Lien Entreprises Durables

RGPD

RGPD : Lien Entreprises Durable

Auteur :
Christophe Nouhau

Entité :
proximit

Destinataires :
LED et adhérents

Version :
V 2.2

Date :
06 Juin 2019

RGPD : petits rappels

GDPR ou RGPD : C'est quoi ?

CNIL : Loi n°78-17 du 6 janvier 78 relative à l'informatique, aux fichiers et aux libertés

RGPD : Nouveaux droits pour les PC : 25 mai 2018

Le RGPD (Règlement Général sur la Protection des Données) :

ou (GDPR) General Data Protection Regulation en Anglais.
C'est le texte de référence Européen en matière de protection des données personnelles qui vise à protéger le droit à la vie privée

La réforme de la protection des données poursuit trois objectifs :

1.Renforcer les droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;

2.Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants) ;

3.Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées.

RGPD : Qui est concerné ?

Tous les professionnels :

- Ceux de l'internet bien sûr
- Ceux du secteur marchand
- Ceux du secteur public
- Ceux du secteur **associatif**

Tout en respectant le droit des états membres

Le RGPD s'applique quand :

- Une organisation traite des données personnelles
- Un résident de l'UE est directement visé par un traitement de données

Responsabilité de la structure « responsable de traitements » ET de ses sous-traitants

Données à caractère personnel (DCP) c'est quoi ?

D C P

Données permettant l'identification

D C P

- Données se rapportant à une personne physique identifiée ou identifiable

Directement

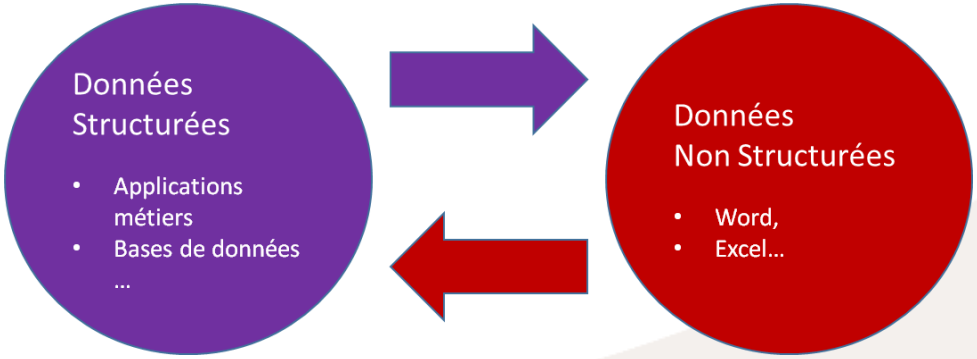
- Nom, Prénom, etc.
- Images (caméras de surveillance)
- Photos
- Voix, conversations,
- Données biométriques

Indirectement

- Coordonnées géographiques (géolocalisation)
- Numéro de comptes (carte de paiement)
- Numéro de Sécu (NIR)
- Matricules d'employés
- Logins et autres identifiants numériques
- @IP

Informations se rapportant à une personne identifiée

- Fichier client / Prospects / Fournisseurs…
- Fichier paie / RH
- Badgeuse / Pointeuses
- Contrôle d'accès
- Données de production
- Dossiers santé
- Information financières, fiscales
- Informations sur les médias sociaux
- Données issues d'objects connectés
- Parcours scolaire
- Dossier d'assurance de crédit
- Informations volontairement rendues publiques
- Condamnations
- Géolocalisation
- ETC… ETC… ETC…



Obligations qui incombent aux organismes

6 Principes :

- *Licéité, Loyauté, transparence*
- *Limitation des finalités*
- *Minimisation des données*
- *Exactitude des données*
- *Limitation de la conservation*
- *Intégrité et confidentialité*

➔ *Le* responsable du traitement est en mesure de **démontrer** le respect de ces principes

➔ *Grande échelle = DPD + PIA (analyse d'impact)*

DPO
Data Protection Officer

pia analyse d'impact sur la protection des données privacy impact assessment

Les droits de la PC :

- *Droit d'accès*
- *Droit de rectification*
- *Droit à l'effacement (« oubli »)*
- *Limitation du traitement*
- *Droit d'opposition*
- *Droit à la portabililté*
- *DIA (décision Individuelle Automatisée / hors données médicales dans certaines conditions)*

➔ *La PC (personne concernée) doit être informée*

Principe de « Licéité, Loyauté, transparence »

Licéité, Loyauté (au moins une condition remplie de l'Article 6 du règlement) :

- Ce qui est traité doit correspondre à ce qui a été décrit à la personne concernée. Cette information claire lui permet par exemple de donner un consentement valide ou d'exercer ses droits.
  - ✓ La PC a consenti au traitement de ses DCP pour une ou plusieurs finalités spécifiques *(il faut le prouver !)*
  - ✓ Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable de traitement est soumis
  - ✓ Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la PC ou d'une autre personne physique
  - ✓ 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 de traitement

Transparence (l'information relative au prélèvement des DCP):

- Les personnes concernées sont en droit d'obtenir les informations nécessaires pour assurer un traitement loyal (notamment les informations sur les finalités du traitement). Il convient de bien identifier le responsable du traitement.

Autres principes

Limitation des finalités :

- Les données personnelles ne peuvent être obtenues que pour des « finalités déterminées, explicites et légitimes » (article 5.1.b). Les données ne peuvent être utilisées qu'aux fins spécifiques ayant justifié la collecte et/ou traitement en premier lieu.

Exactitude des données :

- Les données doivent être « exactes et, si nécessaire, tenues à jour » (article 5.1.d). Il incombe aux détenteurs de données, de créer des processus de rectification et suppression dans les bases de données des données des sujets. Ce qui rejoint le principe du droit d'accès et ses composantes.

Limitation de la conservation des données :

- Le RGPD dispose que les données personnelles soient « 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 » (article 5.1.e). En d'autres mots, les données qui ne sont plus requises doivent être supprimées.

Risques en cas de non-conformité ?

Le règlement RGPD prévoit deux niveaux de sanctions, pour les entreprises, en cas de non-respect :
Des amendes administratives pourront s'appliquer pour un montant allant de 10 à 20 000 000 €,
ou bien 2 à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent .

L'hôpital de Barreiro a écopé d'une amende de 400 000 euros en raison de sa politique d'accès aux bases de données des patients.

La CNIL avait prévenu dès avril 2018. Le 21 janvier 2019, elle passe à l'acte. Sanction de 50 millions d'euros à Google.

RGPD : Synthèse

DPO
Data Protection Officer

pia
analyse d'impact sur la protection des données
privacy impact assessment

Personne concernée (PC)

DCP

Responsable Traitement

Sous - Traitant

Personne physique ou morale, autorité publique, service ou autre organisme qui traite de DCP pour le compte du responsable de traitement sur instruction documentée

Traitement

CID
- Confidentialité
- Intégrité
- Disponibilité

+

6 principes

Et

Droit des PC

Démarches à engager pour assurer la conformité selon la CNIL :

Conformité :

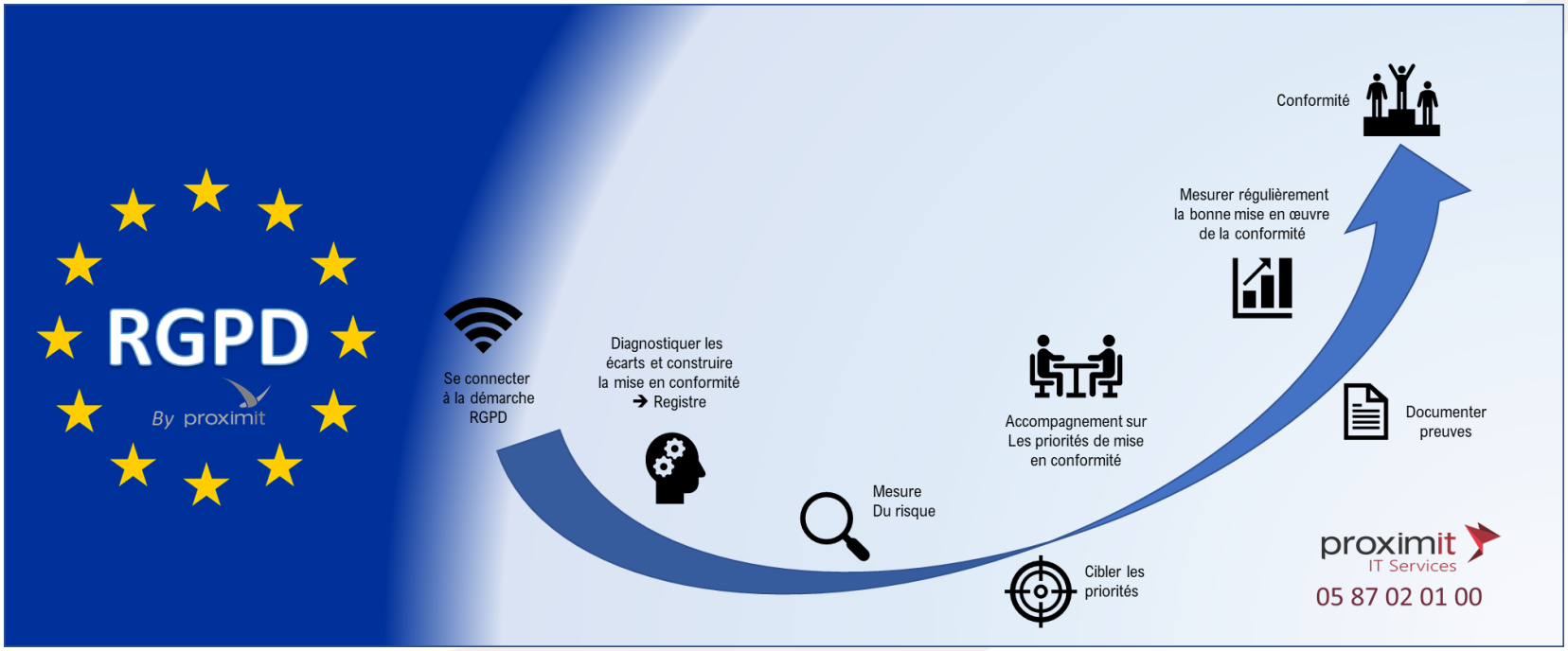
- Méthodes en 6 étapes

Démarches à engager pour assurer la conformité

Les mesures à adopter pour respecter le RGPD

source : CNIL – La CNIL propose une démarche en 6 étapes

1 – Désigner un DPD ou un pilote identifié (interne ou externe) / Une personne disposant de relais internes et externes chargée de s'assurer de la mise en conformité au règlement européen;
2 - Cartographier vos traitements de données personnelles ;
3 - Priorisez les actions à mener au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées ;
4 - Gérer les risques, en menant une étude d'impact sur la protection des données pour chacun de vos traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées ;
5 - Organiser les processus internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement ;
6 - Documenter la conformité au règlement et la tenir à jour.



Lien Entreprises Durables

Merci de votre attention