RGPD

LE RGPD, QU’EST-CE-QUE C’EST ?

Le RGPD impose des exigences détaillées aux entreprises et organisations en ce qui concerne la collecte, la conservation et la gestion des données à caractère personnel. Elles s'appliquent tant aux organisations européennes qui traitent des données à caractère personnel de personnes établies dans l'UE qu'aux organisations établies en dehors de l'UE qui ciblent des personnes vivant dans l'UE.

Quand le règlement général sur la protection des données (RGPD) s'applique-t-il ?

Le RGPD s'applique à votre entreprise si :

- Elle traite des données à caractère personnel et est établie dans l'UE, quel que soit le lieu où se déroule effectivement le traitement des données ;
- Elle est établie en hors de l'UE, mais elle traite des données à caractère personnel dans le cadre de la fourniture de biens ou de services à des personnes établies dans l'UE ou elle analyse le comportement de ces personnes.

Les entreprises non établies dans l'UE qui traitent les données de citoyens de l'UE doivent désigner un **représentant dans l'UE**.

Quand le règlement général sur la protection des données (RGPD) ne s'applique-t-il pas ?

Le RGPD ne s'applique pas si :

- La personne concernée est décédée ;
- La personne concernée est une personne morale ;
- Le traitement est effectué par une personne agissant à des fins qui n'entrent pas dans le cadre de son activité commerciale ou professionnelle.

Qu'entend-on par « données à caractère personnel » ?

Les données à caractère personnel désignent toute information relative à une personne identifiée ou identifiable (la « **personne concernée** »). Elles comprennent notamment les informations suivantes :

- Nom,
- Adresse,
- Numéro de carte d'identité ou de passeport,
- Revenus,
- Profil culturel,
- Adresse IP (Internet Protocol),
- Données détenues par un hôpital ou un médecin (qui identifient de manière unique une personne à des fins médicales).

Catégories de données particulières

Aucune donnée à caractère personnel ne peut être traitée concernant :

- L'origine raciale ou ethnique d'une personne,
- Son orientation sexuelle,
- Ses opinions politiques,
- Ses convictions religieuses ou philosophiques,
- Son affiliation à des organisations syndicales,
- Des informations génétiques, biométriques ou en matière de santé, sauf dans certains cas particuliers (par exemple, lorsque vous avez obtenu le consentement explicite de la personne concernée ou lorsque le traitement est motivé par un intérêt public majeur, en vertu de la législation nationale ou de l'UE),
- Des condamnations pénales ou des infractions, à moins que cela ne soit autorisé par la législation nationale ou de l'UE.

Qui traite les données à caractère personnel ?

Lors de leur traitement, les données à caractère personnel peuvent transiter par différentes entreprises ou organisations. Parmi celles-ci, on distingue deux profils principaux :

- Le **responsable du traitement des données**, qui décide des fins et modalités du traitement des données à caractère personnel,
- Le **sous-traitant** des données, qui détient et traite les données pour le compte du responsable du traitement.

Qui surveille la manière dont les données à caractère personnel sont traitées au sein d'une entreprise ?

Le **délégué à la protection des données (DPD)**, qui peut avoir été désigné par l'entreprise, est chargé de surveiller la manière dont les données à caractère personnel sont traitées et d'informer et de conseiller les membres du personnel qui traitent des données à caractère personnel quant à leurs obligations. Le DPD coopère également avec l'autorité chargée de la protection des données (APD), dont il est le point de contact, tout comme celui des particuliers.

Quand devez-vous désigner un délégué à la protection des données ?

Votre entreprise est tenue de désigner un délégué à la protection des données (DPD) lorsque :

- Elle suit des personnes ou traite des catégories particulières de données de manière régulière ou systématique,
- Ce traitement fait partie de ses activités principales,
- Ce traitement se fait à grande échelle.

Par exemple, si vous traitez des données à caractère personnel pour de la publicité ciblée faite par l'intermédiaire de moteurs de recherche analysant le comportement des internautes, vous devez désigner un DPD. Toutefois, si vous n'envoyez votre matériel promotionnel qu'une fois par an à vos clients, vous n'avez pas besoin de DPD. De même, un médecin qui recueille des données sur la santé de ses patients n'a probablement pas besoin de DPD. Par contre, un DPD est requis dans le cadre du traitement de données à caractère personnel sur la génétique et la santé pour le compte d'un hôpital.

Le DPD peut être un membre du personnel de votre organisation ou un expert externe avec lequel elle a conclu un contrat de service. Le DPD ne doit pas nécessairement faire partie d'une organisation.

Traitement de données pour le compte d'une autre entreprise

Un responsable du traitement des données ne peut recourir qu'à un sous-traitant offrant suffisamment de garanties, lesquelles doivent figurer dans un contrat écrit entre les parties concernées. Ce contrat doit également comporter un certain nombre de clauses obligatoires, dont celle stipulant que le sous-traitant ne traitera des données à caractère personnel que sur instruction du responsable du traitement des données.

Transfert de données en dehors de l'UE

Lorsque des données à caractère personnel sont transférées en dehors de l'UE, la protection offerte par le RGPD doit accompagner ses données. Cela signifie que si votre entreprise exporte des données à l'étranger, elle doit veiller à ce que l'une des mesures suivantes soit respectée :

- Les protections offertes par les pays non membres de l'UE sont jugées adéquates par l'UE
- Votre entreprise prend les mesures nécessaires pour fournir des garanties appropriées, telles que l'introduction de clauses spécifiques dans le contrat conclu avec l'importateur non européen de données à caractère personnel
- Votre entreprise se base sur des motifs spécifiques pour le(s) (dérogations au) transfert, comme le consentement de la personne concernée

Quand le traitement de données est-il autorisé ?

Selon les règles de l'UE en matière de protection des données, vous devez traiter les données de manière loyale et licite, pour des finalités explicites et légitimes, et ne traiter que les données nécessaires pour servir ces finalités. Vous devez veiller à remplir une des conditions suivantes pour traiter les données à caractère personnel :

- Vous avez obtenu le **consentement** de la personne concernée,
- Vous avez besoin des données à caractère personnel pour remplir une **obligation contractuelle** à l'égard de la personne concernée,

- Vous avez besoin des données à caractère personnel pour respecter une **obligation légale**,
- Vous avez besoin des données à caractère personnel pour sauvegarder les **intérêts vitaux** de la personne concernée,
- Vous traitez les données à caractère personnel pour mener à bien une **mission d'intérêt général**,
- Vous agissez pour protéger les **intérêts légitimes** de votre entreprise, tant que les libertés et droits fondamentaux de la personne concernée ne sont pas gravement menacés. Si les droits de la personne concernée prévalent sur les intérêts de votre entreprise, vous ne pouvez pas traiter les données à caractère personnel.

Donner son accord (« consentement ») pour le traitement des données

Le RGPD prévoit des règles strictes pour le traitement de données fondé sur le consentement. Elles ont pour objectif de **garantir que la personne concernée comprenne à quoi elle consent**. Aussi le consentement doit-il être libre, spécifique, éclairé et univoque, et faire l'objet d'une demande formulée en des termes clairs et simples. Le consentement doit être donné par un acte positif, comme le fait de cocher une case en ligne ou de signer un formulaire.
Lorsqu'une personne consent au traitement de ses données à caractère personnel, seules les données pour lesquelles le consentement a été donné peuvent être traitées. Vous devez également permettre à la personne concernée de retirer son consentement.

Fournir des informations transparentes

Vous devez indiquer clairement à la personne concernée qui traite ses données à caractère personnel et pourquoi. Les informations suivantes doivent figurer, au minimum :

- Qui vous êtes,
- Pourquoi vous traitez les données à caractère personnel,
- Quel est le fondement juridique du traitement,
- Qui recevra les données (le cas échéant).

Dans certains cas, vous devez également indiquer :

- Les coordonnées du délégué à la protection des données (DPO) (le cas échéant),
- Quel est l'intérêt légitime poursuivi par l'entreprise lorsqu'elle se repose sur ce fondement juridique pour traiter les données,
- Les mesures appliquées pour le transfert de données dans un pays non membre de l'UE,
- Pendant combien de temps les données seront conservées,
- Les droits de la personne concernée en matière de protection des données (à savoir les droits d'accès, de rectification, d'effacement, de limitation, d'objection, de portabilité, etc.),
- Comment le consentement peut être retiré (lorsque le consentement constitue le fondement juridique du traitement des données),
- S'il existe une obligation légale ou contractuelle de fournir les données,
- En cas de prise de décision automatisée, des informations sur la logique, la portée et les conséquences de la décision.

Vous devez présenter ces informations en des termes clairs et simples.

Règles spécifiques pour les enfants

Pour recueillir les données à caractère personnel d'un enfant sur la base d'un consentement, par exemple au moyen d'un compte de média social ou d'un compte de téléchargement, **vous devez d'abord obtenir un consentement parental**, en informant un de ses parents ou son tuteur légal, par exemple. L'âge jusqu'auquel une personne est considérée comme un enfant varie selon le pays, mais il se situe entre 13 et 16 ans.

Droit d'accès et droit à la portabilité des données

Vous devez veiller à ce que la personne concernée ait le **droit d'accéder à ses données à caractère personnel** gratuitement. Si vous recevez une demande d'accès, vous devez :

- Indiquer à la personne concernée si vous traitez ses données à caractère personnel,

- L’informer sur le traitement (finalité du traitement, catégories de données à caractère personnel concernées, destinataires des données, etc.),
- Lui fournir une copie des données à caractère personnel traitées (dans un format accessible).

Lorsque le traitement est fondé sur le consentement ou un contrat, la personne concernée peut également vous demander de lui renvoyer ses données à caractère personnel ou de les transmettre à une autre entreprise. Ce droit au transfert des données est également appelé « portabilité des données ». Vous devez fournir les données dans un format couramment utilisé et lisible par machine.

Droit à la rectification et droit d'opposition

Si une personne concernée estime que ses données à caractère personnel sont incomplètes ou inexactes, elle a le **droit de les faire rectifier ou compléter** dans les meilleurs délais.
Dans ce cas, vous devez informer tous les destinataires des données à caractère personnel que celles que vous avez partagées avec eux ont été modifiées ou supprimées. Si des données à caractère personnel que vous avez partagées étaient inexactes, il se peut que vous deviez également en informer toute personne les ayant vues (sauf si cela exige des efforts considérés comme disproportionnés).

Une personne **peut s'opposer à tout moment au traitement de ses données à caractère personnel** pour un usage particulier lorsque votre entreprise les traite pour son propre intérêt légitime ou dans le cadre d'une mission d'intérêt général. Vous devez arrêter de traiter ses données à caractère personnel, sauf si vous poursuivez un intérêt légitime qui prévaut sur les intérêts de la personne concernée.
De même, une personne peut demander que le traitement de ses données à caractère personnel soit limité le temps que soit déterminé si votre intérêt légitime prévaut ou non sur ses intérêts. Toutefois, en cas de marketing direct, vous devez toujours arrêter le traitement des données à caractère personnel lorsque la personne concernée le demande.

Droit à l'effacement (« droit à l’oubli »)

Dans certaines circonstances, une personne peut demander au responsable du traitement des données d'effacer ses données à caractère personnel, par exemple si ces données ne sont plus nécessaires pour atteindre la finalité du traitement. Toutefois, votre entreprise n'est pas tenue de le faire si :

- Le traitement est nécessaire pour respecter la liberté d'expression et d'information,
- Vous devez conserver les données à caractère personnel pour respecter une obligation légale,
- La conservation des données à caractère personnel se justifie par d'autres motifs d'intérêt public, comme la santé publique ou la recherche scientifique et historique,
- Vous devez conserver les données à caractère personnel dans le cadre d'une procédure judiciaire.

Prise de décision et profilage automatisés

Une personne a le **droit de ne pas faire l'objet d'une décision prise sur le seul fondement d'un traitement automatisé**. Il existe cependant des **exceptions à cette règle**, par exemple, si elle a donné son consentement explicite à la décision automatisée. Hormis les cas où la décision automatisée possède un fondement juridique, votre entreprise doit :

- Informer la personne concernée du caractère automatisé de la prise de décision,
- Lui permettre de faire réexaminer la décision automatisée par une personne,
- Lui permettre de contester la décision automatisée.

Par exemple, si une banque automatise la décision d'accorder ou non un prêt à une personne, celle-ci doit être informée de la décision automatisée et pouvoir la contester et demander une intervention humaine.

Violations de données et communication adéquate

Une **violation de données désigne la divulgation non autorisée, accidentelle ou illicite, de données à caractère personnel dont vous être responsable**, leur inaccessibilité temporaire ou leur modification.
Si une violation de données se produit et engendre un risque pour les libertés et droits individuels, vous devez en informer votre autorité chargée de la protection des données dans un délai de 72 heures après avoir eu connaissance de la violation.

Suivant que la violation de données engendre ou non un risque élevé pour les personnes touchées, votre entreprise peut également être tenue d'informer toutes les personnes concernées.

Répondre aux demandes

Si votre entreprise reçoit la demande d'une personne souhaitant exercer ses droits, vous devez y répondre dans les meilleurs délais et, en tout état de cause, moins d'un mois après réception de la demande. Ce délai de réponse peut être prolongé de deux mois pour les demandes multiples ou complexes, à condition que la personne concernée soit informée de cette prolongation. Les demandes doivent être traitées gratuitement.

Si une demande est rejetée, vous devez informer la personne concernée des raisons de ce rejet et de son droit d'introduire une réclamation auprès de l'autorité chargée de la protection des données.

Analyses d'impact

Une analyse d'impact relative à la protection des données est obligatoire lorsque le traitement envisagé **engendrerait un risque élevé** pour les droits et libertés des personnes, par exemple en cas d'utilisation de nouvelles technologies.
Un tel risque existe lorsque :

- Des dispositifs de traitement et de profilage automatisés sont utilisés pour évaluer des personnes,
- Une zone accessible au public fait l'objet d'une surveillance à grande échelle (par des caméras de sécurité, par exemple),
- Des catégories particulières de données ou des données à caractère personnel relatives à des condamnations pénales ou à des

infractions sont traitées à une grande échelle (données médicales, par exemple).

Remarque : les autorités chargées de la protection des données peuvent également considérer d'autres catégories de traitement des données comme étant à haut risque.
Si les mesures mentionnées dans l'analyse d'impact relative à la protection des données ne suppriment pas tous les risques élevés soulevés, l'autorité chargée de la protection des données doit être consultée avant le début du traitement des données.

Garder une trace

Votre entreprise doit être capable de prouver qu'elle agit en conformité avec le RGPD et remplit toutes ses obligations, notamment en cas de demande ou d'inspection de l'autorité chargée de la protection des données.

Une façon d'y parvenir consiste à tenir un registre détaillé où figurent notamment les éléments suivants :

- Nom et coordonnées de votre entreprise intervenant dans le traitement des données,
- Raison(s) du traitement des données à caractère personnel,
- Description des catégories de personnes fournissant des données à caractère personnel,
- Catégories d'organisations recevant les données à caractère personnel,
- Transfert de données à caractère personnel vers un autre pays ou une autre organisation,
- Période de conservation des données à caractère personnel,
- Description des mesures de sécurité prises lors du traitement des données à caractère personnel.

Votre entreprise doit également disposer de procédures et lignes directrices écrites, mises à jour régulièrement, et les communiquer à son personnel.

Avertissement

Si votre entreprise n'est pas plus grande qu'une PME , elle n'est obligée de garder une trace de ses activités de traitement, à condition que celles-ci :

- Ne soient pas exercées régulièrement,
- Ne portent pas atteinte aux droits et libertés des personnes concernées,
- Ne concernent pas des données sensibles ou des casiers judiciaires.

Protection des données dès la conception et protection des données par défaut

La **protection des données dès la conception** désigne le fait que votre entreprise doit envisager des mesures de protection des données dès qu'elle prévoit d'utiliser un nouveau moyen de traiter les données à caractère personnel. En vertu de ce principe, le responsable du traitement doit prendre toutes les mesures techniques et organisationnelles qui s'imposent pour mettre en œuvre les principes de protection des données et pour protéger les droits des personnes concernées. Ces mesures peuvent inclure, par exemple, la pseudonymisation.
La **protection des données par défaut** désigne le fait que votre entreprise doit toujours utiliser par défaut les paramètres les plus favorables au respect de la vie privée. Par exemple, s'il est possible de choisir entre deux paramètres relatifs à la protection de la vie privée et si l'un de ces paramètres empêche l'accès de tiers aux données à caractère personnel, c'est ce paramètre qui doit être utilisé par défaut.

Violation des règles et sanctions

Le non-respect du RGPD peut entraîner d'importantes sanctions financières, pouvant s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial d'une entreprise pour certaines infractions. L'autorité chargée de la protection des données peut imposer d'autres mesures correctives à une entreprise, comme l'interdiction du traitement de données à caractère personnel.