L'impact du RGPD sur les institutions genevoises de droit public

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

RÉVISION DE LA LOI SUR LA PROTECTION DES DONNÉES (LPD)

CAPT
& WYSS
AVOCATS ASSOCIES
ATTORNEYS

RGPD

Champ d’application territorial du RGPD

Champ d'application territorial du RGPD

- En adoptant le RGPD (applicable dès le 25 mai 2018), le législateur a souhaité mieux protéger les données à caractère personnel des personnes physiques établies dans l'Union européenne (UE).

- Ainsi, l'une des grandes modifications introduites par le GDPR est le fait qu'il pourra s'appliquer, à certaines conditions, à des organisations qui ne sont pas établies dans l'UE.

- A cet égard, on parle d'application extraterritoriale du règlement.

Champ d'application territorial

Organisations visées par le RGPD

différents cas de figure

1. organisations établies dans l'UE
2. organisations non établies dans l'UE qui offrent des biens ou des services à des personnes dans l'UE
3. organisations non établies dans l'UE qui effectuent un suivi du comportement de personnes dans l'UE

Champ d'application territorial

1. Organisation établies dans l'UE

Établissement sur le territoire de l'UE

- Le RGPD s'applique, en premier lieu, aux organisations qui disposent d'*« établissements »* dans l'UE, dès lors que des données à caractère personnel sont traitées *« dans le cadre des activités »* de tels établissements (art. 3 al. 1).

Établissement sur le territoire de l'UE

- Concrètement, cela signifie que le RGPD s'applique à une entreprise basée en Suisse qui traite (en Suisse) des données à caractère personnel dans le cadre des activités de l'un de ses établissements sur le territoire de l'UE (filiale, succursale, représentant, etc.).

Établissement sur le territoire de l'UE

- S'agissant des institutions genevoises de droit public, elles ne disposent - en principe - pas d'établissements dans l'UE.

- Par conséquent, elle ne semblent *prima facie* pas soumises au RGPD à raison de ce critère d'application.

Champ d'application territorial

2. Organisation non établies dans l'UE qui offrent des biens ou des services à des personnes dans l'UE

Pas d'établissement dans l'UE

- Pour qu'une organisation soit soumise au RGPD en raison du fait qu'elle offre des biens ou des services à des personnes dans l'UE, il doit être apparent que celle-ci *« envisage »* que ses activités cibleront ces personnes.

- C'est l'*intention* de l'organisation de diriger son offre vers l'UE qui est déterminante.

Pas d'établissement dans l'UE

- Le terme *«offre»* fait essentiellement référence à une offre de nature commerciale, de sorte que cette notion ne devrait en principe pas englober les services fournis par des entités administratives ou des institutions de droit public suisses.

- On ne peut toutefois exclure sans nuances l'application extraterritoriale du RGPD à des entités publiques suisses qui fournissent des prestations sociales ou des services (gratuits ou onéreux) à destination de personnes dans l'UE (p.ex. lignes de transports publics qui desservent la France voisine, MOOC des Universités, etc.).

Suivi du comportement

3. organisations non établies dans l'UE qui effectuent un suivi du comportement de personnes dans l'UE

Suivi du comportement

- La notion de « *suivi du comportement* » désigne spécifiquement le fait de procéder à un suivi des Internautes aux fins de créer des profils de personnalité et/ou d'analyser/prédire leurs préférences et leurs comportements.

- Cette disposition vise typiquement les exploitants de moteurs de recherche et les entreprises actives dans le marketing en ligne.

- Par conséquent, dans la mesure où les entités administratives ou institutions genevoises de droit public n'effectuent – en principe - pas de suivi du comportement des Internautes, elles ne devraient pas non plus être soumises au RGPD pour cette raison. Des exceptions sont toutefois envisageables, p.ex. en cas d'analyse du comportement d'un Internaute basé dans l'UE dans le contexte d'un MOOC.

Champ d’application matériel du RGPD

Champ d’application matériel du RGPD

Champ d'application matériel du RGPD

- Le RGPD s'applique au traitement de « *données à caractère personnel* » (art. 2 par. 1).

- Cette notion désigne toute information relative à une personne physique (salarié, candidat, client, prospect, administré, contact, visiteur, etc.), identifiée ou qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification (numéro de téléphone, de carte bancaire, etc.), des données de localisation (adresse, coordonnées GPS, etc.), un identifiant en ligne (adresse IP, adresse MAC, etc.), ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Champ d'application matériel du RGPD

- La notion de *données à caractère personnel* est interprétée de manière très large, de sorte que toutes les données non rigoureusement anonymes doivent être considérées comme des données à caractère personnel.

Champ d'application matériel du RGPD

Licéité du traitement

Licéité du traitement

Données personnelles en général
(données «non sensibles»)

Licéité du traitement

- Un traitement est licite, notamment, si l'une des conditions suivantes au moins est remplie (art. 6 par. 1) :
  - la personne concernée y a consenti ;
  - le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ;
  - le traitement est nécessaire au respect d'une obligation légale ;
  - le traitement est justifié par un intérêt prépondérant du responsable de traitement ou d'un tiers.

Licéité du traitement

Données personnelles «sensibles»

Licéité du traitement

- Les conditions de licéité du traitement de catégories particulières de données, également appelées données personnelles «*sensibles*», sont plus restrictives.

- Il s'agit du traitement de données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que du traitement des données génétiques, des données biométriques 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.

Données de santé

- Parmi les données précitées, le RGPD définit notamment ce qu'il faut entendre par *«données concernant la santé»*:

  «les données concernant la santé sont les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne» (art. 4 par. 15).

Données de santé

- Cela comprend les informations suivantes:
  - celles collectées lors de l'inscription en vue de bénéficier de services de soins de santé ;
  - celles collectées lors de la prestation de service ;
  - celles obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques ou d'échantillons biologiques ;
  - celles concernant une maladie, un handicap, un risque de maladie ;
  - celles concernant les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical ;
  - un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique.

Conditions de licéité pour les données sensibles

- Le traitement de données sensibles est en principe interdit (art. 9 par. 1), à moins qu'il existe un motif justificatif. Sont notamment des motifs justificatifs :
  - la personne concernée a donné son consentement explicite ;
  - le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
  - le traitement est nécessaire pour des motifs d'intérêt public important (p.ex. santé publique; prévention d'épidémies; gestion des systèmes et des services de soins de santé ou de protection sociale).

Licéité du traitement

- En pratique, le recueil du consentement de la personne concernée est le moyen à la fois le plus simple et le plus sûr de s'assurer qu'un traitement de données à caractère personnel - sensibles ou non - est licite.

Licéité du traitement

Le recueil du consentement

Consentement

- Le RGPD a introduit de nouvelles exigences s'agissant des modalités relatives au recueil du consentement de la personne concernée (art. 7).

- Pour que le consentement soit valable, la personne concernée doit effectuer un acte positif et clair, qui exprime son accord de façon libre, spécifique, éclairée et univoque.

- Cet accord doit être donné pour chaque finalité de traitement, et doit pouvoir être retiré à tout moment, et ce aussi simplement qu'il a été donné.

Consentement

- Le consentement de la personne concernée n'est pas valable dans les cas suivants :
  - silence ou absence d'action de la personne concernée ;
  - cases pré-cochées ;
  - déséquilibre manifeste entre la personne concernée et le responsable de traitement ;
  - lien de subordination ;
  - contrats d'adhésion.

Nouveautés

Nouveaux droits
de la personne concernée

Droits de la personne concernée

- Le RGPD confère de nouveaux droits aux personnes concernées par un traitement de données à caractère personnel (art. 12), notamment :
  - droit à l'oubli/effacement (art. 17) ;
  - le droit à la limitation du traitement des données (art. 18 ; p.ex. en cas de contestation de la licéité du traitement) ;
  - le droit à la portabilité des données (art.20) ;
  - le droit d'opposition au profilage lié à la prospection (art. 21) ;
  - autres droits (art. 15, 16, 19, 22, 34).

Nouveautés

Nouvelles obligations du responsable du traitement

Nouvelles obligations

- Obligation d'informer la personne concernée par le traitement (art. 13, 14) :
  - du fondement juridique du traitement; cas échéant, de l'existence d'une prise de décision automatisé ou d'un profilage; de l'origine des données en cas de collecte indirecte; etc.
  - de ses droits, soit notamment de son droit à la portabilité des données, de son droit à la limitation des traitements (p.ex. en cas de contestation de la licéité), de son droit d'opposition au profilage, ou encore de son droit de déposer une plainte devant l'autorité de protection des données compétente.

Nouvelles obligations

- Obligation de désigner un *data protection officer* (DPO)
  - Le DPO est le point de contact entre l'organisation et les tiers (personnes concernées et autorités), ainsi que la personne en charge de veiller à la conformité de l'organisation.
  - Toutefois, le DPO n'est pas légalement responsable de la conformité de son organisation; son rôle consiste essentiellement à émettre des recommandations à destination des organes dirigeants.
  - En cas de contrôle ou de litige, l'organisation devra être en mesure de démontrer, documentation à l'appui, que le DPO remplit de manière satisfaisante les missions qui lui sont attribuées par le règlement.

Nouvelles obligations

- Obligation de désigner un représentant dans l'UE
  - Les organisations soumises au RGPD, et qui ne sont pas établies dans l'UE, ont l'obligation de nommer un représentant sur le territoire de l'UE.
  - Ce devoir tombe lorsque le traitement est seulement occasionnel, qu'il n'implique pas de catégories particulières de données personnelles et est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.
  - Le règlement manque de précision à cet égard.

Nouvelles obligations

- Obligations en cas de violation de données à caractère personnel (art. 33) :
  - le responsable de traitement doit en informer l'autorité de contrôle dans un délai de 72 heures après en avoir eu connaissance ;
  - lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les personnes concernées, le responsable de traitement doit également informer ces dernières dans les meilleurs délais (à moins que les données ne soient chiffrées et/ou pseudonymisées, ou que le risque ait été écarté).

Nouveautés

Relations entre le responsable de traitement et les sous-traitants

Responsable de traitement et sous-traitants

- Une organisation soumise au RGPD doit uniquement faire appel à des sous-traitants qui présentent des garanties suffisantes.

- Ainsi, par exemple, des clauses contractuelles qui prévoient que le sous-traitant est exclusivement responsable en cas de violation de données à caractère personnel ne sont pas opposables aux autorités de contrôle et aux personnes concernées.

Responsable de traitement et sous-traitants

- En revanche, les contrats avec les sous-traitants doivent être adaptés pour définir clairement les obligations respectives de chacun, notamment s'agissant de la sécurité, de l'obligation de rendre compte sur les mesures prises pour garantir les droits des personnes concernées, etc.

- Dans tous les cas, le responsable de traitement devra interpeller le sous-traitant à intervalles réguliers pour, par exemple, se ternir informé des mesures prises par ce dernier, pour savoir s'il a subi des attaques informatiques et quels en ont été les conséquences, etc.

Nouveautés

Privacy by design & privacy by default

Privacy by design, Privacy by default

- Privacy by design (art. 25 par. 1)
  - Mise en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées.
- Privacy by default (art. 25 par. 2)
  - Mise en œuvre des mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.

Nouveautés

Sanctions

Actions correctives

- Actions correctives (art. 58), notamment:
  - ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du règlement ;
  - imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement ;
  - ordonner la rectification ou l'effacement de données à caractère personnel ;
  - ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ;
  - autre.

Amendes administratives

- Amendes administratives (art. 83)

  Les violations du règlement peuvent faire l'objet d'amendes administratives pouvant s'élever jusqu'à **20'000'000 EUR** ou, pour les entreprises, jusqu'à **4 % du chiffre d'affaires annuel mondial total** de l'exercice précédent, le montant le plus élevé étant retenu.

Autres sanctions

- Le droit national d'un Etat membre peut fixer d'autres sanctions, notamment pour les violations qui ne font pas l'objet d'amendes administratives (art. 84).
- En sus de l'amende administrative, les possibilités d'actions en réparation du dommage ou du tort moral exercées par les personnes concernées sont réservées (art. 82).

Impact du RGPD

Nouveaux standards de protection des données

Nouveaux standards de protection des données

- Eu égard à son champ d'application très étendu, il fait peu de doutes que les principes et le niveau de protection des données personnelles établis par le RGPD vont constituer le nouveau standard pour les pays entourant l'UE.

- Le Conseil fédéral considère que la loi fédérale sur la protection des données (LPD) doit se rapprocher des standards établis par le RGPD, notamment aux fins de faciliter les relations économiques avec l'UE.

- Ainsi, le Conseil fédéral a récemment rendu public le projet de nouvelle LPD, lequel puise son inspiration dans la réglementation européenne, sans toutefois aller aussi loin.

Nouveaux standards de protection des données

- Même si la LPD ne s'applique pas aux administrations genevoises, le changement de paradigme a déjà des impacts sur les législations cantonales.

- Une révision du règlement d'application de la LIPAD (RIPAD) est entrée en vigueur le 15 février 2017.

- Le nouvel art. 13A adapte le cadre réglementaire à la pratique fédérale et européenne, tout en limitant la communication de données vers des Etats assurant un niveau de protection adéquat.

Nouveaux standards de protection des données

- Le nouvel art. 13A fusionne en une seule et même disposition les questions de sous-traitance et de communication transfrontière de données.

- Elle assure donc une meilleure sécurité des données personnelles en encadrant précisément leur sous-traitance, ce qui n'était pas le cas jusqu'à présent.

Nouveaux standards de protection des données

- Il faut relever encore que la protection des données est une garantie constitutionnelle, qui doit être respectée par les institutions cantonales.

- La Constitution fédérale suisse prévoit à son art. 13 que toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent.

- L'art. 21 de la Constitution genevoise a la même teneur.

Nouveaux standards de protection des données

- Les standards en matière de protection des données étant revus à la hausse, il n'est pas impossible que les lois cantonales relatives à la protection des données soient révisées, notamment afin de respecter le droit constitutionnel.

CONCLUSION

- A votre disposition pour prolonger l'échange:

CAPT & WYSS Avocats/Attorneys

Me Nicolas Capt

capt@cw-avocats.ch

022.347.77.11