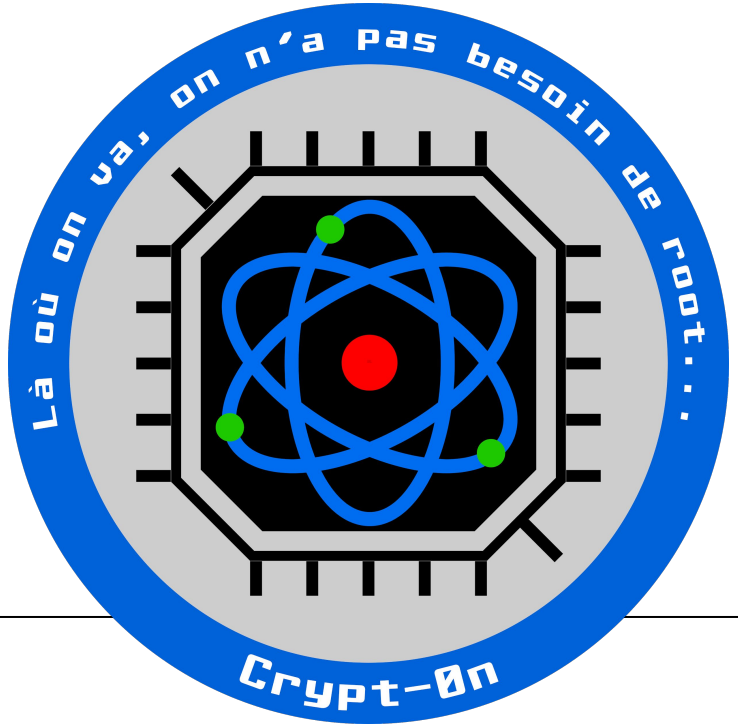

Le RGPD / GDPR

Le 16/05/2018

TLP:WHITE

https://www.crypt-0n.fr

Décharge de responsabilité

Ce document est mis à disposition par l'association Crypt-0n **uniquement à titre informatif et à des fins pédagogiques**.
Les informations qu'il contient sont publiées "en l'état" sans aucune sorte de garantie ni expresse ni implicite. Les informations contenues dans ce document peuvent être mises à jour sans préavis.
Crypt-0n décline toute responsabilité pour les éventuelles erreurs ou omissions figurant dans ce document.

GDPR

General **D**ata **P**rotection **R**egulation

RGPD

Règleement **G**énéral sur la **P**rotection des **D**onnées

Sommaire

1

Présentation

Le droit protégeant notre vie privée doit aujourd'hui être adapté à l'ère numérique

Qu’est-ce que la GDPR ?

Règlement européen qui redéfinit le régime de protection des données personnelles en Europe

- Il simplifie, harmonise et renforce la protection des données personnelles
- Il entre en vigueur le **25 mai 2018**
- Les entreprises contrevenantes s’exposent à de fortes amendes (jusqu’à **20 millions** d’euros ou, dans le cas d’une entreprise, **4% du chiffre d’affaires** annuel mondial)

Le règlement s’applique à toute personne ou entité :

- Qui met en œuvre un ou plusieurs traitements de données à caractère personnel ;
- En tant que responsable de traitement ou que sous-traitant;
- Dès lors que les traitements ont un lien avec l’Union européenne.

NB : Le règlement ne s’applique pas aux personnes physiques dans le cadre d’une activité strictement personnelle ou domestique.

Les données à caractère personnel

Est une donnée à caractère personnel toute information relative à une personne physique **identifiée ou identifiable de manière directe ou indirecte**.

➔ C’est donc un concept très large

Exemples :

- Numéro de sécurité sociale,
- Matricule salarié,
- Géolocalisation,
- Adresse IP,
- Adresse email,
- Photographie,
- Enregistrement vocal,
- Identification indirecte par référence à un identifiant en ligne
- Etc...

Les données dites sensibles

Les données dites « sensibles » sont des informations:

- concernant l'origine raciale ou ethnique, les opinions ou convictions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé (physique et mentale), les données génétiques, les données biométriques, la vie sexuelle ou l'orientation sexuelle…

Principe d'interdiction du traitement des données « sensibles » sauf exceptions :

- si le consentement explicite de la personne a été recueilli,
- ou que le traitement nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale …

Qu’est-ce qu’un traitement ?

Toute opération ou tout ensemble d’opérations **effectuées ou non** à l’aide de procédés automatisés et appliqués à des **données** ou des **ensembles de données** à caractère personnel.

Exemples :

- collecte,
- enregistrement,
- conservation,
- consultation,
- organisation,
- structuration,
- adaptation,
- extraction,
- modification,
- utilisation,
- transmission,
- mise à disposition,
- etc...

Le traitement doit être **licite** :

- **Base légale** (consentement, contrat, intérêts légitimes…);
- **Finalités** : limitées, spécifiques, déterminées, explicites et légitimes; obligation de ne pas traiter ultérieurement les données d’une manière incompatible avec les finalités initiales;
- **Transparence** envers la personne concernée sur l’utilisation des données et les droits de la personne.

2

Lorsque l’on traite des données personnelles

Il est temps de prendre ses responsabilités

Les nouveaux rôles

Le DPO *

- Le DPO (Data protection officer) doit s'assurer que son employeur ou son client respecte la législation lorsqu'il utilise les données à caractère personnel. En cas de manquement à la loi, il est tenu d'alerter sa direction dans les plus brefs délais.

Le responsable de traitement

- La personne physique ou morale, l’autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d’autres, détermine les finalités et les moyens du traitement

** Le DPO est obligatoire lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement de données à grande échelle.*

Les obligations

- Tenir un registre des traitements
- Privacy by design et security by default
- L’analyse d’impact pour les traitements critiques
- Le signalement des violations de données à l’autorité de contrôle sous 24 heures (CNIL pour la France)
- Le signalement des violations de données aux personnes concernées
- La garantie de nouveaux droits des personnes concernées et le renforcement du droit à l’effacement et à l’oubli.

Les sous traitants

Le responsable de traitement ne peut pas se décharger de ses responsabilités si celui-ci fait uniquement appel à des sous-traitants.

Il doit s’assurer que le sous-traitant :

- Utilise uniquement les données nécessaires à ce traitement
- S'engage à ce que le personnel respecte la confidentialité
- Prend toutes les mesures requises pour la protection des données
- Selon le choix du responsable du traitement, supprime ou renvoie au responsable du traitement toutes les données à caractère personnel
- Met à la disposition toutes les informations nécessaires pour apporter la preuve du respect des obligations
- Supprime les données à la fin de la prestation

3

Les personnes concernées

Reprendre ses données en main

Leurs droits

Consentement

- Il doit être libre, clairement distinct, éclairé (compréhensible et simple), univoque (acte positif) et documenté…
- Protection spécifique des enfants de moins de 16 ou 13 ans.

Transparence

- Sur l’utilisation des données
- Sur les droits des personnes (retrait du consentement, minimisation des données, droit à l’oubli …)

Merci !

Des questions ?

Pour me contacter :

- @jlequen
- jlequen@crypt-0n.fr