Nouveau règlement européen

Contexte et procédure

L'Union européenne dispose d'un cadre pour la protection des données depuis 1995, sous la forme d'une directive, transposée par chaque État membre dans son droit national.

En 2012, la Commission européenne a proposé de faire évoluer la législation, afin de corriger les incohérences liées aux différences de mise en œuvre entre les États membres, et de l'adapter aux nouveaux services en ligne (réseaux sociaux, géolocalisation, etc.), qui impliquent toujours plus de traitements de données à caractère personnel.

Après son examen par les différentes institutions européennes, le nouveau cadre législatif a finalement été publié en avril 2016. Son application est prévue pour fin mai 2018. L'instrument juridique retenu est un règlement, ce qui signifie qu'il est directement applicable dans les États membres et que ses dispositions sont uniformément appliquées sur le territoire européen.

Contenu de la réforme

Objet et champ d'application

Le premier objectif du règlement est la protection des personnes dont les données à caractère personnel sont soumises à un traitement. Une ***donnée à caractère personnel*** peut être n'importe quelle information qui se rapporte à une personne physique identifiable (par son nom, un identifiant, un numéro, sa localisation…). Peuvent être désignés comme un ***traitement*** la collecte, l'enregistrement, la consultation, la communication, la diffusion, etc. de ces données. Le second objectif du règlement est de fournir des règles pour la libre circulation des données à caractère personnel dans l'UE.

Le règlement concerne toute personne, entreprise ou autorité publique qui traite des données à caractère personnel et qui se trouve dans l'Union européenne. Il concerne aussi le traitement de données par des personnes ou entreprises se trouvant hors de l'UE, si ces données sont traitées pour fournir des biens ou des services, ou pour suivre le comportement d'une personne située dans l'UE. Ainsi, **dès qu'un citoyen européen est visé par un traitement de données, le règlement s'applique**. Tout responsable de traitement situé hors UE souhaitant traiter des données de citoyens européens doit ainsi respecter le règlement et désigner un représentant dans l'UE, qui sera la personne de contact pour les autorités de contrôle et les personnes concernées par le traitement.

Principes généraux pour le traitement des données

Le traitement des données doit être « **licite, loyal, transparent** ». Pour cela, le responsable du traitement doit systématiquement : expliciter la finalité de la collecte, se restreindre à la collecte des données nécessaires à cette finalité, s'assurer que les données sont exactes et actualisées, ne conserver les données que si cela est nécessaire, assurer la sécurité des données qu'il collecte.

En outre, pour être licite, le traitement doit être nécessaire à l'exécution d'un contrat, ou répondre à une obligation légale, à une mission d'intérêt public ou à l'intérêt légitime du responsable, ou encore être **fondé sur le consentement de la personne concernée**. Dans ce dernier cas, le responsable du traitement doit pouvoir démontrer que le consentement a bien été donné par la personne. Si la personne concernée est un **mineur de moins de 16 ans**, alors le consentement est donné par le titulaire de l'autorité parentale. Enfin, les données liées à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, les données génétiques ou biométriques, concernant la santé ou encore la vie ou l'orientation sexuelle d'une

personne, disposent d'un statut particulier : leur traitement est interdit sauf cas spécifiques (dont le consentement de la personne pour une finalité spécifique).

Droits des personnes relatifs au traitement de leurs données

Les premiers droits concernent **l'information de la personne dont les données sont collectées**. Le responsable du traitement doit toujours fournir à la personne concernée les informations suivantes : son identité et ses coordonnées, les finalités du traitement, les destinataires des données à caractère personnel, le transfert éventuel vers un pays tiers, la durée de conservation des données, l'existence de droits liés à ces données, le cas échéant la façon dont il a accédé aux données…

À tout moment, la personne concernée a un **droit d'accès à ses données**. Le responsable fournit alors une copie de ses données à la personne qui peut, si elle le souhaite, également exercer son **droit à la portabilité des données**. Dans ce cas, ses données lui sont fournies dans un format courant, lisible par machine, ce qui lui permet de réutiliser directement ses données auprès d'un autre prestataire de services.

De même, la personne concernée peut faire **rectifier des données inexactes ou compléter des données incomplètes**. Elle peut également demander que ses données soient effacées. C'est ce que l'on appelle le « **droit à l'oubli** ». Celui-ci est possible si : les données ne sont plus nécessaires au regard des finalités du traitement, la personne s'oppose au traitement ou retire son consentement, le traitement est illicite, les données concernent un mineur. Dans certains cas spécifiques, l'effacement n'est pas adéquat (vérification en cours de l'exactitude des données, données nécessaires pour l'exercice de droits en justice…). La personne peut alors demander une **limitation des données**. Celles-ci seront conservées mais non traitées. Pour toute rectification, effacement ou limitation de données, le responsable du traitement doit informer tous les destinataires à qui les données ont été communiquées des demandes de la personne concernée.

Enfin, il est possible pour une personne d'exercer son **droit d'opposition** au traitement de ses données, si celui-ci est fondé sur l'intérêt légitime du responsable ou sur une mission d'intérêt publique. Les droits et libertés de la personne seront alors mis en balance avec le motif du responsable pour juger si le traitement des données est licite ou non.

Afin d'assurer aux personnes l'exercice effectif de ces différents droits, le responsable du traitement est dans l'obligation de prendre les mesures pour fournir les informations demandées et d'informer la personne de manière transparente, dans un délai maximum d'un mois, des mesures prises ou de son impossibilité d'y donner suite.

Obligations des entreprises et personnes traitant des données

Les principes qui doivent être au cœur de l'action des responsables de traitements sont la protection des données dès la conception et par défaut. La **protection dès la conception** signifie que le responsable du traitement doit mettre en œuvre les principes relatifs à la protection des données en amont, lorsqu'il détermine les moyens du traitement, mais aussi au moment d'effectuer le traitement. La **protection par défaut** signifie que le responsable du traitement doit prendre des mesures pour garantir que, par défaut, seules les données nécessaires pour chaque finalité spécifique seront traitées.

Les entreprises responsables du traitement des données à caractère personnel désignent un **délégué à la protection des données**. Celui-ci est le contact pour les personnes ayant des questions relatives au traitement de leurs données. En interne, le délégué informe et conseille le responsable et ses employés de leurs obligations, contrôle le respect du règlement, coopère et communique avec l'autorité publique de contrôle. La désignation d'un délégué est obligatoire pour les autorités publiques et pour les entreprises ayant une activité de suivi des personnes régulière et à grande échelle, notamment pour les catégories de données particulières (religion, opinions politiques,…).

Pour garantir le respect du règlement, plusieurs outils de conformité sont proposés ou imposés aux responsables de traitements :

- La tenue d'un **registre des activités de traitement** contenant toutes les informations relatives aux traitements effectués et devant être mis à disposition sur demande de l'autorité de contrôle. Cette obligation s'applique pour les entreprises de plus de 250 salariés, et pour les entreprises de moins de 250 salariés dont les traitements sont fréquents et comportent un risque pour les droits et libertés des personnes concernées.
- La **notification des violations de données à caractère personnel** à l'autorité de contrôle compétente dans les meilleurs délais, et à la personne concernée si la faille de sécurité comporte un risque élevé pour ses droits et libertés.
- La conduite d'**études d'impact** quand le traitement des données peut présenter un risque élevé pour les droits et libertés des personnes.
- L'adhésion à un **code de conduite** sectoriel, élaboré pour une catégorie particulière de responsables (les PME par exemple), qui vise à préciser les modalités d'application du règlement pour les entreprises concernées.
- Le recours à **une certification ou un label** de protection des données, qui atteste que le responsable du traitement respecte les exigences du règlement.

Les **amendes applicables** en cas de violation par les responsables de traitements de leurs obligations ont été renforcées : selon les infractions, elles peuvent aller jusqu'à 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, jusqu'à 2% ou 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

Transfert de données vers des pays tiers

Le nouveau règlement pose un principe simple : le transfert de données à caractère personnel vers un pays tiers, dans l'objectif de les traiter a posteriori, est **autorisé seulement si les conditions sont réunies pour assurer la protection des personnes concernées**. Cette garantie de protection des personnes peut être apportée par plusieurs moyens :

- La Commission européenne peut rendre au sujet d'un pays une **décision d'adéquation**, c'est-à-dire qu'elle affirme que le niveau de protection des données à caractère personnel y est adéquat. Pour cela, elle observe dans le pays le respect des droits de l'homme, la législation pertinente en vigueur, l'existence d'autorités de contrôle indépendantes…
- Si le pays tiers en question n'a pas fait l'objet d'une décision d'adéquation, le responsable du traitement peut prévoir des **garanties appropriées** pour protéger les libertés et droits fondamentaux des personnes. Celles-ci peuvent prendre plusieurs formes : un accord entre autorités, des règles d'entreprise contraignantes, un code de conduite, une certification…
- Enfin, en l'absence des autres conditions, le consentement explicite de la personne, la nécessité d'un traitement pour l'exécution d'un contrat conclu avec la personne concernée, des motifs importants d'intérêt public ou encore les intérêts vitaux de la personne concernée peuvent permettre sous certaines conditions le transfert de données vers un pays tiers.

À noter que le règlement est sans incidence sur les accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers qui ont été conclus avant le 24 mai 2016.

Autorités de contrôle

Dans chaque État membre, une ou plusieurs autorités sont chargées de surveiller l'application du règlement. En France, il s'agit de la CNIL. Les États membres choisissent librement l'organisation interne de leurs autorités, à condition qu'elles disposent de pouvoirs suffisants (pouvoirs d'enquête, de coercition, d'ester en justice, etc.) pour remplir leurs missions. Celles-ci impliquent, outre le contrôle de l'application du règlement, la sensibilisation du public et des responsables de

traitements, le conseil des autorités publiques en matière de protection des données, le traitement des réclamations des personnes concernées…

Lorsqu'un citoyen veut porter une réclamation devant une autorité de contrôle, un principe simple s'applique : le **guichet unique**. Cela signifie que le citoyen peut s'adresser à l'autorité de contrôle de son pays, même si le responsable du traitement est établi dans un autre pays. De manière symétrique, chaque responsable de traitements de données à caractère personnel est rattaché à une seule autorité de contrôle, même s'il a des activités dans plusieurs pays. L'autorité de contrôle concernée est alors celle du pays où l'entreprise a son établissement principal.

Dans le cas où le citoyen et le responsable du traitement sont dans des pays différents, l'autorité dont relève l'entreprise est désignée comme **autorité « chef de file »** : c'est elle qui prend les décisions. Le règlement prévoit ainsi un mécanisme de coopération entre les différentes autorités de contrôle : l'autorité qui reçoit une réclamation en fait part à l'autorité chef de file, qui soumet rapidement un projet de décision aux autres autorités concernées, puis le met en œuvre en informant les acteurs concernés, l'auteur de la réclamation étant quant à lui informé par l'autorité auprès de laquelle il a introduit sa réclamation. Ce mécanisme est complété par des mécanismes d'assistance mutuelle et des opérations conjointes des autorités de contrôle.

La coordination des activités de contrôle et le règlement d'éventuels désaccords entre les autorités nationales sont assurés par un **Comité européen de la protection des données**. Il est composé d'un responsable d'autorité de contrôle de chaque État membre et du Contrôleur européen de la protection des données (autorité de contrôle indépendante créée en 2004 pour contribuer à la protection de la vie privée au niveau européen).

Voies de recours

En cas de litige, les personnes physiques ou morales ont plusieurs voies de recours :

- **Réclamation auprès d'une autorité de contrôle** : tout citoyen peut introduire une réclamation auprès de l'autorité de contrôle du pays où il habite.
- **Recours juridictionnel contre une autorité de contrôle** : un recours peut être formé contre une décision juridiquement contraignante d'une autorité de contrôle, ou encore lorsqu'une autorité de contrôle ne traite pas une réclamation ou n'informe pas (sous 3 mois) la personne de l'état d'avancement ou de l'issue de sa réclamation. Ce recours doit être formé devant les juridictions de l'État membre dont relève l'autorité de contrôle.
- **Recours juridictionnel contre un responsable de traitement** : un recours peut être formé en cas de violation d'un droit conféré par le règlement en matière de traitement des données à caractère personnel. Dans ce cas, le recours peut être formé devant les juridictions de l'État membre où le responsable du traitement a un établissement, ou bien devant les juridictions de l'État membre où la personne concernée habite.
- **Représentation des personnes (action collective)** : les associations actives dans le domaine de la protection des données ont la possibilité d'introduire des recours collectifs en matière de protection des données personnelles.
- **Réparation** : toute personne a droit à réparation pour un préjudice moral ou matériel lié à une violation du règlement.