Conformité au RGPD (GDPR)

Pascal Verniory
Christian Geffcken

Café république numérique – hepia

22 mai 2018

REPUBLIQUE ET CANTON DE GENEVE

POST TENEBRAS LUX

Sommaire

Sommaire

Définitions

1

RGPD :

Règlement général 2016/679 du parlement européen du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel.
En anglais: GDPR.
Début d'application : 25 mai 2018

2

Résident :

personne ayant son domicile principal d'un pays de l'UE, indépendamment de sa nationalité.

3

Personne identifiable (selon la CNIL) :

personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant (nom, numéro d'identification…), ou à un ou plusieurs éléments spécifiques propres à son identité (physique, physiologique…).

Sommaire

Champ d'application du RGPD

Deux conditions cumulatives (art. 3, § 2 RGPD) :

1. Traiter des données personnelles relatives à des résidents de l'UE

2. offrir à ces résidents des biens et services

OU

suivi du comportement ("monitoring") de ces résidents lorsque ce comportement a lieu au sein de l'UE

Le Conseil fédéral n'a pas tenu compte de cette condition

Champ d'application du RGPD

Deux conditions cumulatives (art. 3, § 2 RGPD) :

2

offrir à ces résidents des biens et services

OU

suivi du comportement = analyse des préférences ou du comportement de l'internaute, prédiction, prise de décisions le concernant (consid. 24 RGPD)

DIP: élèves enfants de frontaliers scolarisés en Suisse

Aéroport, TPG, Fondation des Parkings, HUG : services de transport et de santé

Télétravail depuis l'UE ?
Oui, mais pratique abolie à l'EGE

Gestion RH ? Non

Site Internet officiel de l'EGE ?
Oui, par Google analytics

Champ d'application du RGPD: EGE

Conclusion :

l'Etat de Genève semble marginalement soumis au RGPD

Dans le même sens, pour le PPDT, " **le RGPD devrait s'appliquer lorsqu'un résident européen, peu importe sa nationalité, sera directement visé par un traitement de données** "
(*Le RGPD et ses conséquences pour la Suisse*, p. 4)

Deux bémols s'imposent :

- Difficulté d'interprétation quant au champ d'application : le RGPD ne définit pas la notion de "prestation"
- Les autorités européennes n'ont toujours pas clarifié la situation comme demandé pourtant par diverses autorités suisses.

Champ d'application du RGPD: entreprises

Conclusion :

Toute entreprise

qui offre des prestations
(y compris par le biais d'un site Internet)
à des personnes ayant leur domicile principal dans l'UE
(quelle que soit leur nationalité)

ou

qui trace l'activité
(à l'aide de Google Analytics par exemple)
de personnes sur le territoire de l'UE
(y compris sur son site Internet suisse, lorsque le poste de l'utilisateur se trouve sur le territoire de l'UE)

est soumise au RGPD

Sommaire

Les nouveautés du RGPD

1. Application extraterritoriale

2. *Data Protection Officer* (DPO) obligatoire basé sur territoire européen
(sauf pour les administrations – art. 27, § 2, let. b RGPD)

3. Protection des données dès la conception et par défaut
(suppose une analyse d'impact en amont du projet)

Les prinipales nouveautés du RGPD

4

Champ étendu des données spéciales, les données "à haut risque":

- Données sensibles, analyses prédictives de comportement, données traitées à large échelle, données concernant des personnes vulnérables (employés, mineurs, malades), données pouvant entraîner une restriction des droits, données transférées hors UE
- Ex : le revenu fiscal devient une donnée spéciale, puisqu'il peut entraîner une restriction du droit à obtenir des subventions sociales….

5

Portabilité des données à transmettre à la personne concernée

(facilite le changement de fournisseur)

6

Droit à l'oubli

(gestion de vie des données, examen de pertinence et de sensibilité de la donnée, destruction effective en fin de vie – arrêt CJUE C-131/12 rendu en 2014 contre Google)

Les principales nouveautés du RGPD

7

Droit de regard sur les algorithmes de traitement

(pas seulement sur les données)

8

Droit de mettre fin en tout temps au consentement donné

9

Obligation de notifier en cas d'intrusion

- délai de **72 heures** *dès la connaissance* de l'intrusion pour informer les autorités européennes (consid. 85 ; art. 33 § 1 RGPD)
- Exception : s'il est peu probable que la violation engendre un risque pour les droits et libertés des personnes physiques concernées.

Les principales nouveautés du RGPD

Le montant des amendes explose :
4% du CA mondial ou 20 Millions €
(le plus élevé des deux – en comparaison, le projet LPD prévoit un maximum de CHF 250'000)

Bémols quant à l'applicabilité du RGPD à la Suisse :

- Il ne semble pas exister de procédure permettant à un Etat de l'UE de réclamer le paiement de cette pénalité à une administration suisse.
- L'autorité de contrôle pour les entreprises dont le siège est situé hors de l'UE ne semble pas désignée par le RGPD.

Sommaire

Les conséquences du RGPD

1. Le traitement des *données à haut risque* rend nécessaire la constitution d'un *Data Privacy Impact Assessment* (DPIA).

2. La cartographie (ou le recensement consolidé) des flux récurrents inter offices est vivement recommandée: elle est du reste requise par le projet de RAeL

3. **Obligation de rendre compte des mesures mises en place pour assurer la conformité avec le GDPR**

Les conséquences du RGPD

4

Le *Data Protection Officer* (DPO)

- Le poste reste obligatoire pour les entités traitant à grande échelle des données sensibles (art. 27, § 2, let. a RPDG *a contrario*)
- Il est *de facto* toujours incontournable pour assurer l'annonce des intrusions dans les délais (72 heures) et assurer la rédaction du DPIA

5

Chaque responsable de traitement doit annoncer les intrusions à la fois auprès des autorités suisses (PPDT) et européennes (mais lesquelles ?)

6

Les questions de protection des données revêtent un réel enjeu économique ; le rôle du DPO s'en trouve accru

Les conséquences du RGPD

7

Le droit suisse n'est plus à la pointe

- Cela peut contrarier ses ambitions de devenir le coffre-fort numérique de l'Europe

8

La Suisse pourrait perdre son statut de "pays offrant une protection suffisante"

- C'est le RGPD qui risque de servir de norme désormais
- A lui seul, le montant dérisoire des amendes prévues par la LPD pourrait entraîner la requalification de la Suisse
- Cela rendrait problématique l'échange de données avec les entreprises de l'UE

9

Même si le RGPD n'était pas applicable, le risque d'image est grand pour les entreprises suisses qui ne s'aligneraient pas sur cette norme.

Sommaire

Situation dans l'Union européenne

1

Convention 108, nouvelle version (amendement)
a été adoptée le 18 avril 2018 à Elseneur, Danemark

2

Directive européenne 2016/680 du 27 avril 2016 en vigueur dans l'UE
(protection des données personnelles applicable à la prévention et à la détection des infractions pénales)

3

RGPD (UE) 2016/679 en vigueur ;
appliqué dès le 25 mai 2018

Et la Suisse ?

1

Convention 108, nouvelle version (amendement)

(la Suisse est partie à la Convention 108)
a été adoptée le 18 avril 2018

2

La Directive européenne est un acte Schengen* :

elle s'applique à la Suisse, mais par voie de ratification
La Directive n'a pas encore été ratifiée par la Suisse

3

RGPD en vigueur ; appliqué dès le 25 mai 2018

Modification de la LPD en deux temps (11.01.2018) :

1/ adaptations aux acquis Schengen, notamment Directive 2016/680
2/ révision totale de la loi sur la protection des données pour l'adapter à l'évolution de la société suisse et au droit européen, notamment le RGPD.

* Accord entre la Confédération suisse, l'Union européenne et la Communauté européenne (RS 0.362.31); la Directive figure dans la liste des actes Schengen (Annexe B).

Mise en application à l'Etat

- Deux instruments indépendants existent pour déterminer les priorités
  - → CATFICH inventorie les fichiers de données personnelles
  - → La liste des applications prioritaires établit une hiérarchie entre les applications
- La combinaison des deux permet de dégager une priorité de traitement, si cela s'avère nécessaire
- Les HUG ont décidé d'appliquer une politique similaire

Sommaire

Les instruments de mise en conformité

1

Établir une feuille de route de mise en conformité

2

Établir un *Data Privacy Impact Assessment* (DPIA) et mettre en place le RGPD

- Intégrer dans la vie de validation des projets un examen de la protection de la confidentialité dès la conception. Cela semble être déjà le cas à l'EGE.
- Mise en place d'un PIA (tentative d'implémentation à l'EGE en 2014-2015 avec TICIA)

3

Centraliser les données

Centraliser = mise en place de référentiels, évite multiplication des données sans empêcher le fractionnement des bases de données !

Avantages de la centralisation :

- Plus grande transparence ;
- Contrôle accru des accès ;
- Réduit le risque de traitement accidentel

Les instruments de mise en conformité

4

Cartographier les flux de données personnelles

- Répertorie les flux récurrents de données, base légale justifiant le traitement, classement des données en termes de risques ;
- Les informations remontées par les offices peuvent être analysées par la direction, qui décide des règles à appliquer en matière de traitement.

5

Mettre en place un système de mise à jour systématique de la cartographie

- à intégrer au processus de conduite du changement ;
- réviser les directives EGE si nécessaire (en parallèle des évolutions LIPAD et LPD).

6

Installer un processus éprouvé de gestion des intrusions par des tiers

et assurer l'information aux personnes intéressées et aux autorités de contrôle dans les 72 heures.

Les instruments de mise en conformité

7

Rédiger un référentiel documentaire

- permet de montrer à première demande des autorités ce qui est mis en place pour assurer la conformité au GDPR (et à la LIPAD / à la LPD);
- Établir une circulaire opérationnelle
- Le PIA offrirait un cadre (*Privacy Maturity Model* – PMM) et un tel référentiel à l'occasion des évaluations qu'il nécessite.

8

Adapter, compléter les processus

tenir compte des exigences du GDPR en matière d'obligation de notifier :

- Processus de gestion de la continuité (intrusion = crise)
- Atelier communication en cas d'incident majeur et de crise informé de cette obligation d'aviser
- Prévoir les informations à inclure dans la communication aux autorités (cf. art. 33 § 3 RGPD).
- Déterminer l'autorité européenne de contrôle à qui notifier les intrusions!

Les instruments de mise en conformité

9

Adapter si nécessaire les contrats

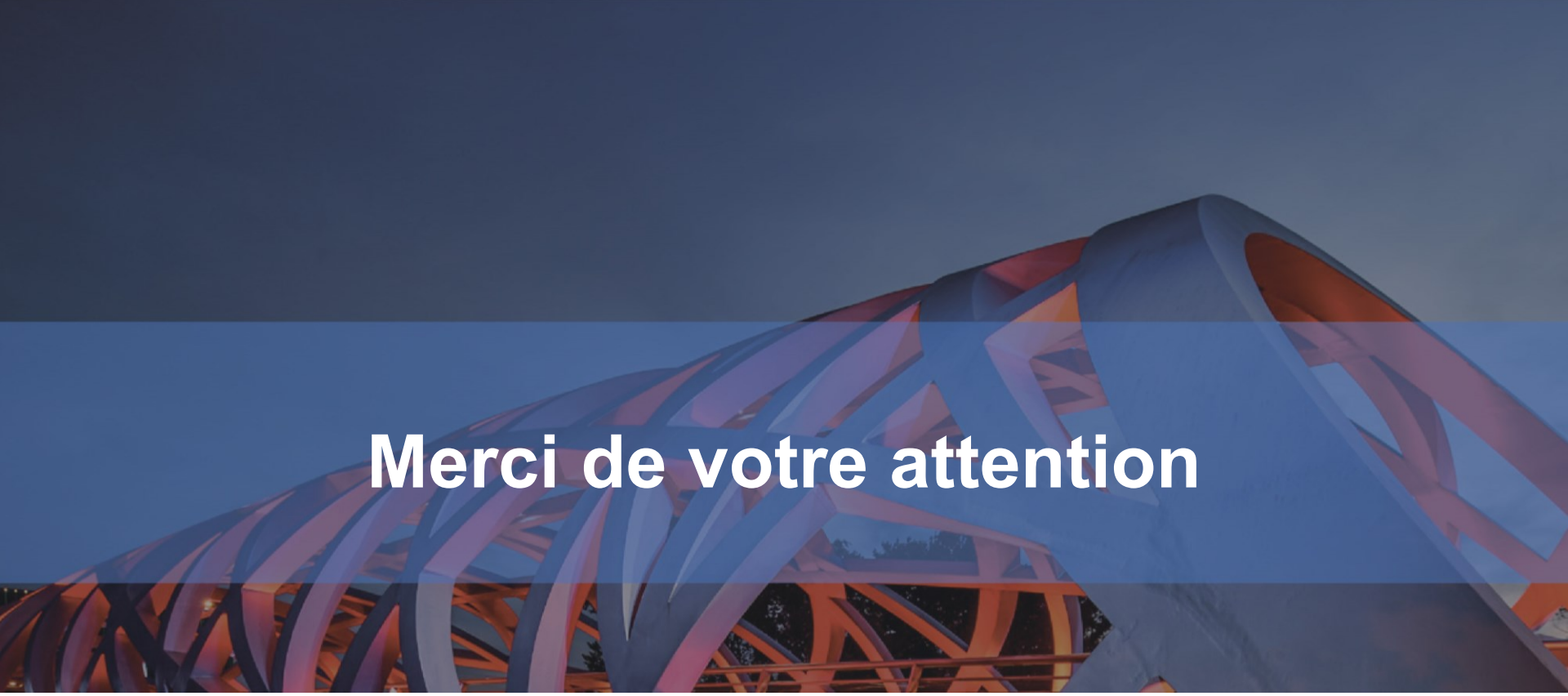
Tenir compte des exigences du GDPR et du RIPAD en matière de sous-traitance, notamment :

- S'assurer que son sous-traitant a son siège dans un pays offrant une protection suffisante ;
- Passer un contrat avec ses sous-traitants :
  - les engageant à respecter la loi applicable au responsable du traitement en matière de protection des données ;
  - interdisant la sous-traitance en cascade ou obligeant le sous-traitant
    - à n'avoir lui-même que des sous-traitants établis dans des pays offrant une protection suffisante, voire à communiquer leur raison sociale
    - et à imposer à ses propres sous-traitants le respect de la loi applicable au responsable du traitement ;
  - assurant une assistance (aide à la preuve) au responsable du traitement en cas de demande d'une personne concernée ou de litige, notamment judiciaire ;
  - assurant la possibilité d'auditer le site et les procédures des sous-traitants ;
  - prévoyant la remontée de l'information au responsable du traitement dans les 24 heures en cas d'intrusion, (pour pouvoir informer autorités et victimes dans les 72 heures)
- S'opposer à ce que les contrats prévoient l'applicabilité du RGPD !

Le RGPD pour les entreprises – campagnes

Actions de la DG DERI, de la FER et du CLUSIS :

- La DG DERI a co-organisé avec le CLUSIS et la FER deux conférences (février et avril 2018), suivies d'une séance de consultation où les entreprises ont pu bénéficier gratuitement de conseils d'experts RGPD au cours d'entretiens particuliers.
- Plus de 1'000 entreprises au total ont participé à ces conférences pour lesquelles plus de 30 experts du domaine ont été mobilisés.
- La DG DERI, le CLUSIS et la FER ont mis gratuitement en ligne un kit d'accompagnement RGPD qui comprend des outils de diagnostic et de eLearning pour les PME (https://www.ge.ch/document/module-formation-rgpd-pme; https://www.fer-ge.ch/web/fer-ge/-/kit-rgpd)
- La DG DERI a de plus contribué au volet RGPD de la campagne Cybersécurité lancée par le DSE au printemps 2018.
- Une liste d'entreprises qualifiées par le CLUSIS offrant des services d'accompagnement pour la mise en conformité des pratiques de protection des données avec le RGPD est publiée sur le site Swiss Made Security (https://www.swissmadesecurity.org/liste-des-entreprises-et-experts).



Merci de votre attention

Verniory Pascal — pascal.verniory@etat.ge.ch — 022 388 00 33

Christian Geffcken — christian.geffcken@etat.ge.ch — 022 388 03 37