet d'une décision individuelle automatisée y compris le profilage.

Les droits précités reçoivent des limitations, notamment lorsqu'une base légale prévoit une telle limitation et qu'elle constitue une mesure nécessaire et proportionnée pour garantir, notamment :

- la sécurité nationale ;
- la défense nationale ;
- la sécurité publique ;
- la prévention et la détection d'infractions pénales
- d'autres objectifs importants d'intérêt public ;
- la protection de l'indépendance de la justice et des procédures judiciaires ;
- la prévention et la détection de manquement à la déontologie des professions réglementées.

Conformité au RGPD

Outre le respect des principes relatifs au traitement des données à caractères personnel, la conformité au RGPD suppose la mise en œuvre de mesures techniques et organisationnelles dont l'analyse excède le cadre du présent guide pratique, étant précisé que de telles mesures doivent être en adéquation avec la taille et la nature des activités de chaque organisation.

Par ailleurs, si les institutions publiques n'ont pas à désigner un représentant dans l'Union européenne (art. 27 RGPD), elles doivent toutefois désigner un délégué à la protection des données (art. 37 § 1 let. a RGPD), qui peut, à notre sens, être le responsable LIPAD.

[12] Cf. art. 12 RGPD.

Conclusion

Le RGPD est un instrument d'application récente qui pose des problèmes notables de prévisibilité quant à son application concrète, spécialement extraterritoriale. Si certaines dispositions doivent à l'évidence être interprétées à la lumière d'analogies (on pense par exemple aux exceptions du champ d'application matériel), de nombreuses questions demeurent, notamment quant à la compatibilité de son application avec le respect de la souveraineté de la Confédération et des cantons. Ainsi, à titre d'exemple, il est à l'heure actuelle douteux que les sanctions financières éventuelles pourront être exécutées par les tribunaux suisses.

Il sied de relever qu'un processus de mise en conformité RGPD, s'il est jugé nécessaire, doit impérativement se construire autour de trois piliers : organisationnel, technique et juridique. On considérera ainsi avec circonspection les officines qui proposent une mise en conformité clefs en mains sans respect de cette démarche en triade.

Quoi qu'il en soit, il est important pour les collectivités publiques de s'assurer, dans tous les cas, que les traitements de données personnelles (et à plus forte raison les traitements de données personnelles sensibles) reposent sur une base légale, idéalement une base légale au sens formel, ou à tout le moins entrent dans le cadre de leur mission légale (mission d'intérêt public au sens du RGPD).

Par ailleurs, 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 collectivité ou entité 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). Cela étant, dans certains cas, il est parfois plus efficient et économique de soumettre l'entier des traitements de données aux principes du RGPD et de ne pas avoir des bases de données séparées soumises à des règles différentes.

Enfin, le RGPD ne doit pas être l'arbre qui cache la forêt : les collectivités et entités de droit public sont également, et au premier chef, soumises à la LIPAD et à son règlement d'application, le RIPAD. Dans un proche avenir, la loi fédérale sur la protection des données (LPD) révisée entrera en vigueur et les lois cantonales, dont la LIPAD, seront nécessairement amendées elles-aussi, avec comme intention affichée de reprendre la majorité des principes directeurs émanant du RGPD.

Ainsi, même si une collectivité ou une entité publique devait estimer ne pas être soumise au RGPD, cet examen devrait être l'occasion de s'assurer de la conformité des traitements de données personnelles avec le droit cantonal applicable.

Nicolas CAPT

Alexis CONSTANTACOPOULOS