



Veremes

 #FMEWT



FME
WORLD TOUR
2018

RGPD : contrainte ou bonne pratique ?

Dominique GAYTE – NoToS – dgayte@notos.fr

Qu'est-ce que le RGPD ?



Règlement Général sur la Protection des Données

GDPR: *General Data Protection Regulation*

Règlement européen applicable à partir du 25 mai 2018

Obligatoire

Pour tous États membres de l'Union Européenne

Est en train de devenir une législation de référence au niveau mondial

Le Congrès des États-Unis l'a cité à plusieurs reprises à propos de l'affaire *Cambridge Analytica* lors de l'audition du dirigeant de Facebook (Mark Zuckerberg)



*Les personnes physiques doivent
avoir le contrôle de leurs données
à caractère personnel !*

Le 25 mai 2018

Ce n'est pas la fin du projet

Au contraire, c'est là que tout commence !

Le RGPD doit s'envisager dans le temps

Il faut s'habituer à vivre avec et c'est justement l'objectif de ce règlement

Tout nouveau projet Informatique devra se faire dans le contexte du RGPD

Protection des Données à Caractère Personnel (DCP) dès la conception

Sécurisation des DCP par défaut

Tenue du registre des traitements

Protection des communications...



*La mise en conformité doit être
vue comme une chance et non
comme une charge!*

La mise en conformité est porteuse de valeurs

Prise de conscience de défauts dans l'organisation

C'est l'occasion de redéfinir certains processus

Conduit à une meilleure sécurisation du SI

Permet de mieux connaître son SI

Cartographie des DCP

Données structurées (bases de données)

Relativement maîtrisées

Données non structurées

Non maîtrisées !

Il existe des outils bien adaptés

Papier

Droits de la personne concernée

Durée de rétention

Problématique car généralement non gérée

Il faut mettre en place des processus pour l'acquisition (consentement explicite) et la suppression des DCP

Droit à l'oubli

Ne s'applique pas s'il y a une obligation légale

Pendant la durée de la contrainte

Portabilité

« On verra bien si on a une demande.... »

Données sensibles

Les données sensibles sont définies par le GDPR

Données génétiques, biométriques

Relatives à la santé, à la vie ou à l'orientation sexuelle

Révélant l'origine raciale ou ethnique, les opinions politiques les convictions religieuses ou philosophiques, l'appartenance syndicale

Par défaut, interdiction de les traiter !

Il ne faut pas les confondre avec celles qui font courir un risque important à la personne physique

Numéro de CB

Il faut leur prêter une attention particulière (sécurisation, cryptage, archivage...)

Le site web

Le site web doit être mis en conformité

Sauf s'il est purement statique

Les cookies

Souvent utilisés simplement pour tracer les actions sur le site (Google Analytics)

Il faut demander le consentement explicite de l'utilisateur s'il y a un lien possible avec la personne physique (adresse IP, par exemple !)

Attention dans ce cas, la durée de conservation de ces données est limitée à 13 mois

Suppression au-delà

Donc nouvelle demande de consentement en cas de nouvelle visite du site

Le site web (2)

Pour les données recueillies par des formulaires divers

- Information sur les finalités des traitements

- Durée de conservation de ces données

- Consentement explicite

Utiliser des pages Web indiquant la politique de protection des DCP

Privilégier HTTPS pour préserver la confidentialité

- Surtout s'il y a des DCP sur le site

 - Documents officiels, factures...



« Afin de démontrer qu'il respecte le présent règlement, le responsable du traitement ou le sous-traitant devrait tenir des **registres pour les activités de traitement** relevant de sa responsabilité. Chaque responsable du traitement et sous-traitant devrait être tenu de **coopérer avec l'autorité de contrôle** et de mettre ces **registres à la disposition** de celle-ci, sur demande, pour qu'ils servent au contrôle des opérations de traitement. »

Registre de traitements

Il n'y a plus de déclaration préalable mais un contrôle à posteriori

Sauf pour les traitements des données les plus sensibles

Données biométriques

Numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (NIR)

Le Registre de traitements est le (seul) moyen de prouver votre conformité !

Sous forme

Papier

Excel

Logiciels spécialisés

Registre de traitements (2)

Description des traitements et des occurrences

Les sous traitants

Sont ils conformes ?

Le DPO

Et tous documents prouvant vos actions de mise en conformité

Audit et mise en œuvre des préconisations

Formations

Analyses lors des phases de conceptions

Traçabilité

Indispensable afin

- De comprendre ce qui s'est passé en cas de violation

- Répondre aux besoins d'un contrôle

- D'anticiper

A permis de comprendre/constater certaines connexions

- Tentatives de pénétration à partir d'Internet

- Accès en production à des données de serveurs de test/développement

- Utilisation de « vieux » comptes

- Détail des requêtes et des connexions SQL ODBC/JDBC...



Conclusions

Envisagez la mise en conformité
comme une chance pas comme
une charge

Ne relâchez pas vos efforts après le
25 mai

Tenez un registre des traitements

Merci !



Dominique GAYTE - NoToS
dgayte@notos.fr

<https://www.power-gdpr.com>

