www.lacitedesentreprises.com

Le BIM.

Numéro 173
Mars/Avril 2022

La revue qui décrypte l'actualité juridique

FOCUS SUR LES PRINCIPES ESSENTIELS DU RÈGLEMENT EUROPÉEN DE PROTECTION DES DONNÉES (RGPD)

Adopté en 2016 et entré en vigueur le 25 mai 2018, le RGPD est le règlement européen constituant le texte de référence en matière de protection des données personnelles au sein de l'Union européenne.

L'objectif est de « redonner aux citoyens le contrôle de leurs données personnelles, tout en simplifiant l'environnement réglementaire des organismes ».

Cité des Entreprises.

L'essentiel

1. En préambule, les bases du RGPD

Rappelons les grands principes régissant la mise en œuvre du RGPD.

1.1 Application du RGPD

Tout d'abord, les règles de protection des données ne protègent pas les personnes morales mais **uniquement les personnes physiques.**

La **donnée à caractère personnel** est une information relative à une personne physique identifiée ou identifiable, directement ou indirectement par référence à un numéro d'identification ou à plusieurs éléments qui lui sont propres. Par exemple, une donnée directement identifiable peut être le nom, une donnée indirectement identifiable peut notamment se faire par référence à un identifiant comme le numéro de sécurité sociale (NIR) ou être identifiée par croisement, par exemple le sexe, l'adresse et la date de naissance.

Le **traitement** est une opération portant sur des données personnelles, comme la collecte, l'enregistrement, la conservation, la communication, la destruction…

Il faut distinguer les données personnelles des **données sensibles**, qui peuvent concerner les opinions philosophiques, les origines raciales et ethniques, les données génétiques, les convictions religieuses, les données relatives à la vie sexuelle ou à l'orientation sexuelle, les appartenances syndicales, les données biométriques, les opinions politiques et les informations de santé. Conformément à l'article 9 du RGPD, le principe est l'interdiction de la collecte des données sensibles, sauf circonstances exceptionnelles.

Le RGPD concerne tout organisme public ou privé établi sur le territoire de l'Union européenne ou qui effectue des traitements visant des citoyens résidents de l'Union européenne.

1.2 Les acteurs du traitement

La **personne concernée** est toute personne dont les données, permettant de l'identifier ou de la rendre identifiable, font l'objet d'un traitement. Par exemple, il s'agit des salariés de l'entreprise.

Le **responsable du traitement** est une personne ou un organisme qui détermine la finalité et les moyens du traitement de données. Il s'agit de la personne à l'initiative du traitement. Par exemple, il peut s'agir de l'employeur.

Le **sous-traitant**, lui, traite des données pour le compte du responsable de traitement. Par exemple, c'est le cas d'un cabinet RH.

Le **destinataire** est la personne habilitée à obtenir communication de données en raison de ses fonctions. Par exemple, ce sont les personnes habilitées du domaine RH pour la gestion administrative du personnel.

Un **tiers autorisé** peut accéder à certaines données contenues dans des fichiers parce qu'une loi l'y autorise expressément. Par exemple, cela peut être un huissier de justice, la police ou encore l'administration fiscale.

Le **délégué à la protection des données**, encore appelé DPO, est une personne dont la désignation est obligatoire si l'activité principale consiste à suivre le comportement des personnes à grande échelle. Il peut être interne ou externe. En dehors des cas obligatoires, sa désignation reste conseillée.

Son rôle est de contrôler le respect du RGPD, informer et conseiller, coopérer avec la CNIL et conseiller sur la réalisation d'études d'impact.

La **CNIL, commission nationale de l'informatique et des libertés** est une autorité administrative indépendante, créée en 1978 et chargée de veiller au respect de la réglementation sur la protection des données personnelles. Elle a pour mission d'informer et de protéger les droits ainsi que d'accompagner la conformité et de conseiller. Par ailleurs, elle a pour mission de contrôler et de sanctionner.

2. L'impact du RGPD pour l'employeur

2.1 Le traitement

D'abord, il s'agit de recenser les traitements de données des salariés. Il s'agit d'élaborer le **registre des traitements**. Son intérêt est double, c'est un outil de recensement des traitements mais aussi un outil d'analyse et de suivi. En outre, il permet d'apporter la preuve des démarches entreprises en vue de la conformité au RGPD et en cas de contrôle, il est le premier élément que la CNIL demandera de produire. Les informations à porter au registre sont :

- nom et coordonnées du responsable de traitement ;
- finalité du traitement ;
- catégorie de personnes concernées ;
- catégorie de données personnelles traitées ;
- catégorie de destinataires auxquels les données sont communiquées ;
- durée de conservation ;
- description générale des mesures de sécurité techniques/ organisationnelles.

Le **traitement** mis en œuvre doit répondre à un objectif précis et être justifié au regard des missions et des activités de l'organisme. Par exemple, il peut s'agir du recrutement, de la gestion administrative du personnel, de la gestion des rémunérations et l'accomplissement des formalités administratives y afférant, la mise à disposition du personnel d'outils professionnels, le suivi des carrières et des mobilités.

2.2 L'obligation d'information

Il existe également une obligation d'information. En effet, « le responsable du traitement fournit à la personne concernée, au moment où les données en question sont obtenues, toutes les informations suivantes» :

- identité et coordonnées du responsable de traitement ;
- coordonnées du DPO;
- finalités du traitement et base juridique du traitement ;
- destinataires ou catégories de destinataires des données ;
- durée de conservation ;
- droits de la personne concernée ;
- faculté d'introduire une réclamation auprès de la CNIL.

L'obligation d'information suppose le respect de plusieurs principes qui sont détaillés ci-dessous.

Le premier principe consiste **dans la transparence et la loyauté**. Le RGPD impose une information complète, compréhensible et transparente des personnes concernées, dès la collecte des données personnelles les concernant. Par exemple, pour les salariés, cela peut être les contrats de travail ou la charte informatique. Plus généralement, il peut s'agir des affichages (panneau vidéosurveillance à l'entrée du parking) ou des mentions du site web.

Les données personnelles sont collectées pour une finalité déterminée, elles ne doivent pas être utilisées pour une autre finalité. Par exemple, pour la géolocalisation des véhicules des salariés, la finalité est d'optimiser les déplacements ou pour la vidéosurveillance, la finalité est de protéger les personnes et les biens. Les données collectées ne peuvent pas avoir pour finalité de surveiller ou de contrôler les salariés en permanence, il s'agirait d'un traitement illicite.

Le deuxième principe se compose **de la minimisation et de la proportionnalité**. Un traitement de données personnelles repose nécessairement sur la poursuite d'un objectif précis. Par exemple, lorsque le recruteur doit procéder à la vérification du casier judiciaire d'un candidat, il lui est strictement interdit dans conserver une copie ou encore de recopier à la main les éléments qu'il comporte. Il doit se contenter d'indiquer dans le fichier qu'il en a bien pris connaissance. Le principe est le même pour la conservation du permis de conduire ou de la carte d'identité du salarié.

Le troisième principe repose sur **la confidentialité et la sécurité**. Le RGPD met à la charge du responsable de traitement une obligation de sécurisation des données. Il est nécessaire d'être vigilant sur ce point, la grande majorité des décisions de sanctions récentes de la CNIL concernent des manquements à l'obligation de sécurité.

Le quatrième principe est constitué **de la conservation des données limitée dans le temps**. Les données personnelles traitées ne peuvent être conservées de façon indéfinie dans des fichiers dématérialisés ou sur support papier. Une durée de conservation de ces données doit être déterminée en fonction de l'objectif qui a conduit à leur collecte. Une fois cet objectif atteint, les données doivent être supprimées ou anonymisées.

Le cinquième principe est la **documentation de la conformité**. L'ensemble des actions entreprises par le responsable de traitement en vue de sa mise en conformité doit être consigné par écrit. Le RGPD lui impose également la formalisation de certaines procédures, par exemple, pour répondre à une demande d'exercice de droit ou traiter une violation de données.

3. Les droits des salariés

En matière de RGPD on peut compter six droits pour les personnes, dont les quatre suivants existaient auparavant :

- le droit d'accès visé à l'article 15 : il permet de connaitre quelles sont les données détenues sur vous par un organisme ;
- le droit à la rectification visé à l'article 16 : il permet de corriger des données inexactes vous concernant ;
- le droit à l'effacement visé à l'article 17 : il s'agit du droit de demander l'effacement de vos données (droit à l'oubli);
- le droit d'opposition visé à l'article 21 : il vous permet de vous opposer à ce que vos données soient utilisées par un organisme pour un objectif précis.

De nouveaux droits ont été créés, il s'agit du droit à la limitation visé à l'article 18 et le droit à la portabilité visé à l'article 20.

Rappelons que la réponse doit être faite dans un délai de 30 jours maximum, sauf en cas de circonstances exceptionnelles où le délai peut être porté à 2 mois.

4. La violation des données personnelles et les sanctions

L'article 33 du RGPD impose au responsable de traitement de notifier les violations de données personnelles, à l'autorité de contrôle **dans les 72 heures suivant la découverte de la violation**, à moins que la violation ne soit pas susceptible d'engendrer un risque pour les droits et libertés de personnes physiques.

En vertu de l'article 4 du RGPD, une violation de données à caractère personnel est un incident de sécurité qui a pour conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles. Il peut s'agir d'une perte de confidentialité, une perte de disponibilité ou encore une perte d'intégrité. Les sources d'une violation de données peuvent être multiples : un piratage informatique, un envoi d'un mail au mauvais destinataire, une perte de l'ordinateur ou du téléphone professionnel. Face une violation de données, il est nécessaire d'avertir le DPO ou le référent sans délai.

En cas de non-respect du RGPD, il existe **différentes sanctions administratives**. Elles peuvent consister dans :

- un avertissement,
- une mise en demeure,
- une injonction de mise en conformité sous astreinte,
- une demande de réponse à l'exercice de droit sous astreinte,
- une suspension des flux de données

Par ailleurs, il peut s'agir de **sanctions financières qui peuvent aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial**, le montant le plus élevé est retenu.

Cité des Entreprises.

Parole d'expert

Interview
réalisée le 17 mars 2022

Pierre MILLE

De formation juridique – Master 2 Droit de la Propriété Industrielle – j'ai occupé la fonction de juriste généraliste au sein du Barreau de Lille pendant 8 ans. Je me suis spécialisé dans la protection des données personnelles pour être DPO de l'Ordre des avocats au Barreau de Lille et de la Caisse Autonome des Règlements Pécuniaires des Avocats de Lille (CARPAL).

J'ai rejoint Extern DPO en mai 2019 afin de me consacrer exclusivement à la protection des données personnelles en tant que consultant externe. La même année, j'ai obtenu la certification AFNOR de Délégué à la Protection des Données

Pouvez-vous en préambule vous présenter ainsi que votre structure ?

Pierre MILLE, juriste de formation, est consultant en protection des données au sein de la société EXTERN DPO, qui a été créée en 2018 et située à Wambrechies. Composée de quatre collaborateurs permanents, elle accompagne une quarantaine d'organismes situés pour la plupart d'entre eux, dans les Hauts-de-France. Il s'agit de structures de toutes tailles et de tous secteurs comme par exemple, les services de santé au travail ou encore des services sociaux-médicaux.

Quels conseils donneriez-vous pour entamer la démarche de mise en conformité avec la réglementation du RGPD ?

La première démarche à opérer pour bien mettre en œuvre la protection des données est de recenser l'ensemble des données personnelles collectées, en établissant une cartographie de l'ensemble des données traitées au sein de l'entreprise. L'entreprise doit établir un registre des traitements, faire le tri dans les données collectées, renforcer son obligation d'information et de transparence à l'égard des personnes dont elle traite les données et sécuriser les données de l'entreprise.

Quels sont les points de vigilance en cas de recours à la sous-traitance ?

Les entreprises ont recours à de nombreux sous-traitants. Elles doivent être vigilantes et s'assurer que le prestataire, avec lequel elles contractent, respecte la réglementation relative au RGPD, en vérifiant dans les contrats commerciaux que figurent bien les mentions y afférant.

Si la réglementation relative à la protection des données personnelles n'est pas respectée, la CNIL peut prononcer des sanctions administratives, comme des avertissements ou des mises en demeure, mais aussi des sanctions financières qui selon la gravité du manquement, peuvent aller jusqu'à 4% du chiffre d'affaires annuel mondial.

La loi du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure, vient doter la Commission Nationale de l'Informatique et des Libertés (CNIL,) d'une nouvelle procédure simplifiée pour le prononcé de sanctions financières d'un montant limité, applicable aux seules affaires simples et de faible gravité. Cette nouvelle loi ouvre la possibilité au Président de la CNIL, statuant seul, ou à l'un des membres de la CNIL qu'il aura désigné à cet effet, de prononcer des sanctions administratives limitées dans leurs montants :

- une injonction de mettre en conformité le traitement avec les obligations résultant du RGPD et de la loi dite "Informatique et Libertés", ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie d'une astreinte dont le montant ne peut excéder 100€ par jour de retard à compter d'une date fixée par le Président de la CNIL ; et
- une amende administrative ne pouvant excéder 20 000 euros.

Cité des Entreprises.

Il faut savoir que tout salarié ou tout client peut adresser des plaintes à la CNIL. On peut s'interroger sur un accroissement des contrôles opérés par la CNIL avec le développement de procédures simplifiées.

Quels sont les principaux manquements en cas de non-conformité au RGPD et quelles sont les sanctions appliquées ?

Avec la COVID-19, on a constaté une limitation de l'activité de la CNIL et par conséquent une diminution du nombre de sanctions. Actuellement, la tendance s'inverse, avec un fort accroissement de sanctions prononcées. Elles visent toutes les entreprises qu'elle que soit leur taille, et quel que soit leur secteur d'activité. Les manquements sont de différente nature. 40 à 50% des manquements sont liés à un manque de sécurisation des données. C'est pourquoi, il est impératif de veiller au bon cloisonnement des données personnelles dans les entreprises, afin que les personnes non habilitées ne puissent y accéder. D'autres sanctions prononcées par la CNIL concernent le non-respect des durées de conservation des données ou encore l'envoi de prospection commerciale (mail, SMS) sans avoir demandé le consentement du destinataire.

Soulignons la nécessité de respecter les finalités du traitement. Par exemple, dans le cadre de la vidéosurveillance, les caméras doivent être installées sur le lieu de travail de façon à protéger la sécurité des personnes et des biens, mais, il est interdit de disposer des caméras de manière à contrôler l'activité des salariés, sauf dans certaines hypothèses particulières, par exemple si un employé manipule de l'argent ou travaille dans un entrepôt stockant des biens de valeur.

Il est nécessaire de rappeler que les personnes doivent être informées sur les données qui peuvent être traitées, en respectant le principe de proportionnalité.

Quels sont les obligations en matière de RGPD et de droit à l'image ?

Les notions de RGPD et de droit à l'image sont liées. On ne peut pas utiliser la photographie d'un salarié sans son accord, qu'il s'agisse de la communication interne ou externe de l'entreprise. Il est nécessaire que le salarié soit informé et que son accord soit donné, tout en lui ayant précisé le périmètre précis de la diffusion de son image, notamment la nature du support, la durée d'utilisation, la finalité... A de rares exceptions près, il est difficile de rendre obligatoire la diffusion de la photographie d'un salarié.

Combien d'entreprises ne sont pas à jour des formalités liées au RGPD en France ?

Fin 2018, on comptait 15% d'entreprises se déclarant en conformité avec le RGPD. Aujourd'hui, on estime à 50% le nombre d'entreprises qui se disent en conformité avec le RGPD. Nous sommes beaucoup sollicités par les entreprises qui n'ont pas encore initié la démarche.

Au regard de l'actualité, que préconisez-vous à nos adhérents en matière de sécurité informatique et de lutte contre la cybercriminalité ?

Il est important d'auditer le système informatique de la société, notamment en se faisant aider par des entreprises externes. Des règles de base peuvent être appliquées en entreprise notamment, la gestion des mots de passe qui doivent être robustes et renouvelés régulièrement, pratiquer des sauvegardes des données, disposer d'antivirus à jour... Il est nécessaire de sensibiliser les collaborateurs aux risques numériques. Dans l'actualité, nous avons vu des problèmes dans les hôpitaux qui n'étaient pas suffisamment protégés et qui ont été la cible de cyber hacker. Avec la guerre en Ukraine, les entreprises qui hébergent des données en Russie, s'interrogent sur le maintien de l'hébergement des données sur ce territoire.

La Cité des Entreprises - MEDEF Lille Métropole
Campus Entreprises et Cités
40, Rue Eugène Jacquet - 59708 Marcq-en-Baroeul Cedex
Tél. : 03 20 99 45 35
lacitedesentreprises@citeonline.org

Directeur de la publication :
Yann ORPIN

Rédacteur en chef :
Arnaud COUSIN

Rédactrice :
Astrid FEUILLET

Responsable de la Communication :
Marion SIGIER

Le service juridique de La Cité des Entreprises reste à votre disposition pour répondre aux questions des adhérents.

Vous pouvez retrouver ce BIM et les précédents sur le site internet :
www.lacitedesentreprises.com