PrestaShop

L'essentiel du RGPD

Livre Blanc

ATTENTION

Le présent document n'a pas vocation à offrir de quelconques conseils juridiques mais simplement une information exhaustive relative aux dispositions du Règlement européen du 27 avril 2016.

PrestaShop ne peut répondre aux questions spécifiques de ses utilisateurs relatives à la mise en œuvre des dispositions dudit règlement.

En cas d'interrogations, il est conseillé de prendre attache avec un Avocat spécialiste des questions relatives au droit des données personnelles.

Le Règlement européen 2016 / 679 du 27 avril 2016 sur la protection des données à caractère personnel est entré en vigueur le 4 mai 2016.

Toutefois, afin de laisser le temps aux acteurs économiques de s'y conformer, son application a été différée au 25 mai 2018.

Il est par conséquent, si tel n'est pas déjà le cas, grand temps de s'interroger quant aux implications concrètes qui en découlent.

Le présent article a ainsi vocation à vous fournir quelques clés de compréhension concernant les grands principes réaffirmés ou créés par ces nouvelles dispositions mieux connues sous son acronyme : RGPD.

Pourquoi ce règlement ?

Ces nouvelles dispositions créent un cadre européen unifié en matière de protection des données des personnes jusqu'alors régie par la Loi Informatique et Libertés du 6 janvier 1978 et la directive n°95/46/CE adoptée en 1995 et transposée en droit français par la loi 2004-801 du 6 août 2004.

Ces textes ont instauré des principes relatifs à la manière de collecter et de traiter les données personnelles des personnes physiques : consentement de la personne ; finalité préalable à la collecte; sécurisation des données ; encadrement des transferts etc.

Adoptés à la fin des années 70 et 90, ces textes ne pouvaient prévoir l'explosion de l'informatique personnelle et d'internet, les réseaux sociaux, les objets connectés, le cloud-computing, etc. qui font apparaître les limites de ces dispositifs et rendent nécessaire une mise à jour.

Par ailleurs, la transposition de la directive dans les différents Etats membres de l'UE avait abouti à des divergences dans les législations nationales, appelant à une harmonisation.

En conséquence, la rédaction d'un projet de règlement ne nécessitant pas de transposition et permettant ainsi d'assurer une meilleure harmonisation a été initié en 2012 pour remplacer la directive. Il a été adopté le 27 avril 2016.

Quel est le champ d'application de ce règlement ?

Le RGPD a vocation à s'appliquer à tout traitement de donnée à caractère personnel, automatisé ou non.

Un traitement de données est défini comme une opération ou un ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel.

Exemple :
collecte, conservation, modification, extraction, consultation, utilisation, communication, destruction, etc.

Une donnée à caractère personnel est constituée par toute information se rapportant à une personne physique et permettant directement ou indirectement de l'identifier.

Exemple :
identité (nom/prénom), adresse mail, adresse IP, numéro de téléphone, données de localisation, habitudes de consommation, etc.

Compte tenu de l'étendue de ces notions et de votre activité de e-commerce, il est fort probable que vous mettiez en œuvre des traitements de données à caractère personnel.

Par ailleurs, l'autre critère d'application du règlement est relatif aux traitements de données à caractère personnel ayant un lien géographique avec le territoire de l'Union Européenne.

Plus concrètement, le RGPD trouvera à s'appliquer lorsque :

- Le responsable de traitement ou son sous-traitant dispose d'un établissement situé sur le territoire de l'Union Européenne,

- Le responsable de traitement ou son sous-traitant ne dispose pas d'un établissement situé sur le territoire de l'Union Européenne mais les personnes dont les données sont traitées se situent sur celui-ci.

Autrement dit, que votre société soit ou non située sur le territoire de l'Union Européenne, le règlement s'applique à la majeure partie des entreprises !

Que prévoit le règlement ? Comment s'y conformer ?

Le Règlement vient réaffirmer ou créer des obligations qui s'imposent aux responsables de traitement (I) qui doivent s'assurer de leur respect au travers de la mise en place de diverses mesures techniques et organisationnelles désignées sous le terme d' « accountability » (II).

Enfin, une des nouveautés du règlement tient notamment au rôle accru joué par l'autorité de contrôle et à l'importance des sanctions en cas de non-respect de ses dispositions par le responsable de traitement (III).

I. LES OBLIGATIONS INCOMBANT AUX RESPONSABLES DE TRAITEMENT

Le règlement impose au responsable de traitement de respecter des obligations relativement :

- Aux traitements (**A**),
- Au respect des droits des personnes concernées (**B**).

A. Les obligations du règlement en matière de traitement

1. Les principes de base applicables aux traitements de données à caractère personnel

L'article 5 du RGPD énumère les différents principes relatifs au traitement des données à caractère personnel.

En vertu de ce dernier, les **données** doivent être :

a – Traitées de manière **licite (voir I.2 ci-dessous), loyale et transparente** ;

b – Collectées pour une **finalité déterminée, explicite et légitime** et ne pas être réutilisées ultérieurement pour une finalité incompatible avec celle initialement prévue au moment de la collecte ;

> Pour savoir si le traitement ultérieur envisagé est ou non compatible avec celui indiqué lors de la collecte initiale, il faut prendre en compte différents critères, tels que : l'existence d'un lien entre les finalités initiale et ultérieure (par exemple, un archivage ultérieur des données afin de satisfaire une obligation légale ou encore à des fins statistiques), la nature des données traitées, la relation entre la personne concernée et le responsable de traitement (par exemple, l'existence d'un contrat), etc

c – **Adéquates, pertinentes et limitées** au regard de la finalité pour lesquelles elles sont traitées (principe de minimisation) ;

Cela se traduit par la nécessité de ne collecter que les données nécessaires à la finalité du traitement mis en œuvre.

d – **Exactes**, et, le cas échéant, tenue à jour **(voir sur ce point I.B ci-dessous)** ;

e – **Conservées** sous une forme permettant l'identification des personnes concernées et **pour une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées** ;

Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes uniquement le temps nécessaire à l'accomplissement de l'objectif qui était poursuivi lors de leur collecte.

La durée de conservation des données ainsi que le point de départ de cette dernière sont librement déterminés par le responsable de traitement dès lors que cette durée n'excède pas celle nécessaire au regard des finalités pour lesquelles les données sont traitées.

Ces données constituent les archives dites « courantes » du responsable de traitement. Dès lors qu'elles ne présentent plus d'intérêt, les données doivent être supprimées sans délai. Par exception, il existe des cas dans lesquels les données doivent faire l'objet d'un archivage.

Il s'agit des données constituant les archives dites intermédiaires regroupant « données qui présentent encore pour les services concernés un intérêt administratif ».

Les durées de conservation de ces données, à des fins et sous la forme d'archive, sont fixées par des dispositions légales ou réglementaires : **Référentiel des durées de conservation de la CNIL**.

Les données conservées afin de satisfaire à une obligation légale ou réglementaire doivent être archivées le temps nécessaire à l'accomplissement de l'obligation et être supprimées dès lors que le motif justifiant leur archivage n'a plus raison d'être.

Enfin, le responsable du traitement dispose également de la possibilité (et non de l'obligation, contrairement aux données qui constituent les archives intermédiaires) de conserver certaines données, notamment lorsque celles-ci présentent un intérêt historique, scientifique ou statistique. Ces données constituent alors les archives définitives du responsable.

Si le choix du mode d'archivage est laissé à l'appréciation du responsable du fichier. Certaines mesures techniques et organisationnelles doivent toutefois être prévues pour protéger les données et assurer un niveau de sécurité approprié à la nature des données.

S'agissant des archives intermédiaires, **la délibération de la CNIL du 11 octobre 2005** relative aux modalités d'archivage électronique recommande d'en limiter l'accès à un service spécifique (par exemple au service contentieux) et de procéder, « a minima, à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations) ».

Quant aux archives définitives, la CNIL recommande de conserver ces dernières « sur un support indépendant, non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à consulter ce type d'archives ».

La CNIL recommande en outre de « mettre en œuvre des dispositifs de traçabilité des consultations des données archivées » ainsi que, d'utiliser « en particulier en cas de données sensibles (...) des procédés d'anonymisation ».

Sur ce point, voir également II ci-dessous.

f – Traitées de façon à garantir aux personnes concernées une sécurité appropriée desdites données au moyen de mesures techniques et/ou organisationnelles (Sur ce point, voir II ci-dessous).

2. Les obligations relatives aux traitements : le principe de « licéité » du traitement

Comme le prévoit le 1 a) de l'article 5 du règlement, un traitement de données à caractère personnel doit être licite.

Or, l'**article 6** du RGPD prévoit qu'un traitement n'est licite que s'il est mis en œuvre sur le fondement de l'une des conditions alternatives suivantes :

- La personne a consenti au traitement.

Le responsable de traitement doit pouvoir prouver que la personne concernée a bien consenti à l'opération de traitement de manière libre (la personne doit avoir le choix de consentir ou non au traitement mais doit également pouvoir retirer son consentement ou refuser de le donner sans subir de préjudice) et éclairée (après avoir été informée de manière claire et complète sur les caractéristiques et les modalités du traitement).

- Le traitement est nécessaire à l'exécution d'un contrat ou de mesures précontractuelles.

Pour mettre en œuvre un traitement sur ce fondement, la personne dont les données font l'objet du traitement doit être partie au contrat.

- Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable de traitement est soumis ou à l'exécution d'une mission d'intérêt public ou relevant de l'autorité publique dont il est investi.

Le traitement que vous mettez en œuvre doit avoir un fondement dans le droit de l'Union Européenne ou d'un Etat membre.

- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

Un traitement ne peut entrer dans le cadre de ce fondement que s'il est motivé par l'urgence de la situation médicale et qu'il est nécessaire à l'administration de soins correspondants.

- Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable de traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données.

Le règlement donne des exemples de finalités répondant à un intérêt légitime du responsable de traitement (ex : prospection commerciale, prévention de la fraude) mais il convient d'effectuer une analyse au cas par cas pour chacun des traitements ayant vocation à être mis en œuvre sur ce fondement.

Si vous souhaitez mettre en œuvre un traitement dans le cadre de ce fondement, vous devez alors vous interroger sur le point de savoir si votre intérêt légitime à mettre en œuvre le traitement prévaut ou non sur l'intérêt de la personne concernée à ce que ses données ne soient pas traitées.

Pour répondre à cette question, un faisceau d'indices doit être analysé : pertinence et réalité des intérêts en présence, type et volume des données traitées, incidences du traitement sur les personnes concernées, modalités du traitement (mutualisation, sécurités, etc.), garanties offertes aux personnes concernées (méthode de chiffrement notamment), etc.

Outre des obligations propres au traitement, le règlement prévoit également des obligations relatives aux droits des personnes concernées.

B. Les obligations relatives aux droits des personnes concernées

Afin de respecter les obligations relatives aux droits des personnes, il convient de ne collecter et traiter les données des personnes concernées qu'après avoir informé ces dernières par une communication facilement accessible (ex : via la politique de confidentialité disponible en ligne) et facile à comprendre, c'est-à-dire, formulée en termes clairs et simples.

Le RGPD liste un ensemble **d'informations devant être obligatoirement délivré par écrit ou** par **tout autre moyen approprié** (notamment électronique) aux personnes concernées par le traitement initial et ultérieur (le cas échéant) **au moment où les données sont obtenues**, et notamment :

- L'identité et les coordonnées du responsable du traitement et de son représentant, les coordonnées du délégué à la protection des données (le cas échéant),

- Le fondement du traitement (voir Article 6 du RGPD) et les conséquences de la non-fourniture de ces données pour la personne concernée,

- L'existence du droit de retirer son consentement, des droits d'accès, de rectification, d'effacement, de limitation, d'opposition et à la portabilité.

ATTENTION : L'information relative au droit d'opposition doit être portée à la connaissance de la personne concernée lors de la première communication avec cette dernière et être présentée séparément de toute autre information.

- Le destinataire des données, l'existence de transferts en dehors de l'UE et garanties associées,
- La durée de conservation,
- Le droit d'introduire une réclamation auprès de l'autorité de contrôle (CNIL),
- L'existence (le cas échéant) d'une prise de décision automatisée, logique, importance et conséquence du traitement.

À SAVOIR : Vous êtes dispensé de cette obligation d'information si la personne concernée dispose déjà de ces informations.

Outre un droit à l'information sur les éléments énumérés ci-dessus, les personnes dont les données sont collectées disposent du droit de demander d'effectuer certaines actions, et notamment :

- **le droit d'accéder à leurs données**, Article 15 du RGPD
Concrètement, dans le cas où la personne concernée vous adresse une telle demande, vous devrez lui indiquer si les données la concernant font ou non l'objet d'un traitement et, le cas échéant, lui communiquer une copie de ces données ainsi que des informations relatives aux caractéristiques du traitement.

ATTENTION :
Une personne qui exerce son droit d'accès doit pouvoir obtenir la communication de l'intégralité des données la concernant.

- **le droit d'obtenir la rectification** des informations inexactes et de compléter les données incomplètes, (Article 16 du RGPD) – Sur ce point, voir II.1 ci-dessous.

- **le droit à l'effacement**, qui peut être mis en œuvre dans les hypothèses énumérées par l'Article 17 du RGPD
- le droit à la limitation, qui peut être également mis en œuvre dans les hypothèses énumérées par l'Article 18 du RGPD

- **le droit à la portabilité**, Article 20 du RGPD : consiste, pour la personne concernée, en le droit d'obtenir dans un format structuré, couramment utilisé et lisible par machine, les données déjà communiquées à un responsable de traitement et de les transmettre à un autre responsable de traitement sans que le premier puisse s'y opposer. Si certaines conditions sont remplies (possibilités techniques, traitement fondé sur le consentement ou sur contrat et effectué à l'aide de procédés automatisés), la personne concernée peut demander que ses données soient directement transmises d'un responsable à un autre.

Pour en savoir plus sur le droit à la portabilité : Guidelines du G29 adoptées le 13 décembre 2016 & FAQ

- **le droit d'opposition**, Article 21 du RGPD
La personne concernée dispose du droit de s'opposer à l'utilisation de ses données à des fins de prospection et, sous certaines conditions, du droit de demander au responsable de traitement de ne plus traiter ses données.

- **le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé**, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative. S'il existe des exceptions à ce droit, vous devez tout de même permettre à la personne concernée d'obtenir une « intervention humaine », d'exprimer son point de vue et de contester la décision - Article 22 du RGPD

ATTENTION

En cas de demande relative à la mise en œuvre de l'un de ses droits, vous devez apporter une réponse à la personne concernée dans les meilleurs délais et, en tout état de cause, dans le délai de 1 mois à compter de la réception de la demande. Ce délai peut être prolongé dans certaines hypothèses mais vous devez en informer la personne concernée.

Si vous ne donnez pas suite à la demande de la personne concernée, vous devez informer cette dernière dans le délai de 1 mois des motifs de votre refus ainsi que de la possibilité pour elle d'introduire une réclamation auprès de la CNIL ou un recours juridictionnel.

En tant que responsable de traitement, vous devez démontrer que vous remplissez l'ensemble de ces obligations.

Afin d'y parvenir, vous devez être en mesure de documenter l'ensemble des mécanismes et procédures internes. C'est le principe « d'accountability » (II).

II.

II. LA MISE EN ŒUVRE DES MESURES TECHNIQUES ET ORGANISATIONNELLES APPROPRIÉES POUR REMPLIR L'OBJECTIF DE CONFORMITÉ AUX DISPOSITIONS DU RÈGLEMENT

L'obligation générale de sécurité de l'article 32 du RGPD **impose** tant au responsable du traitement qu'au sous-traitant **de mettre en œuvre**, compte tenu de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du traitement, du degré de probabilité et de gravité des risques pour les droits des personnes concernées, **toutes les mesures nécessaires et appropriées permettant d'assurer un niveau de sécurité adapté**.

Le respect de cette obligation générale se fait au travers de l'« accountability » qui désigne :

- la mise en œuvre de mesures techniques et organisationnelles de nature à s'assurer que les traitements sont effectués de manière conforme au Règlement (1),
- l'identification et la documentation des mesures mises en œuvre (2).

Il s'agit en réalité pour le responsable de traitement, de rendre des comptes aux autorités et de leur permettre de vérifier les mesures prises.

Jusqu'alors, le préalable à toute mise en œuvre de traitement de données à caractère personnel consistait en la réalisation de formalités préalables (déclarations ou demandes d'autorisation) auprès de la CNIL.

Le règlement vient ainsi modifier cette logique en responsabilisant les acteurs intervenant dans le process de traitement qui devront désormais mettre en œuvre toutes les mesures nécessaires pour démontrer que leurs pratiques sont conformes aux dispositions du règlement.

Afin de remplir leur obligation de sécurité, les responsables de traitement doivent garantir aux personnes concernées un haut niveau de protection de leurs données à caractère personnel.

Pour ce faire, il est nécessaire d'organiser des procédures internes et d'adapter les outils.

Quelles mesures concrètes peuvent être mises en œuvre ?
- Réduire la quantité de données collectées et l'étendue du traitement,
- Pseudonymiser les données collectées dès que possible,
- Permettre aux personnes concernées d'exercer leurs droits (voir II ci-dessus),
- Mettre en place des dispositifs afin d'assurer la sécurité des données collectées et les faire évoluer.

1. L'organisation de procédures internes et l'adaptation des outils

L'article 25 du RGPD introduit des concepts **tels que la « privacy by design » et la « privacy by default »**

La « privacy by design » consiste à prendre les mesures nécessaires et appropriées pour intégrer les obligations en matière de protection des données à l'origine des projets et de s'assurer de la conformité des outils développés tout au long de leur utilisation.

Il s'agit en réalité d'une logique d'anticipation des contraintes juridiques relatives à la protection des données à caractère personnel au moment du choix du traitement afin d'intégrer ces dernières lors de la mise en œuvre du traitement.
Afin d'intégrer ces contraintes juridiques relatives à la protection des données à caractère personnel, il est utile de réaliser un cahier des charges traduisant ces dernières en contraintes techniques.

La « privacy by default » consiste quant à elle à implémenter les mesures techniques et opérationnelles qui vont permettre d'assurer aux personnes concernées que, seules les données nécessaires au regard de la finalité poursuivie par le traitement sont collectées et traitées et que ces opérations sont encadrées par le plus haut niveau de protection possible.

Gérer les demandes des personnes concernées par le traitement

Le responsable de traitement doit s'assurer que les procédures en place permettent aux personnes concernées d'exercer leurs droits et de traiter leurs demandes dans les délais prévus par le règlement (voir II ci-dessus).

Désigner un délégué à la protection des données (DPD)

Le DPD joue un rôle crucial dans la logique de l'accountability dans la mesure où il informe et conseille les décideurs sur les mesures de sécurisation à mettre en œuvre et vérifie que celles-ci répondent aux exigences du règlement.

Quelles mesures concrètes peuvent être mises en œuvre ?

- Désigner les acteurs chargés de répondre aux demandes et réclamations reçues,
- Rédiger des modèles de réponse type afin de fournir une réponse rapide aux personnes,
- Mettre en place les outils nécessaires pour répondre efficacement à certaines demandes (notamment droit d'accès et droit à la portabilité), telles que, par exemple, la possibilité de procéder à un export de l'ensemble des données de la personne.

EST-IL OBLIGATOIRE DE DÉSIGNER UN DPD ?

L'**article 37** du RGPD prévoit l'obligation de désigner un DPD dans certaines hypothèses, et plus particulièrement lorsque :

- le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;
- 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; ou-
- les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

Outre ces hypothèses, la désignation d'un DPD est facultative, sauf si le droit de l'Union européenne ou d'un Etat membre l'exige.

ATTENTION

Les termes de l'**article 37** du RGPD sont suffisamment larges pour que cette obligation soit interprétée largement par les autorités de contrôle.
Par ailleurs, il ressort des **guidelines et de la FAQ du G29 en date du 13 décembre 2016** que la désignation d'un DPD est fortement encouragée même dans les cas où elle n'est pas obligatoire...

Sécuriser les traitements et anticiper les violations

Le responsable de traitement doit garantir la sécurité des données, identifier les risques liés aux traitements mis en œuvre et prendre les mesures préventives nécessaires.

En plus de la prévention, le règlement impose au responsable de traitement de mettre en place les procédures appropriées afin de pouvoir identifier toute violation de données à caractère personnel et, le cas échéant, la notifier à l'autorité de contrôle :

Article 33 du RGPD
Notification à l'autorité de contrôle

Obligation de prévenir de la faille de sécurité dans les meilleurs délais et si possible dans les 72 heures après en avoir eu connaissance + motifs du retard si délai de 72 heures dépassé, contenu de la notification précisée par l'article 33 du RGPD

Article 34 du RGPD
Communication à la personne concernée

Si violation susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

Quelles mesures concrètes peuvent être mises en œuvre ?

- Chiffrer les données (notamment en cas de transferts),
- Limiter et contrôler l'accès physique et numérique aux données,
- Effectuer des sauvegardes régulières sur des supports différents et sécurisés,
- Installer des firewalls et anti-virus.

Par ailleurs, afin de répondre dans les meilleurs délais aux exigences posées par les articles 33 et 34 du RGPD, il est notamment conseillé de :

- Mettre en place une procédure de gestion des failles de sécurité qui en précise les différentes étapes : identification et correction de la faille, rassemblement des preuves techniques et juridiques, dépôt de plainte, déclaration de sinistre à l'assurance, notification à l'autorité de contrôle et, le cas échéant, communication à la personne concernée, et enfin, éventuellement, communication publique relative à la faille de sécurité,
- Rédiger des modèles-types de notification à l'autorité de contrôle,

Sensibiliser et former l'ensemble des collaborateurs

Compte tenu de la valeur que représentent les données personnelles et de leur manipulation par la totalité des acteurs au sein des entreprises, il est nécessaire que le responsable de traitement sensibilise l'ensemble de ses collaborateurs aux questions relatives à leur protection en mettant en place, par exemple, un plan de communication, une charte ou bien encore des procédures relatives à leur utilisation.

Important :

Afin d'aider les professionnels dans leur mise en conformité, la CNIL publie **un guide rappelant les précautions élémentaires** devant être mises en œuvre de façon systématique.
L'autre volet de l'accountability consiste en l'élaboration de la documentation nécessaire à assurer la traçabilité des mesures prises par le responsable de traitement.

2. Rendre compte des mesures prises

- Tenir un registre des activités de traitement – Article 30 du RGPD

Le RGPD prévoit que les traitements mis en œuvre doivent être répertoriés dans un « registre des activités de traitement ».

Ce registre doit se présenter sous forme écrite et doit répertorier tous les traitements, nouveaux et/ou existants. Il doit ainsi être régulièrement mis à jour et être mis à disposition de l'autorité de contrôle en cas de demande.

Les informations contenues dans ce registre diffèrent selon qu'il s'agit du registre des activités de traitement du responsable ou du sous-traitant.

Attention : si le règlement n'impose pas aux entités de moins de 250 salariés de tenir un registre, cette exception ne s'applique pas dès lors que le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées ou s'il n'est pas occasionnel.

Ainsi, tout traitement mis en œuvre et présentant une certaine pérennité doit être retranscrit dans le registre, que l'entité comporte plus ou moins de 250 salariés.

Autrement dit, le champ d'application de cette exception est considérablement réduit.

L'élaboration de ce registre doit être précédée de différentes actions permettant d'identifier les traitements mis en œuvre.

Afin d'accompagner les entreprises,

la CNIL met à disposition sur son site un **modèle de Registre des activités de traitement**

- Réaliser une ou plusieurs analyses d'impact (PIA) – **Article 35** du RGPD

Lorsqu'un traitement de données à caractère personnel est susceptible d'engendrer un risque élevé au regard des droits et libertés des personnes concernées, une analyse doit être menée afin d'évaluer l'origine, la particularité et la gravité du risque afin de déterminer, selon le résultat, les mesures à mettre en œuvre.

La réalisation d'une analyse d'impact est toutefois obligatoire lorsque :

- Les opérations servent à traiter un volume considérable de données susceptibles d'engendrer un risque élevé en raison, par exemple, de leur caractère sensible,

- Les traitements présentent des risques particuliers compte tenu de la particularité des informations traitées (infractions ou condamnations pénales, évaluations automatisées, systématiques et approfondies d'aspects personnels en vue de prendre une décision produisant des effets juridiques, surveillances systématiques à grande échelle d'une zone accessible au public)

- Les traitements présentent un risque pour les droits et libertés des personnes concernées.

Elle doit conduire à la détermination des mesures appropriées à mettre en œuvre pour démontrer que le traitement respecte les exigences

Le règlement n'impose pas de méthodologie spécifique pour la réalisation de ces analyses mais prévoit ce qu'elles doivent contenir. Pour en savoir plus sur l'Analyse d'Impact, n'hésitez pas à consulter la page correspondante du site de la CNIL et à télécharger, le cas échéant, le logiciel open-source développé par cette dernière permettant

- L'encadrement des transferts de données en dehors de l'UE – **Articles 44 à 50** du RGPD

Le règlement prévoit l'encadrement des transferts vers un pays tiers à l'Union européenne, des données qui font ou sont destinées à faire l'objet d'un traitement postérieurement au transfert.

Bien que la notion de transfert ne soit pas définie par le règlement, la CNIL édite un **guide sur les transferts de données à caractère personnel vers des pays non membres de l'UE** dans lequel il est possible de trouver des illustrations de transferts de données.

Un tel transfert peut être effectué sans qu'il soit nécessaire d'obtenir une autorisation préalable si le pays tiers ou l'organisation internationale a été reconnu par la Commission européenne comme assurant un niveau adéquat de protection des données.

En l'absence de décisions d'adéquation, il est également possible de procéder à des transferts de données sans obtenir d'autorisation préalable si les transferts sont encadrés par des mécanismes offrant des garanties appropriées telles que **clauses contractuelles** types et les « Binding Corporate Rules » (BCR).

Il est également possible, en l'absence de décision d'adéquation ou de garanties appropriées, de procéder à un transfert si ce dernier est fondé sur l'une des exceptions énumérées à l'**article 49** du RGPD.

En dernier lieu, si aucune de ces dérogations ne trouve à s'appliquer (absence de décision d'adéquation, absence de mécanismes offrant des garanties appropriées, inapplicabilité des exceptions de l'article 49 du RGPD), le règlement prévoit qu'un transfert de données peut être mis en œuvre si les conditions suivantes sont cumulativement remplies :

- Absence de caractère répétitif,

- Nombre limité de personnes concernées,
- Nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable de traitement sur lesquels ne prévalent pas les intérêts ou droits et libertés des personnes concernées,
- Evaluation par le responsable de traitement de toutes les circonstances entourant le transfert et des garanties appropriées prises sur la base de cette évaluation,
- Information de l'autorité de contrôle,
- Information de la personne concernée, notamment sur le transfert et les intérêts légitimes impérieux poursuivis.

ATTENTION

Dans la mesure où ces dérogations peuvent faire l'objet d'une interprétation restrictive par les autorités de contrôle, il convient au responsable du traitement de se montrer prudent dans leur recours à l'une de ces dernières pour fonder un transfert. En outre, lorsqu'il n'existe pas de décision d'adéquation, le droit de l'Union européenne ou d'un Etat membre peut fixer des limites aux transferts vers des Etats non membre de l'UE ou des organisations internationales.

Quelles mesures concrètes mettre en œuvre ?

Afin de remplir son obligation de documentation à cet égard, il est conseillé au responsable de traitement, outre de s'assurer que le traitement mis en œuvre repose sur l'une des exceptions dudit article, de conserver les modèles de recueil du consentement (par tout moyen : écrit, numérique, enregistrement oral, etc.). Lorsque le traitement a pour fondement « l'intérêt légitime », il faudra vérifier et documenter l'équilibre entre l'intérêt légitime invoqué par le responsable de traitement et les droits des personnes concernées.

- Mettre en place une politique de durée de conservation claire des données – voir I.A.1.e ci-dessus

- Documenter le fondement légal du traitement

Pour être licite, le traitement doit être fondé sur l'une des exceptions de l'article 6 du RGPD (voir I.A.2 ci-dessus).

- Informer les personnes

Au moment de la collecte des données, certaines informations doivent être données aux personnes concernées (voir I.B ci-dessus).

En pratique, la preuve que les obligations relatives aux droits des personnes sont bien respectées peut être notamment rapportée au moyen des actions suivantes : rédaction et mise à disposition des autorités de la politique de confidentialité à destination des personnes concernées ainsi que de tous documents à destination des salariés et imposant à ces derniers de traiter les données collectées en conformité avec le RGPD (charte informatique annexée au règlement intérieur, circulaires d'information relatives à la collecte des données communiquées, emails, informations présentes sur les panneaux d'affichage présents au sein de l'entreprise, etc.).

- Encadrer la sous-traitance - Article 28 du RGPD

Le règlement impose la conclusion d'un contrat écrit entre le responsable de traitement et son sous-traitant.

En plus des informations relatives au traitement en lui-même (finalité, objet, durée, etc.), le contrat doit prévoir que le sous-traitant s'engage à : n'agir que sur instructions documentée du responsable de traitement, assurer la confidentialité et la sécurité des données, obtenir une autorisation en cas de sous-traitance à un autre prestataire, etc.

- Réaliser des audits réguliers

Il est conseillé de mettre en œuvre des procédures de vérifications (audit des outils et des sous-traitants) pour s'assurer de la réalité et de

l'efficacité des mesures prises ainsi que pour identifier, le cas échéant, les éventuels manquements afin de prendre les mesures de corrections adéquates.

- Appliquer des codes de conduites et certifications – Articles 40 à 43 du RGPD

Le RGPD indique que l'adhésion et l'application d'un code de conduite ainsi que les certifications sont des outils de preuve de la conformité et constituent une « circonstances atténuantes » à prendre en compte par les autorités de contrôle en cas de décision de sanction.
S'il n'existe pas de « certification RGPD », la CNIL propose **plusieurs labels** (« Gouvernance Informatique & Libertés », « Formation », « coffre-fort numérique ») et a récemment publié une **mise à jour des labels de formation et gouvernance prenant en compte les exigences du RGPD**.

- Rendez-vous sur le site de la CNIL pour en savoir plus sur la **procédure d'obtention d'un label CNIL**

Le RGPD prévoit enfin la possibilité pour l'autorité en charge de contrôler la bonne application du règlement, de prononcer des amendes administratives en cas de manquement (III).

III. LES POUVOIRS D'ENQUÊTE ET DE SANCTION DE L'AUTORITÉ DE CONTRÔLE EN CAS DE NON-RESPECT DES DISPOSITIONS DU RÈGLEMENT

Afin de mener à bien sa mission, l'autorité de contrôle dispose de pouvoirs d'enquêtes (1) ainsi que de la possibilité de sanctionner financièrement les personnes qui ne respecteraient pas les dispositions du règlement (2).

1. Les pouvoirs d'enquête de l'autorité de contrôle

L'autorité de contrôle peut, de sa propre initiative ou suite à une réclamation adressée par une personne concernée, procéder à une enquête et notamment :

- Auditer les mesures de protection des données,
- Examiner les éventuelles certifications délivrées,
- Se faire communiquer toute information nécessaire à la réalisation de sa mission,
- Accéder aux données à caractère personnel collectées et traitées,
- Accéder aux locaux, aux installations et aux moyens de traitement,
- Notifier les violations alléguées du règlement.

Suite à son enquête, l'autorité peut adopter l'une des mesures suivantes :

Avertissement	Pouvoir de prononcer un avertissement sur le fait que les opérations de traitements envisagées sont susceptibles d'une violation de règlement.
Rappel à l'ordre	Pouvoir de prononcer un rappel à l'ordre en cas de violation du règlement.

Mise en conformité	Pouvoir d'ordonner une mise en conformité avec le règlement des opérations de traitement (le cas échéant, d'une manière particulière et dans un délai déterminé).
Respect des droits des personnes	- Pouvoir d'ordonner de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, - Pouvoir d'ordonner de communiquer à la personne concernée, une notification de violation de données, - Pouvoir d'ordonner la rectification ou l'effacement des données, ou la limitation du traitement conformément au règlement, et la notification de ces mesures aux destinataires auxquels les données ont été divulguées.
Limitation	Pouvoir d'imposer une limitation (temporaire ou définitive), y compris une interdiction du traitement.
Retrait / refus de certification	Pouvoir de retirer une certification, de demander à l'organisme de certification de retirer ou de ne pas délivrer une telle certification si les conditions requises ne sont pas ou plus satisfaites.
Suspension des flux	Pouvoir d'ordonner la suspension des flux de données adressées à un destinataire situé hors UE ou à une organisation internationale.

En complément ou à la place de ces mesures, l'autorité peut également prononcer des amendes administratives.

2. Le pouvoir de sanction de l'autorité de contrôle

L'**article 83** du RGPD distingue deux montants de sanctions différentes selon la catégorie de l'atteinte :

Sanction	Type de violation
Jusqu'à 10 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2% du CA annuel mondial total de l'exercice précédent	- Non-respect des principes de Privacy « by design » et « by default », - Non-tenue du registre des activités de traitement (lorsqu'il est obligatoire), - Absence de notification à l'autorité de contrôle ou à la personne concernée d'une violation de données à caractère personnel, - Insuffisance, inadéquation ou absence de mesures de sécurité des données, - Non-réalisation de l'analyse d'impact lorsqu'elle est nécessaire, - Absence d'encadrement contractuel des relations entre les responsables conjoints de traitement ou avec les sous-traitants, - Non-désignation d'un DPO lorsqu'une telle désignation est obligatoire, Etc.

Jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4% du CA annuel mondial total de l'exercice précédent	- Non-respect des principes applicables aux traitements de données (transparence, loyauté, etc. voir I ci-dessus), - Non-respect des conditions de licéité du traitement (voir II ci-dessus), - Non-respect des droits des personnes concernées (information, accès, rectification, etc. voir I.1 ci-dessus), - Non-respect d'une injonction prononcée par l'autorité de contrôle, Etc.

En outre, l'autorité de contrôle dispose de la possibilité d'introduire une action en justice.

De même, les personnes concernées disposent d'un droit à un recours juridictionnel si elles considèrent que les droits conférés par le règlement ont été violés par un traitement de données.

Le recours juridictionnel pouvant être exercé par les personnes concernées n'exclut pas la réclamation auprès de l'autorité de contrôle, et inversement.

ATTENTION

Le règlement prévoit que les Etats membres pourront déterminer le régime d'autres sanctions en cas de violation du règlement et notamment la possibilité de déterminer le régime de sanctions pénales.