R G P D

Renforcer les données à caractères personnels

15 OCTOBRE 2018

CESI DE PAU

Table des matières

Le RGPD est l'acronyme de Règlement Général sur la protection des données.

Le RGPD est un texte de loi européen adopté le 27 avril 2016 et qui est entrée en vigueur le 25 mai 2018. Il a pour but de responsabiliser les organismes traitant des données personnelles et de renforcer les droits des personnes dont les données sont traitées.

Il est directement applicable et a force obligatoire depuis cette date.

Le RGPD est né de la volonté européenne de créer un cadre juridique unifié, afin de faire face aux enjeux majeurs que représente le traitement des données personnelles.

1. Quel public concerné ?

Le RGPD s'applique à tout organisme, quelle que soit sa taille, traitant des données personnelles pour son compte ou non, dès lors qu'il est établi sur un territoire de l'union européenne ou que son activité cible directement des résidents européens.

2. Les 3 enjeux de la RGPD

1. **Créer la confiance**. Entre collecteur et les données personnelles collectées
2. **Sécuriser les données**. Tout responsable de traitement des données, qui gère et collecte des données doit sécuriser ses données.
3. **Responsabiliser** les acteurs et sous-traitant pour leurs faire prendre conscience que tout collecteurs de données est responsable des données qu'il collecte

3. Qu'est-ce qu'une donnée personnelle ?

La notion de donnée personnelle est extrêmement large puisqu'elle est définie par la CNIL comme toute *information se rapportant à une personne physique identifiée ou identifiable.*

L'identification peut se faire de manière directe (nom, prénom, adresse postale) ou de manière indirecte (éléments physiques, identifiant, adresse IP, numéro).

Par ailleurs, sont également considérées comme personnelles les données qui, par le recoupement de plusieurs informations, (date de naissance, sexe, ville, diplôme, etc.) ou l'utilisation de divers moyens techniques, permettent d'identifier une personne.

4. Quelles obligations pour les entreprises ?

Selon l'article 5.1 du RGPD, les données personnelles doivent être :

- Traitées de manière licite, loyale et transparente ;
- Collectées à des fins déterminée, explicite et légitimes ;
- Adéquates, pertinentes et limitées ;
- Exactes et tenues à jour ;
- Conservées pendant une durée raisonnable ;
- Traitées de façon à garantir leur protection.

Les 6 étapes pour y arriver :

1. **Désigner** un pilote (DPO)
2. **Cartographier** les traitements des données personnelles
3. **Prioriser** les actions à mener
4. **Gérer** les risques
5. **Organiser** les processus internes
6. **Documenter** la conformité

La mise en œuvre du RGPD se base sur un fort désir de responsabilisation des différentes structures et acteurs. Les contrôles, organisations formelles et bureaucratiques sont ainsi supprimées pour laisser place au principe d' "accountability". Les entreprises s'engagent ainsi à documenter l'action qu'elles mettent en œuvre afin de pouvoir en analyser l'impact et ajuster leurs décisions en continu. La CNIL recommande ainsi

plusieurs actions à mettre en œuvre afin de s'inscrire pleinement dans la bonne marche du règlement ; afin de procéder à une autoévaluation, pour mettre en place les mesures nécessaires, il est dans un premier temps primordial de désigner un pilote.

4.1. Désigner un pilote :

La désignation d'un pilote signifie la désignation d'un Délégué à la Protection des Données (DPO).

4.2. De l'obligation de nomination.

Le Délégué à la Protection des Données (en anglais DPO : Data Protection Officer) est la personne chargée de mettre en œuvre l'harmonisation de la législation au niveau européen au sein de sa structure d'appartenance.

Sa nomination peut être obligatoire en fonction du rôle et du statut de son organisation ; celle-ci est ainsi obligatoire dans le cadre des organisations de statut public, à l'exception des fonction juridiques et juridictionnelles.

Dans le cas des structures privées, elle est obligatoire en fonction de la nature de leur activité de base. Si celle-ci conduit, à grande échelle, à un traitement de données sensibles, et dans le cas du suivi permanent et régulier de personnes.

4.3. Prérogatives.

Le règlement européen du RGPD stipule qu'il est le garant indépendant, et en toute probité, des questions relatives à la protection des données personnelles et de la vie privée des usagers. Il donne par ailleurs des exemples concrets quant aux prérogatives découlant de la fiche de poste :

* Une mission d'information et de conseil à l'intention des collaborateurs de la structure

* Une mission de formation et de réalisation d'audits

* Une mission de contrôle et de veille permanente quant aux règles et politiques édictées par l'organisme concernant la protection des données personnelles

* Un engagement de coopération avec l'organisme de contrôle

* S'assurer d'être un point de contact pertinent avec celui-ci

Le DPO ne peut cependant être tenu juridiquement responsable des manquements éventuels vis-à-vis du règlement ; ce rôle incombe directement à la personne morale.

4.4. Cartographier les traitements des données personnelles

La cartographie de l'état actuel du traitement des données au sein de la structure permet de se positionner par rapport au nouveau règlement européen, il s'agit ici de réaliser un inventaire documenté complet de la situation.

Fiche de registre	ref-ooo
Description du traitement	
Nom / sigle	
N° / REF	ref-ooo
Date de création	
Mise à jour	

Acteurs	Nom	Adresse	CP	Ville	Pays	Tel
Responsable du traitement						
Délégué à la protection des données						
Représentant						
Responsable(s) conjoint(s)						

Finalité(s) du traitement effectué	
Finalité principale	
Sous-finalité 1	
Sous-finalité 2	
Sous-finalité 3	
Sous-finalité 4	
Sous-finalité 5	

Mesures de sécurité	
Mesures de sécurité techniques	
Mesures de sécurité organisationnelles	

Catégories de données personnelles concernées	Description	Délai d'effacement
Etat civil, identité, données d'identification, images...		
Vie personnelle (habitudes de vie, situation familiale, etc.)		
Informations d'ordre économique et financier (revenus, situation financière,		
Données de connexion (adress IP, logs, etc.)		
Données de localisation (déplacements, données GPS, GSM, etc.)		

Données sensibles	Description	Délai d'effacement
Données révèlant l'origine raciale ou ethnique		
Données révèlant les opinions politiques		
Données révèlant les convictions religieuses ou philosophiques		
Données révèlant l'appartenance syndicale		
Données génétiques		
Données biométriques aux fins d'identifier une personne physique de manière unique		
Données concernant la santé		
Données concernant la vie sexuelle ou l'orientation sexuelle		
Données relatives à des condamnations pénales ou infractions		
Numéro d'identification national unique (NIR pour la France)		

Catégories de personnes concernées	Description
Catégorie de personnes 1	
Catégorie de personnes 2	

Destinataires	Description	Type de destinataire	
Destinataire 1			
Destinataire 2			

4.5. Prioriser les actions

En fonction des résultats obtenus précédemment, il est ici possible pour la structure de relever les points de discordance avec la règlementation. Il est nécessaire de prioriser les actions de conformisation à mener en fonction du risque pesant sur les données personnelles traitées.

4.6. Gérer les risques

RISQUES	IMPACTS SUR LES PERSONNES	PRINCIPALES SOURCES DE RISQUES	PRINCIPALES MENACES	MESURES EXISTANTES OU PRÉVUES	GRAVITÉ	VRAISEMBLANCE
Accès illégitime à des données						
Modification non désirée de données						
Disparition de données						

Dans le cadre où, au cours des études, des risques critiques pour la protection des données auraient été identifiées, il convient de mener une Etude d'Impact sur la Protection des Données.

4.7. Organiser les processus internes

Le DPO a la charge, une fois les études précédentes menées, d'organiser ses services, procédures (traitement des données) afin qu'elles puissent respecter, sur le long terme, la règlementation du RGPD et la protection des données personnelles qui en découlent.

Le meilleur moyen de parvenir à cette finalité est de prendre en compte ce prérequis dès la conception même de ces procédures et organisations. Une grande part de formation des effectifs internes est également requise afin que chaque collaborateur puisse participer à leur bon déroulement.

4.8. Documenter la conformité

Comme évoqué précédemment, une des parties prépondérantes de l'inscription dans la conformité au RGPD consiste à documenter chacune de ses actions. La démarche d'"accountability" prônée par l'harmonisation nécessite ainsi la constitution d'un dossier documentaire complet prouvant le respect absolu des règles qui en découlent. La bureaucratie est remplacée par le principe d'autoévaluation.

Ce dossier contiendra ainsi la documentation complète sur les traitements de données personnelles (PIA, etc …), les informations relatives aux personnes ainsi que les documents contractuels définissant les responsabilités et les rôles des différents acteurs (liens avec les sous-traitants, etc …)

5. Droits des personnes dont les données sont traitées.

5.1. Renforcement et réaffirmation de droits et principes existants.

Le RGPD reprend et renforce un certain nombre de droits déjà garantis par les lois nationales. Non limités aux usagers de services, ces droits, puis principes s'appliquent également par exemple aux salariés des structures concernées.

Ces personnes bénéficient de nombreux droits :

* **Le droit d'accès** : il s'agit de garantir aux personnes le droit d'accéder aux informations les concernant, ou qui s'y rapportent.

* **Le droit de rectification** : permettre aux personnes le droit d'apporter des modifications aux informations les concernant.

* **Le droit d'opposition** : les personnes peuvent s'opposer au traitement de leurs données personnelles, soit au moment de la collecte, soit après, à condition d'avoir un motif légitime. Néanmoins, ce droit ne peut être garanti lorsque ce traitement découle d'une obligation légale de l'entreprise.

* **Le droit à l'effacement** : garantir aux personnes le droit de supprimer les éventuelles informations obsolètes, erronées ou incomplètes les concernant. Les informations récoltées illégalement sont également concernées.

La loi garanti l'application gratuite de ces demandes dans le cadre où celles-ci seraient justifiées.

5.2. Mise en avant de principes fondamentaux.

En complément de ces droits, certains principes préétablis sont conservés par le RGPD, cela concerne :

*** Le principe de transparence** : dans un premier temps, les organismes récoltant les données personnelles s'engagent à faire preuve de la plus grande honnêteté concernant leur utilisation. Ils s'engagent à respecter la finalité de l'utilisation des données qui a été annoncée à l'utilisateur. Par ailleurs, cette information doit être délivrée de manière claire et concise.

*** Le principe de limitation** : Les utilisateurs, personnes physiques ou morales, peuvent s'opposer temporairement au traitement de leurs données, cela peut être apparenté à une procédure de mise en conservation de ces informations pour plusieurs raisons précises et justifiées telles que la contestation d'informations erronées, l'opposition à l'effacement, la conservation des données pour défendre ses intérêts en justice, etc …

5.3. Garantir de nouveaux droits.

Par sa promulgation, le RGPD garanti de nouveaux droits aux citoyens européens ; sont ainsi concernés :

*** Le droit à l'oubli** : Sorte de consécration du droit au référencement, ce droit vient soumettre les moteurs de recherche aux requêtes d'effacement des données personnelles des utilisateurs le souhaitant.

*** Le droit à la portabilité** : l'analogie peut être faite avec la portabilité que proposent les FAI et autres opérateurs téléphoniques. Toute personne se voit garantir le droit de récupérer auprès d'un responsable de traitement les informations le concernant pour les transférer vers une autre entité. Cette démarche doit être fondée sur une acceptation contractuelle et être automatisée.

En cas de violation des données personnelles, l'entreprise doit informer la CNIL, dans les 72h et la personne concernée, dans les meilleurs délais.

Une telle violation s'analyse selon la CNIL comme celle « entraînant de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ».

6. La CNIL : acteur central de la protection des données en France.

Autorité de contrôle pour la protection des données à caractère personnel en France, la Commission nationale de l'informatique et des libertés (CNIL) est chargée de veiller à la bonne application du RGPD en France.

Elle est également chargée d'accompagner les entités publiques et privées engagées dans leur démarche de mise en conformité avec le règlement.

6.1. Responsabilité directe.

Le responsable du traitement et/ou le sous-traitant sont directement responsables devant les personnes concernées du respect des dispositions du Règlement.

Ainsi, en cas de violation, toute personne peut au choix introduire une réclamation devant l'autorité de contrôle compétente ou saisir directement une juridiction pour solliciter la réparation du dommage qu'elle a subi du fait de cette violation.

La violation du Règlement par le responsable du traitement ou le sous-traitant peut également donner lieu à une action de groupe.

6.2. Sanctions administratives.

Le responsable du traitement et/ou le sous-traitant peut faire l'objet de sanctions administratives importantes en cas de non-respect du RGPD allant du simple avertissement au retrait de la certification délivrée.

Les autorités de protection peuvent notamment mettre en demeure le responsable du traitement ou le sous-traitant, limiter temporairement ou définitivement un traitement, suspendre les flux de données, ordonner de satisfaire aux demandes d'exercice des droits des personnes, ordonner la rectification, la limitation ou l'effacement des données.

Des amendes administratives peuvent également être prononcées et représentent, selon la catégorie de l'infraction 2% à 4% du chiffre d'affaires annuel mondial pour les entreprises et 10 à 20 millions d'euros pour les autres organismes.

7. CONCLUSION.

Le RGPD est entré en application il y a 4 mois, et la CNIL qui veille à la bonne application du RGPD en profite pour tirer un premier bilan de cette mesure. Les entreprises ont su s'adapter progressivement.

De nombreux organismes ont désigné un DPO, plus de 600 notifications de violations de données enregistrées et plus de 3millions de visites sur le site de la CNIL.

Les citoyens seraient plus attentifs aux données personnelles et traces qu'ils laissent sur Internet.

Les affaires Cambridge Analytica dont a été victime Facebook, ont mis l'accent sur cette problématique.

De nouveaux outils de régulations et actions vont être développés tels que des codes de conduite, des référentiels relatifs à la gestion des clients et prospects.