Règlement général sur la protection des données personnelles (RGDP)

Contexte général

Le **Règlement européen sur la protection des données personnelles** (RGDP), adopté en 2016 par le Parlement européen et le Conseil, sera directement applicable en France **à compter du 25 mai 2018**. Il modifie la directive 95/46/UE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

- **Pourquoi un nouveau règlement ?**

La Commission européenne a considéré que la directive 95/46/CE avait été mise en œuvre de manière extrêmement fragmentée dans l'UE et que demeurait dans le public un sentiment de persistance de risques pour la protection des droits et libertés des personnes physiques.

Les différences dans le niveau de protection des personnes physiques en matière de données personnelles empêchent ainsi le libre flux de ces données dans l'ensemble de l'UE, ce qui peut **constituer un obstacle à l'exercice des activités économiques au niveau communautaire**, **fausser la concurrence** et **empêcher les autorités de s'acquitter des obligations qui leur incombent en vertu du droit de l'UE**.

Le présent règlement vise donc à garantir cette harmonisation au niveau européen, tout en laissant des **marges de manœuvre à chaque Etat membre** pour préciser davantage l'application des règles de ce règlement, notamment en ce qui concerne le traitement des données dites « **sensibles** »[1].

- **Quels objectifs et quelles sanctions ?**

Ce règlement opère un **nivellement par le haut des pratiques et mesures pour assurer la protection et la confidentialité des données personnelles**, tout en renforçant le contrôle de l'utilisateur de ces données.

L'innovation de ce règlement est qu'il repose sur le principe de l'*accountability* : il n'y aura plus d'obligations déclaratives à la CNIL, mais chaque entreprise **collectant ou traitant des données personnelles** devra s'assurer elles-mêmes de la **conformité** de leurs traitements (anonymisation, restriction des accès, traçabilité, consentement éclairé…) au règlement. En d'autres termes, le poids de la procédure administrative va être transféré de la CNIL à l'intérieur du magasin.

Ces nouvelles règles s'appliquent à **toutes les entreprises du commerce** (BtoB et BtoC), indépendamment de leur taille, dès lors qu'elles utilisent un fichier salariés et/ou un fichier clients.

Le non-respect de ces obligations par les entreprises peut donner lieu à des **sanctions administratives** dont les plafonds ont été considérablement relevés (jusqu'à 4 % du chiffre d'affaires annuel mondial). La CNIL précise que les sanctions, selon les cas, pourront être précédées d'un avertissement, puis d'une mise en demeure. Les autorités de protection pourront également exiger une suspension des flux de données hors UE, ainsi que la limitation temporaire ou définitive d'un traitement de données.

[1] Considérant 51 : ces données sont celles qui révèlent l'origine raciale ou ethnique par exemple, les opinions politiques, la religion ou les convictions, l'appartenance syndicale, le statut génétique ou l'état de santé, l'orientation sexuelle…

Les grands principes de protection des données

Principe 1 : la finalité

DÉFINIR ET RESPECTER LES OBJECTIFS DU FICHIER

Avant de collecter des données personnelles, le responsable de traitement (voir définition en annexe) doit établir précisément la finalité pour laquelle un traitement va être réalisé, i.e. ce à quoi les données collectées lui serviront. Cette finalité devra être respectée pendant toute la durée du traitement : tout traitement ultérieur réalisé dans un objectif autre que celui déclaré constitue un détournement de finalité, interdit par la loi Informatique et Libertés (IFL).

Principe 2 : la proportionnalité

VÉRIFIER LA PROPORTIONALITÉ ET LA PERTINENCE DES DONNÉES

Le responsable de traitement ne peut collecter que des données qui sont strictement nécessaires à la réalisation de la finalité du traitement qu'il a déclaré. Le principe de minimisation des données, repris par le Règlement Européen, lui interdit de collecter des données excédant celles dont il a réellement besoin pour réaliser son objectif.

Principe 3 : La temporalité

NE CONSERVER LES DONNEES QUE POUR UNE DUREE LIMITEE

Le responsable de traitement ne peut conserver les données collectées que pour une durée limitée, qu'il doit préalablement définir. Cette durée ne peut excéder celle nécessaire pour l'accomplissement des finalités pour lesquelles les données sont traitées, et doit tenir comptes des éventuelles obligations légales de conservation des données. A l'expiration du délai prévu, le responsable de traitement doit impérativement effacer lesdites données (sauf exception légale), sous peine de sanctions pénales (délit).

Principe 3 : la transparence

DECLARER LES TRAITEMENTS ET INFORMER LES PERSONNES

Le responsable de traitement doit agir de manière loyale et transparente, ce qui implique :

- Vis-à-vis des autorités (CNIL)
- Vis-à-vis des personnes concernées, de les informer de l'existence d'un traitement et de sa/ses finalité(s), de son identité, des destinataires des données, des droits dont ils disposent et de la manière dont ils peuvent les exercer, du caractère obligatoire ou facultatif des réponses, de la durée de conservation des données et des transferts éventuels de données en dehors de l'UE.

Principe 4 : le consentement

RECUEILLIR LE CONSENTEMENT DE LA PERSONNE

Avant de traiter les données personnelles d'une personne, le responsable de traitement doit recueillir son consentement, sauf si une des dérogations prévues à l'article 7 de la loi IFL – ou à l'article 8 en cas de données sensibles telles que les données de santé – est applicable.

> Le consentement peut se faire notamment en cochant une case lors de la consultation d'un site internet ou au moyen de toute déclaration ou tout comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel.
> A noter :
> - Le silence, l'inactivité et l'inaction du client ne peuvent pas valoir consentement
> - La charge de la preuve du consentement revient au responsable du traitement

Principe 5 : la sécurité et la confidentialité

ASSURER LA SECURITE ET LA CONFIDENTIALITE DES DONNEES

Le responsable de traitement doit prendre toutes les mesures nécessaires pour garantir la sécurité et la confidentialité des données, c'est-à-dire pour éviter qu'elles ne soient endommagées, déformées, ou que des tiers non-autorisés y aient accès.

Quels droits pour les personnes physiques concernées ?

Le nouveau cadre européen vient **renforcer des droits déjà connus :**

- droit d'accès aux données des personnes
- droit de rectification
- droit d'opposition : ce droit s'applique notamment lorsque des données à caractère personnel sont traitées à des fins de prospection, la personne concernée pouvant notamment s'opposer au profilage dans la mesure où il est lié à une telle prospection.
- droit à l'oubli et à l'effacement : lorsque leurs données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière, lorsque les personnes concernées ont retiré leur consentement au traitement ou lorsqu'elles s'opposent au traitement de données à caractère personnel.

mais innove également en reconnaissant :

- un **droit à la limitation du traitement** : le client pourra ainsi désigner certaines données qu'il ne souhaite pas voir traitées, lorsqu'il conteste l'exactitude de ces données, lorsque leur traitement est illicite ou lorsqu'il en a besoin pour l'exercice de ses droits en justice
- un **droit à la portabilité des données** : concrètement, le client pourra récupérer les données fournies à un commerçant afin de les transmettre à un autre.

> **Considérant 68** : Les personnes devraient aussi avoir le droit de recevoir les données à caractère personnel les concernant, qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé, lisible par machine et interopérable, et de les transmettre à un autre responsable de traitement. Il y a lieu d'encourager les responsables de traitement à mettre au point des formats interopérables (compatibilité avec d'autres produits ou systèmes informatiques) permettant la portabilité des données.

Quelles obligations pour les commerçants ?

➢ *Nommer un délégué à la protection des données*

Le règlement fait référence à la désignation d'un **délégué à la protection des données** lorsque **les activités de base** du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, **exigent un suivi régulier et systématique à grande échelle des personnes concernées**.

Le G29 est venu préciser dans des lignes directrices les critères à prendre en compte pour juger de l'obligation ou non de désigner un DPO :

- le traitement doit concerner les « **activités de base** » de l'organisme. Selon le considérant 97 du RGPD, « *dans le secteur privé, les activités de base d'un responsable du traitement ont trait à ses activités principales et ne concernent pas le traitement des données à caractère personne* ***en tant qu'activité auxiliaire***. »

  Le G29 précise que les activités de base visent les opérations clés nécessaires au responsable de traitement pour atteindre ses objectifs, **en particulier lorsque le traitement de données forme une part inextricable de son activité.**

- le traitement doit être « **à grande échelle** » : le règlement indique qu'il s'agit des traitements « *qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées* » (considérant 91).

Le G29 vient ajouter que les facteurs suivants doivent être pris en compte : le nombre d'individus concernés, le volume de données et/ou les différentes catégories de données traitées, la durée, la permanence du traitement, et l'étendue géographique du traitement. La nomination d'un DPO semble donc réservée aux grandes entreprises[2].

- le traitement doit impliquer « **un suivi régulier et systématique** » : le règlement précise, s'agissant de la notion de « suivi », que « *afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit* » (considérant 24).

  S'agissant de la notion de « régulier », le G29 indique qu'un ou plusieurs des facteurs suivants peuvent le caractériser : le suivi qui intervient à **intervalles particuliers ou à des périodes particulières**, le suivi **récurrent ou répété à des moments fixes**, le suivi intervenant de **façon constante ou périodique**.

  Enfin, s'agissant de la notion de « systématique », le G29 indique qu'un ou plusieurs des facteurs suivants peuvent le caractériser : le suivi intervenant **via un système**, ou **selon une organisation ou une méthode**, le suivi intervenant dans le cadre d'un **plan plus général de collecte de données, le suivi mené dans le cadre d'une stratégie**.

  Sont ainsi donnés à titre d'exemples, la fourniture de services de télécommunications, **l'email retargeting**, le **profiling** et le scoring visant par exemple à évaluer les risques de fraudes, le **suivi de la localisation**, notamment via des applications mobiles, la **publicité comportementale**, etc.

➢ *Cartographier vos traitements de données personnelles*

Dans le cadre du futur règlement, les organismes doivent tenir une documentation interne complète sur leurs traitements de données personnelles et s'assurer que ces traitements respectent bien les nouvelles obligations légales.

Pour être en capacité de mesurer l'impact du règlement sur votre activité et de répondre à cette exigence, il est nécessaire au préalable de recenser précisément :

- les différents traitements de données personnelles ;
- les catégories de données personnelles traitées ;
- les objectifs poursuivis par les opérations de traitements de données ;
- les acteurs (internes ou externes) qui traitent ces données. Ils devront notamment clairement identifier les prestataires sous-traitants afin d'actualiser les clauses de confidentialité ;
- les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne.

Pour retraiter ces données de manière efficace, la tenue d'un registre de traitement (ou de conformité) est obligatoire pour les entreprises de plus de 250 salariés, et fortement conseillée pour les autres. Il existe pour cela des logiciels qui permettent de retracer les traitements mis en œuvre ainsi que les actions de conformité qui devront être menées par la suite et l'état réel de ces actions.

[2] La CNIL évalue le nombre d'organisations concernées à 100 000.

Pour chaque traitement de données personnelles, posez-vous les questions suivantes :	
QUI ?	*• Inscrivez dans le registre le nom et les coordonnées du responsable du traitement (et de son représentant légal) et, le cas échéant, du délégué à la protection des données ;* *• Identifiez les responsables des services opérationnels traitant les données au sein de votre organisme ;* *Etablissez la liste des sous-traitants.*
QUOI ?	*• Identifiez les catégories de données traitées* *• Identifiez les données susceptibles de soulever des risques en raison de leur sensibilité particulière (par exemple, les données relatives à la santé ou les infractions)*
POURQUOI ?	*• Indiquez la ou les finalités pour lesquelles vous collectez ou traitez ces données (exemple : gestion de la relation commerciale, gestion RH…).*
OÙ ?	*• Déterminez le lieu où les données sont hébergées.* *• Indiquez dans quels pays les données sont éventuellement transférées.*
JUSQU'À QUAND ?	*• Indiquez, pour chaque catégorie de données, combien de temps vous les conservez.*
COMMENT ?	*• Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées ?*

➢ *Protéger les données dès la conception et par défaut*

L'article 5 du règlement rappelle que la sécurité et la protection des données est un enjeu fondamental :

> **Article 5.f** : les données sont « traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

Le cœur de l'obligation de sécurité est ensuite défini par **l'article 32**, qui impose :

> **Article 32** : Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:
> a) la pseudonymisation et le chiffrement des données à caractère personnel;
> b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
> c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
> d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Le texte n'entre pas dans les détails techniques des mesures qui doivent être mises en œuvre, sinon de spécifier qu'une étude de risque doit être entreprise, de laquelle doivent ressortir des mesures de sécurité appropriées aux besoins. En termes opérationnels, cela signifie analyser les besoins de sécurité de chaque traitement mis en œuvre et mettre en place les mesures adéquates.

> **Considérant 78 :** ces mesures pourraient consister, entre autres, à réduire à un minimum le traitement des données à caractère personnel, à pseudonymiser les données à caractère personnel dès que possible, à garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel, à permettre à la personne concernée de contrôler le traitement des données, à permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer.

➢ *Notifier les violations de données personnelles (considérant 86)*

Tout responsable de traitement devra **avertir la CNIL** de toute violation de données personnelles (c'est-à-dire toute faille de sécurité ayant entraîné, de manière intentionnelle ou accidentelle, la destruction, la perte, l'altération, la révélation ou l'accès non autorisé à ces données).

Le responsable de traitement devra également avertir les personnes concernées de la violation de leurs données personnelles lorsqu'il y a un grave risque d'atteinte à leurs droits et libertés.

Cette obligation est calée sur la même obligation qui était imposée aux opérateurs de communication électroniques dans l'article 34 bis de la loi informatique et libertés, à la différence qu'elle s'applique aujourd'hui à l'ensemble des responsables de traitement.

➢ *Effectuer des analyses d'impact avant la mise en place d'un traitement de données personnelles*

Cette analyse d'impact doit obligatoirement être menée lorsque le traitement est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées* ».

Les traitements qui remplissent au moins **deux des critères suivants** sont concernés :

- évaluation/scoring (y compris le profilage)
- surveillance systématique
- collecte de données sensibles (origine raciale ou ethnique, opinions politiques, religion ou convictions, appartenance syndicale, statut génétique ou état de santé, orientation sexuelle…)
- collecte de données personnelles à grande échelle
- croisement de données
- personnes vulnérables (patients, personnes âgées, enfants)
- usage innovant (utilisation d'une nouvelle technologie

Cette analyse d'impact devra préciser les caractéristiques du traitement, les risques que peut impliquer ce traitement pour les personnes concernées, leur niveau de gravité et les mesures pour neutraliser ou minorer les risques identifiés.

> **Considérant 84** : Afin de mieux garantir le respect du présent règlement lorsque les opérations de traitement sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque. Il convient de tenir compte du résultat de cette analyse pour déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données à caractère personnel respecte le présent règlement.

Annexe : Définitions

Ces définitions sont tirées de l'article 4 du Règlement général sur les données personnelles

Données à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»).

Personne physique identifiable : personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Limitation du traitement : marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur.

Profilage : toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

Pseudonymisation : traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

Responsable du traitement : personne physique ou morale, autorité publique, service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

Sous-traitant : 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 du traitement.

Destinataire : personne physique ou morale, autorité publique, service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers.

Tiers : personne physique ou morale, autorité publique, service ou organisme autre que la personne concernée, responsable du traitement, sous-traitant et personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.

Consentement : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Violation de données à caractère personnel : violation de la sécurité 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.

Données génétiques : données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question.

Données biométriques : données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

Représentant : personne physique ou morale établie dans l'Union, désignée par le responsable du traitement ou le sous-traitant par écrit, en vertu de l'article 27, qui les représente en ce qui concerne leurs obligations respectives en vertu du présent règlement.

Entreprise : personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris les sociétés de personnes ou les associations qui exercent régulièrement une activité économique.

Règles d'entreprise contraignantes : règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe.

Autorité de contrôle : autorité publique indépendante qui est instituée par un État membre en vertu de l'article 51.

Autorité de contrôle concernée : autorité de contrôle qui est concernée par le traitement de données à caractère personnel parce que:

a) le responsable du traitement ou le sous-traitant est établi sur le territoire de l'État membre dont cette autorité de contrôle relève;

b) des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être; ou

c) une réclamation a été introduite auprès de cette autorité de contrôle.