AUDIT RGPD: Se mettre en conformité

Comprendre ce qui change

MEPERY
EXPERTISE TECHNIQUE ET JURIDIQUE

Cabinet Juridique & Technique
25 Route de Seilh
31700 CORNEBARRIEU
09 88 39 26 77
contact@cabinet-mepery.fr
cabinet-mepery.fr

EDITO

Le règlement n° 2016/679, dit Règlement Général sur la Protection des Données (RGPD), est un règlement de l'Union Européenne qui constitue un des textes de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données personnelles pour les individus au sein de l'Union Européenne.

Le RGPD est applicable à tous types de structures et il les oblige à une meilleure gestion ainsi qu'à une meilleure protection des données personnelles qu'ils collectent.

Le RGPD est entré en vigueur, dans l'ensemble des pays de l'Union Européenne, le 25 mai 2018. La loi sur la protection des données n°2018-493 du 20 juin 2018 et son décret d'application n°2018-687 du 1er août 2018 viennent adapter le RGPD à notre droit national.

L'entrée en vigueur du RGPD force les entreprises à se mettre en conformité avec ses dispositions.

Ainsi, un audit de conformité RGPD aura pour but de permettre aux entreprises de vérifier dans quelles mesures elles le respectent, notamment, sur les points suivants:

- Fonctionnement du système d'information et traitement des données personnelles
- Documentation mise en place par l'entreprise (registre, charte, mentions légales...)
- La sécurité et la fiabilité du système d'information.

Il est désormais temps – pour ne pas dire urgent- pour une entreprise, qui traite d'une façon ou d'une autre des données personnelles, de mettre ses traitements de données en conformité avec la législation, et ce, afin de ne pas risquer des sanctions en cas de contrôle par la CNIL.

Ce fascicule a pour but de vous permettre d'y voir plus clair sur les nouveautés apportées par le RGPD afin de mieux vous y retrouver dans votre mise en conformité.

Bonne lecture!

L'équipe MEPERY

Comprendre la réforme sur les données personnelles: les points essentiels

- Le nouveau règlement sur les données personnelles
- L' « *Accountability* »
- Les nouvelles obligations des responsables de traitements et sous-traitants
- Les nouveaux outils de conformité
- Le renforcement des droits des personnes
- Le renforcement du contrôle et des sanctions prononcées par la CNIL.

Le nouveau Règlement sur les Données Personnelles

Le RGPD

Le Règlement Général sur la Protection des Données ou RGPD est un règlement européen du 27 avril 2016 et entré en vigueur le 25 mai 2018.

Il a pour but d'encadrer les règles sur la protection des données personnelles. Il fixe de nouveaux droits pour les personnes dont les données sont collectées et il impose de nouvelles obligations aux entreprises qui collectent ces données.

Les personnes concernées par le RGPD sont: toute organisation publique ou privée qui **traite des données personnelles pour son compte ou non**, si:

- Elle est établie sur le territoire de l'UE
- Son activité cible directement les résidents de l'UE
- Elle est établie hors UE mais qu'elle a des relations commerciales avec des clients européens.

Les acteurs du RGPD

- Le Responsable de traitement:

Il est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement, détermine les finalités et les moyens de traitement » (art.4.7 RGPD). En d'autres termes, il s'agit de la personne qui décide de la mise en œuvre du traitement et qui en est donc responsable.

- Le sous-traitant:

Il est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement » (art. 4.8 RGPD). En d'autres termes, il s'agit de la personne qui procède aux opérations de traitement pour le nom et pour le compte du responsable de traitement. Le sous-traitant n'est pas le destinataire des données!

- Le Délégué à la Protection des Données ou *Data Protection Officer* (DPO):

Le DPO succède au Correspondant Informatique et Liberté (CIL). Il est un acteur majeur de la conformité au RGPD.

- Le destinataire:

Le destinataire est « la personne physique ou morale, l'autorité publique, le service ou tout organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers » (art. 4.9 RGPD). C'est donc la personne qui recevra, de manière habituelle, communication des données.

Il faut que le destinataire ait au préalable été autorisé par le responsable du traitement à prendre connaissance des données.

- Les autorités de contrôle:

Le RGPD permet, désormais, à un groupe de société établi dans plusieurs Etats membres de désigner une autorité de contrôle dite « autorité chef de file ». Cette dernière sera compétente pour contrôler certain traitement. Elle est définie à l'article 56.1 du RGPD.

Il y a également les « autorités de contrôles concernées » qui sont les autorités de contrôle locales sur le territoire du dommage. En France, il s'agit de la CNIL.

- Les personnes concernées:

Les personnes concernées sont les personnes dont les données sont traitées: clients, prospects, salariés, etc.

- Le Contrôleur Européen de la Protection des Données:

C'est l'organe de contrôle des institutions européennes en la matière. Le Contrôleur Européen est compétent pour contrôler les pratiques des institutions en matière de protection des données.

- Le Groupe de l'article 29 ou G29:

Créé par l'article 29 de la Directive 95/46/CE, il est un organe consultatif et indépendant regroupant l'ensemble des autorités de contrôles, le Contrôleur Européen et la Commission européenne. Il émet des avis et recommandations. Avec l'entrée en vigueur du RGPD, il est devenu le Comité Européen de la Protection des Donnés (CEPD).

Les principe fondamentaux du RGPD

Les principes fondamentaux sont énoncés à l'article 6 du RGPD.

- Le principe de limitation des finalités:

Lorsque les données sont collectées, elles le sont pour des finalités déterminées, explicites et légitimes. La finalité correspond à l'objectif poursuivi par le responsable du traitement.

La ou les finalités doivent être :

- **Déterminées** préalablement
- « **explicites** », c'est-à-dire communiquées à la personne concernée
- « **légitime** » par rapport à l'activité de l'organisme mettant en œuvre le traitement

- Le principe de licéité, de loyauté et de transparence:

En application de l'article 6 du RGPD, les données doivent être traitées de manière licite, loyale et transparente. Pour être licite, la personne concernée doit avoir consenti au traitement de ses données ou que celui-ci soit nécessaire. L'exigence de loyauté et de transparence fait référence à l'information des personnes concernées.

- Le principe de proportionnalité:

Il recouvre deux exigences:

- La minimisation des données qui est prévue par l'article 51-c du RGPD et qui suppose que les données qui font l'objet du traitement doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ». En d'autres termes, il n'est pas permis de collecter des données superflues.
- La limitation dans le temps de la durée de conservation des données, qui est prévue par l'article 51-e du RGPD, suppose que les données doivent être conservées pendant une durée qui n'excèdent pas la durée nécessaire à la finalité du traitement.

- L'exactitude des données:

Les données doivent être exactes et tenues à jour. Pour se faire, le responsable de traitement doit prendre toutes les mesures raisonnables pour que les données inexactes soient traitées, effacées ou rectifiées dans les meilleurs délais.

- Les principes d'intégrité et de confidentialité:

Il s'agit de principes fondamentaux. Le traitement des données doit garantir une sécurité appropriée. Pour se faire, le responsable de traitement devra prendre des mesures techniques et organisationnelles adéquates.

L' « *Accountability* »

Le principe

Le RGPD met en place le principe d' « *Accountability* » soit **le principe de responsabilité**. C'est une nouveauté majeure du RGPD. Avec l' « *Accountability* » on passe d'un régime de formalité préalable à un régime de mise en responsabilité des responsables de traitement et des sous-traitants.

Ce principe est énoncé à **l'article 24 du RGPD**. Il met à la charge du responsable de traitement l'obligation de « *s'assurer et d'être en mesure de démontrer que le traitement est effectué conformément* » au RGPD.

Il fait peser sur le responsable de traitement l'obligation d'adopter des règles internes destinées à garantir le respect du RGPD.

Par ailleurs, **l'article 74 du RGPD** précise que le responsable de traitement va devoir, non seulement **démontrer la conformité du traitement au RGPD** mais il devra, également, **démontrer l'efficacité des mesures prises**.

Privacy by design et *Privacy by default*

Ce sont des principes qui consistent à intégrer la protection des données dès la conception des produits et services et par défaut.

Ces principes sont édictés par **l'article 25 du RGPD**. Ainsi, en application de cet article, le responsable de traitement doit, dès la conception du produit ou du service (*by design*), prendre en compte les principes de protection des données personnelles afin qu'ils soient directement inclus dans le produit ou dans le service dès sa naissance.

De même, il doit mettre en œuvre par défaut (*by default*) les principes les plus protecteurs en matière de données à caractère personnel.

Les codes de conduites et les certifications sont des moyens qui permettent de démontrer le niveau d'*accountability* de l'entreprise.

Le Registre de Traitement

La mise en place d'un registre de traitement a pour but de recenser et d'analyser les traitements de données et de disposer d'une vue d'ensemble de ce que fait l'entreprise avec les données personnelles. Il est prévu par **l'article 30 du RGPD**.

Tous les organismes, publics ou privés, et quelle que soit leur taille doivent tenir un registre de traitement.

Il doit refléter la réalité des traitements des données personnelles et doit permettre d'identifier avec précision:

- Les parties qui interviennent dans le traitement;
- Les catégories de données traitées;
- À quoi elles servent, qui y a accès et à qui elles sont communiquées;
- Combien de temps elles sont conservées;
- Comment elle sont sécurisées.

La CNIL recommande de tenir 2 registres:

- Le registre du responsable de traitement qui doit recenser l'ensemble des traitements mis en œuvre par l'organisme.
- Le registre du sous-traitant qui doit recenser toutes les catégories d'activités de traitement effectuées pour le compte des clients.

Les nouvelles obligations des responsables de traitement et des sous-traitants

Les obligations du responsable de traitement

Le responsable de traitement a pour mission de sécuriser et de garantir les traitements de données dont il a la charge. Pour se faire, il est soumis à un certain nombre d'obligation.

L'obligation d'information

Le responsable de traitement a l'obligation d'informer les personnes concernées du traitement de leurs données personnelles. Il doit porter à la connaissance de la personne concernée des informations précises sur ce traitement. L'information doit se faire au moment de la collecte des données.

L'article 32 de Loi Informatique et Liberté et **l'article 13 du RGPD** précise ses informations:

- Identité du responsable de traitement;
- Finalité du traitement;
- Durée;
- Coordonnées du DPO;
- Droits dont disposent les personnes concernées;
- Etc..

L'obligation de notification en cas de violation

En cas de violation des données, le responsable de traitement est soumis à l'obligation d'informer, dans les meilleurs délais, la personne concernée.

Il devra également en informer la CNIL dans un délai de 72 heures.

L'obligation d'assurer la sécurité et la confidentialité des données

Le responsable de traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer la sécurité et la confidentialité des données récoltées.

Par exemple:

- Pseudonymisation et chiffrement des données
- Moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes de traitements
- Procédures visant à tester, analyser, évaluer de façon régulière l'efficacité des mesures prises.

Cette liste n'est évidemment pas exhaustive et il peut exister d'autres mesures à mettre en œuvre, notamment en fonction du traitement et de la catégorie de données.

Les obligations du sous-traitant

Le RGPD a posé un principe de responsabilisation de ***tous*** les acteurs impliqués dans le traitement des données personnelles, dont le sous-traitant fait partie.

Le sous-traitant est soumis à plusieurs obligations:

- Le RGPD impose la **contractualisation des relations entre le sous-traitant et le responsable de traitement**. En d'autres termes, la relation entre eux doit être formalisée par un contrat.
- L'obligation de tenir un registre de traitement.
- La coopération avec les autorités de contrôles.
- L'obligation de respecter le *Privacy by design* et le *Privacy by default*.
- L'obligation de **garantir la sécurité et la confidentialité des données**. A la fin de sa collaboration avec le responsable de traitement, le sous-traitant devra supprimer toutes les données récoltées et les transmettre au responsable de traitement.
- L'obligation de **notification des violations des données** au responsable de traitement, dans les meilleurs délais.
- L'obligation de conseiller le responsable de traitement, notamment au regard de la légalité des instructions que lui aura donné ce dernier ou en aidant le responsable de traitement dans les demandes d'exercice des droits des personnes concernées.

Les nouveaux outils de conformité

L'Analyse d'Impact sur la Protection des données

Il sera nécessaire pour l'organisme de faire une AIPD si le traitement des données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Il devra faire apparaître les caractéristiques du traitement, les risques et les mesures adoptées.

Un risque élevé est un scénario décrivant:

- Un évènement redouté telle qu'une atteinte à la confidentialité ou à l'intégrité des données;
- Toutes les menaces permettant que le risque survienne.

Le risque élevé est estimé en terme de gravité et de vraisemblance.

Pour que le traitement soit de nature à engendrer un risque élevé, il doit présenter 2 des critères suivants:

- Évaluation/scoring/profilage;
- Décision automatique avec effet légal ou similaire;
- Surveillance systématique;
- Collecte de données sensibles ou hautement personnelles;
- Collecte de données personnelles à large échelle;
- Croisement de données;
- Personnes vulnérables;
- Usage innovant;
- Exclusion du bénéfice d'un droit ou d'un contrat.

Une AIPD peut concerner un seul traitement ou un ensemble de traitements similaires. L'AIPD doit être menée avant la mise en œuvre du traitement et doit être mise à jour tout au long du traitement.

Le Délégué à la Protection des Données Personnelles

Avec le RGPD, le DPO devient un acteur majeur de la protection des données personnelles.

➢ **La nomination d'un DPO est-elle obligatoire?**

La nomination d'un DPO est obligatoire pour les entreprises employant plus de 250 salariés.

Elle est facultative pour les autres mais reste recommandée.

➢ **Qui peut être DPO?**

Le DPO est « *désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions* » (art. 37 RGPD)

Ainsi, le DPO peut être:

- Membre du personnel;
- Personne extérieure rattachée au responsable de traitement par un contrat de service;
- Le Correspondant Information et Liberté.

➢ **Quelles sont les missions du DPO?**

- Informer et conseiller le chef d'entreprise;
- Contrôler la bonne application du RGPD;
- Être le contact entre l'entreprise et la CNIL;
- Être le point de contact avec toutes les personnes concernées;
- Être consulté pour toutes les décisions concernant les données personnelles;
- Être alerté et consulté lorsqu'une violation de données est constatée;
- Réaliser des AIPD, déterminer les actions correctives et vérifier l'exécution.

Le renforcement des droits des personnes

Les droits renforcées

Le RGPD consolide les droits existants.

- **Le droit à l'information:**

Il est le premier droit des personnes concernées et sûrement l'un des plus importants puisqu'il conditionne l'exercice de tous les autres droits. En effet, si la personne ignore que ses données personnelles sont traitées, elle ne pourra pas demander l'accès à ses informations, leur rectification ou encore leur effacement.

La liste des informations à communiquer aux personnes concernées est fixée par **l'article 13 du RGPD**. Ainsi, on peut citer comme information à communiquer: l'identité du responsable de traitement, la finalité du traitement, le destinataire des données, la durée de conservation des données, les droits des personnes concernées, etc.

- **Le droit d'accès, de rectification et d'opposition:**

Le **droit d'accès** suppose que la personne concernée par le traitement de ses données a le droit d'interroger le responsable de traitement afin de savoir s'il traite ses données et d'en obtenir une copie.

Le **droit de rectification** est un droit qui permet à la personne d'obtenir la modification de ses données dans le cas où ces dernières seraient incomplètes ou inexactes. Le responsable de traitement se trouve dans l'obligation de rectifier les données lorsqu'il est saisie d'une demande.

Le **droit d'opposition** permet à la personne de s'opposer à ce que ses données soient traitées, si elle justifie d'un motif légitime. Ce droit s'utilise souvent lorsque la personne n'a pas donné son consentement, qui doit être libre, spécifique et éclairé.

Les nouveaux droits

Le RGPD a créé de nouveaux droits permettant de renforcer la protection des personnes dont les données personnelles sont collectées.

- **Le droit à l'oubli:**

Ce droit permet à la personne dont les données sont collectées d'obtenir l'effacement de ces dernières dès lors:

- Qu'elles ne sont plus nécessaire au regard de la finalité pour laquelle elles ont été collectées;
- Qu'elle doivent être effacées pour respecter une obligation légale;
- Qu'elles ont fait l'objet d'un traitement illicite;
- Que la personne retire son consentement;
- Que la personne a exercé son droit d'opposition à un traitement de prospection commerciale et qu'il n'existe pas de motif légitime permettant au responsable de traitement de poursuivre l'opération;
- Que les données collectées l'ont été auprès d'une personne mineure.

Il sera, néanmoins, possible de refuser le droit à l'oubli en raison de la nature de certains traitements, comme par exemple le droit à la liberté d'expression.

- **Le droit à la limitation:**

Ce droit permet à la personne dont les données sont collectées de demander l'arrêt du traitement de ses données, sans pour autant que ces dernières soient effacées. Il va s'agir d'éviter la diffusion des informations pendant le temps de leurs vérifications par le responsable de traitement.

Ce droit peut s'exercer dans les situations suivantes:

- Contestation de l'exactitude des données traitées;
- Traitement illicite;
- Si la personne concernée a fait usage de son droit d'opposition.

- **Le droit à la portabilité des données:**

Ce droit permet, aux personnes qui en font la demande, de recevoir l'ensemble des données personnelles qu'ils ont transmis au responsable de traitement.

Le renforcement du contrôle et des sanctions prononcées par la CNIL

Les pouvoirs de contrôle de la CNIL

La CNIL a vu ses pouvoirs étendus par le RGPD.

La CNIL va veiller à ce que l'usage des données ne porte pas atteinte aux droits des personnes concernées par les traitements.

La CNIL exerce 3 types de contrôles:

- Contrôle sur audition
- Contrôle sur place
- Contrôle en ligne (ici, la CNIL ne contrôlera que les données de l'entreprise qui sont librement accessible).

Lorsque la CNIL contrôle une entreprise, cette dernière doit être en mesure de lui fournir:

- Le maximum d'informations techniques et juridiques afin d'être en mesure d'apprécier les conditions dans lesquelles sont traitées les données.
- Tous les documents nécessaires
- Les accès aux serveurs, programmes, données, etc.

Les sanctions prononcées par la CNIL

Les sanctions prononcées par la CNIL sont des sanctions administratives. Ainsi, cette dernière peut prononcer:

- Un avertissement
- Un rappel à l'ordre
- Une injonction de répondre aux demandes d'une personne concernée
- Une injonction de mise en conformité
- Une injonction de notifier une violation de donnée à une personne concernée
- Une limitation temporaire ou définitive du traitement
- Une injonction de rectifier ou d'effacer des données
- Un retrait de certification

Elle peut également prononcer des sanctions pécuniaires. Les amendes sont réparties en deux catégories, en fonctions des manquements dont se sera rendue coupable l'entreprise:

- Violations passibles d'une amendes de dix millions d'euros ou de 2% du CA annuel mondial de l'entreprise sur l'exercice précédent
- Violations passibles d'un montant maximum de vingt millions d'euros ou de 4% du CA annuel mondial de l'entreprise sur l'exercice précèdent.

Mettez-vous en conformité!

Se mettre en conformité peut s'avérer fastidieux pour une entreprise. Ainsi, le Cabinet MEPERY vous propose de réaliser, au sein de votre entreprise, un audit RGPD afin d'évaluer votre niveau de conformité à la nouvelle législation et, le cas échéant, d'établir, à vos côtés, un plan d'action afin de pallier aux manquements.

PRESTATION & ACCOMPAGNEMENT

PREPARATION

- Récupération sur place et analyse des documents liés aux données personnelles que vous récoltez
- Identification des besoins selon les parties prenantes internes et externes

AUDIT

- Réalisation sur place des audits sur la protection des données personnelles,
- Adaptation des référentiels d'audits selon le secteur d'activité
- Rédaction des conclusions de conformité et remise d'un tableau de conformité ou de non-conformité – Reporting.
- Conseil sur les process de mise à niveau

MISE EN CONFORMITE

- Plan d'action détaillé et adapté
- Mise en relation avec un spécialiste technique
- Fourniture des outils de mise en conformité
- Possibilité de rédaction de supports juridique (Mentions légales, CGU, Charte de Données Personnelles *)

** Prestations faisant l'objet d'une tarification supplémentaire*

COUT D'UN AUDIT *

1 100€

Pour les autres entreprises

2 200€

6 500€

Sur Devis

Le Cabinet MEPERY vous propose un accompagnement personnalisé et adapté à votre structure. Spécialiste des domaines Juridiques et agréé organisme de Formation, le Cabinet MEPERY vous conseil en Droit du Travail, Droit de la Consommation, des Contrats ou encore Droit des Assurances. Entouré par des avocats reconnus, comme le Cabinet de Maître BERNIAUD et Maître ROUILLE, nous mettons tout en œuvre pour adapter notre offre aux réels besoins de nos clients.

Les enjeux de la Nouvelle Réglementation RGDP sont grands. Parce que les entreprises recueillent et exploitent de plus en plus de données personnelles, les organismes régulateurs ont mis en place de nouvelles législations encadrant de manière plus stricte la collecte et la gestion de ces données. Il est donc de votre responsabilité, vous entreprise, de vous mettre en conformité. Pour ce faire, être accompagné est gage de sérénité.

Contactez-nous!

Cabinet Juridique & Technique

25 Route de Seilh

31700 CORNEBARRIEU

09 88 39 26 77

contact@cabinet-mepery.fr

cabinet-mepery.fr

En collaboration avec le Cabinet de **Maître Marie-Laure BERNIAUD**

BERNIAUD AVOCATS

*Hors Taxe