MALLETTE DU DIRIGEANT 2019
MODULE 7

Protection des données personnelles - RGPD

MARS 2019

SOMMAIRE

I - COMPRENDRE LE RGPD

DÉFINIR LES DONNÉES À CARACTÈRE PERSONNEL

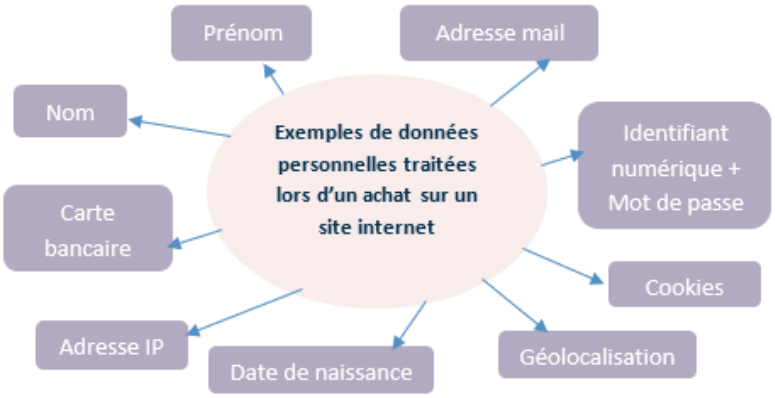
Une donnée à caractère personnel, c'est quoi ?
C'est toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement.
Par exemple : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc.

Peu importe que ces informations soient confidentielles ou publiques.

A noter : pour que ces données ne soient plus considérées comme personnelles, elles doivent être rendues anonymes de manière à rendre impossible toute identification de la personne concernée : noms masqués, visages floutés, etc.

Attention : s'il est possible par recoupement de plusieurs informations (âge, sexe, ville, diplôme, etc.) ou par l'utilisation de moyens techniques divers, d'identifier une personne, les données sont toujours considérées comme personnelles.

Exemple :



NÉCESSITÉ DE PROTÉGER LES DONNÉES PERSONNELS

Collecter et traiter des données personnelles implique avant tout d'informer les personnes sur ce que vous faites de leurs données et de respecter leurs droits. En tant que responsable d'un traitement de données, ou en tant que sous-traitant, vous devez prendre des mesures pour garantir une utilisation de ces données respectueuse de la vie privée des personnes concernées.

Les responsables de traitement et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement.

Les autorités de protection peuvent notamment :

- Prononcer un avertissement ;
- Mettre en demeure l'entreprise ;
- Limiter temporairement ou définitivement un traitement ;
- Suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- Ordonner la rectification, la limitation ou l'effacement des données.

OBJECTIFS ET PÉRIMÈTRE DU RGPD

Le GDPR (ou RGPD) est le nouveau règlement européen sur la protection des données. Il entrera en application en 2018 et impactera toutes les entreprises opérant du traitement de données à caractère personnel sur des résidents européens.

Le RGPD poursuit plusieurs objectifs :

- Uniformiser au niveau européen la réglementation sur la protection des données.
- Responsabiliser davantage les entreprises en développant l'auto-contrôle.
- Renforcer le droit des personnes (droit à l'accès, droit à l'oubli, droit à la portabilité, etc.).

Le périmètre d'application du RGPD

Les règles et obligations du RGPD s'appliquent au traitement – automatisé ou non – des données à caractère personnel. L'objectif du RGPD est de renforcer l'encadrement des pratiques en matière de collecte et d'utilisation des données à caractère personnel.

La RGPD donne une définition précise des « données à caractère personnel » (DCP) : il s'agit de « toute information se rapportant à une personne physique identifiée ou identifiable ». Par personne physique identifiable, il faut comprendre « une 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 ».

Le RGPD concerne uniquement la protection des données personnelles rattachées à des personnes physiques. Ce qui signifie que la **RGPD ne s'applique pas aux entreprises ne traitant que des données relatives à des personnes morales, sauf si celles-ci sont amenées à collecter des données sur des représentants des personnes morales** (ce qui, dans les faits, est presque toujours le cas…).

Pour bien comprendre : la collecte de données sur des représentants d'une entreprise (à partir de cartes de visite par exemple) entre dans le champ d'application du RGPD. En revanche, la collecte d'informations sur l'entreprise (dénomination sociale, objet social, numéro de TVA, SIRET, etc.) en est exclue.

Le « traitement des données », au sens du RGPD, fait référence à la collecte, à l'accès, au stockage, à la manipulation, à la destruction et à la consultation à distance des données. Concrètement, une entreprise qui délègue à un prestataire la collecte et le stockage des données fait néanmoins du traitement de données dans la mesure où elle les consulte. **Au final, l'immense majorité des entreprises est concernée par les dispositions du RGPD.**

ENTREPRISES ET TYPES DE DONNÉES CONCERNÉES

Le principe de co-responsabilité

Le respect des règles en matière de protection des données à caractère personnel n'incombe pas qu'aux seuls responsables du traitement. Les sous-traitants, auxquels les entreprises ont de plus en plus recours, doivent également s'y tenir. Le règlement définit le sous-traitant comme une personne ou une entité publique ou privée qui gère les données à caractère personnel pour le compte de celui qui se présente comme le responsable du traitement.
Il doit présenter des « garanties suffisantes » quant aux moyens techniques et organisationnels mis en œuvre dans le traitement des données. Si le sous-traitant décide à son tour de recruter un autre sous-traitant, il lui faudra obtenir l'autorisation écrite préalable du responsable du traitement.

En cas de manquement à ses obligations, la responsabilité du sous-traitant pourra être engagée. Le montant des amendes est très élevé. Il peut fragiliser la santé financière et la réputation d'une entreprise.

Toutes les organisations réalisant des traitements de données à caractère personnel
Toutes les organisations réalisant des traitements de données à caractère personnel de citoyens européens sont concernées par le RGPD, quelle que soit leur localisation. Pour rappel, on entend par données personnelles « toute information se rapportant à une personne physique identifiée ou identifiable. » Les exemples les plus proches : nom, adresse, adresse IP, identifiant, matricule, N° tél…

La notion de données personnelle recouvre un champ très vaste, et rares sont les organisations qui ne manipulent pas ce type de données. Ainsi, une entreprise qui manipulera les données de son personnel ou qui recueillera des informations sur ses clients sera soumise au RGPD, **y compris les entreprises en BtoB** (données de 'contacts' par exemple).

Le secteur d'activité n'a pas d'importance
Le traitement de données personnelles rassemble diverses notions : collecte de données, stockage, analyse… Et le secteur d'activité de l'entreprise ne compte pas, à partir du moment où une entreprise manipule des données à caractère personnel d'un citoyen européen, elle sera soumise au RGPD, et ce même si ce type de traitement ne constitue qu'une activité secondaire. Les sous-traitants sont également concernés au même titre.

Les petites entreprises comme les grandes
Le respect du RGPD est également obligatoire, quelle que soit la taille de l'entreprise. Il existe cependant un allègement pour les entreprises employant moins de 250 personnes. Pour ces entreprises, la tenue d'un registre des activités de traitement n'est pas obligatoire.

Mais cette exception ne s'appliquera pas :

- Si l'entreprise en question réalise de manière systématique des traitements présentant des risques importants pour les droits et libertés des personnes concernées ;
- Si le traitement porte sur les données décrites au paragraphe 1 de l'article 9 du RGPD : origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques, données biométriques, données sur la santé, données sur la vie sexuelle ;
- Si le traitement porte sur des informations relatives à des condamnations pénales ou à des infractions.
- Ou si l'entreprise opère des traitements récurrents ou non occasionnels (ex : paie !)

Les entités publiques sont aussi concernées
Le Règlement Général sur la Protection des Données ne concerne pas que les entreprises privées. Les institutions publiques, de l'hôpital à la collectivité territoriale, doivent aussi s'y soumettre. Du fait du déploiement de l'e-administration, étape indispensable de la modernisation de la vie publique, les entités disposent d'un nombre croissant de données personnelles.

Dans les établissements scolaires, par exemple, le règlement exige un contrôle très strict de l'utilisation des données et garantit le respect d'un certain nombre de droits, comme celui à la suppression des données si l'élève part de l'établissement, celui à la portabilité des données ou le droit à la rectification.

ENJEUX ET IMPACTS POUR L'ENTREPRISE

Le RGPD peut être vécu comme une contrainte. Comment transformer ce règlement sur les données personnelles en opportunité quand on est une PME ?

Exécutoire depuis le 1ER JANVIER 2019 , le Règlement Général sur la Protection des Données (RGPD) renforce les droits des citoyens et accentue les obligations des entreprises. Pour de nombreuses PME, c'est une contrainte supplémentaire. Ce texte représente pourtant une occasion de renforcer la pérennité de son activité.

Des Obligations pour les entreprises
Pour les entreprises, le RGPD oblige à prendre des « mesures techniques et organisationnelles appropriées ». Cela commence par cartographier l'intégralité de son réseau informatique afin d'identifier tous les supports stockant ce genre d'informations.

Il convient également de :

- **Tenir un registre des traitements** : ce document dresse l'inventaire de chaque traitement effectué sur une donnée personnelle. Il indique aussi les coordonnées du responsable de traitement, les mesures de sécurité mises en place…
- **Informer la CNIL sous 72 heures dès qu'un piratage** du réseau informatique entraîne une fuite de données à caractère personnel;
- **Mettre en conformité son site web et tous ses contrats** (travail, charte informatique, prestataires).
- **S'assurer justement que ses prestataires** (experts-comptables, hébergeurs de données….) ont entamé une démarche de mise en conformité. Le RGPD précise en effet qu'il y a une coresponsabilité entre le chef d'entreprise et son sous-traitant.

Reste la question du DPO (Data protection Officer ou DPD pour Délégué à la protection des données). Il doit veiller à la mise en conformité de tous les traitements. S'il est obligatoire pour les entreprises traitant de données à grande échelle ou à risque et pour les administrations, il ne l'est pas pour les TPE. **Mais la nomination d'un DPO externe (mutualisé entre différentes petites entités) prouve aux yeux de la CNIL que l'entreprise se soucie de la protection de ces informations.**

La majorité des entreprises n'a pas anticipé l'arrivée de ce règlement qui apparaît comme un obstacle insurmontable, car il touche un grand nombre de métiers : RH, comptabilité, juridique, commercial et bien sûr service informatique. « Des PME et TPE le considèrent comme inutile alors qu'elles ne se rendent pas compte des impacts négatifs que peut avoir la négligence de la protection de ces informations », constate Mohamed HASSEN, conseiller en développement Technologique et Innovation à la CCI Nord Isère.

Quelles Opportunités pour les PME

On dit que « la donnée » est l'or du 21ème siècle. Le RGPD est une formidable opportunité pour les PME de connaitre précisément les flux de données dans l'entreprise.
Cette connaissance approfondie, permet de structurer l'activité autour de ce nouvel actif et de sécuriser les informations dans l'entreprise en détectant les failles et les risques.
Travailler sur les données dans l'entreprise permet aussi d'améliorer la connaissance et l'expérience client. Les questions telles que « qui sont mes clients », « comment se comportent-ils », « comment ces données peuvent-elles m'aider à améliorer le service rendu ? » sont autant de clés pour faire grandir l'entreprise vers une approche « customer centric ».

Au final, le RGPD oblige « les entreprises à revoir leurs méthodes de traitement des données et de façon plus globale à améliorer leur niveau de sécurité informatique »

IMPACTS SUR LES SYSTÈME D'INFORMATION DES ENTREPRISES

D'un point de vue logiciel et matériel, les changements éventuels sembles plutôt mineurs pour le traitement global des données. **Les modifications profondes concernent surtout le recueil et la conservation/sécurisation des données.**

Votre organisation devra être en mesure de **justifier de l'accord préalable d'une personne** – le opt-in – au recueil des données la concernant. Ensuite, les modalités de conservation des données devront se faire par le biais de **solutions cryptées et hyper-sécurisées** en interne ou dans un datacenter : un véritable coffre-fort électronique. Les entreprises auront l'obligation de veiller à l'intégrité de ce dernier. **Les questions de sécurisation seront sans conteste le point crucial** de la mise en conformité des organisations. Plusieurs niveaux de supervision et de contrôle devront être renforcés sur le plan logiciel : dans un environnement connecté en permanence la surveillance doit être constante.

Les éditeurs de solutions ont déjà intégré ces questions et des mises à jour sont prévues en conséquences. Néanmoins de plus en plus de sociétés font appel à des auditeurs et cabinets de conseil afin d'anticiper leur besoins, notamment pour les questions liées à la sécurité des données. Si la majorité des technologies de cryptage et de sécurisation des informations existe déjà, leur implémentation dans les systèmes et processus métiers en place constitue dès à présent un défi. Tout ou partie d'un ERP par exemple, doit s'adapter à ces nouvelles contraintes.

Viennent ensuite les **services client et/ou marketing** qui sont en première ligne pour la collecte d'informations personnelles. Ces opérationnels vont devoir être formés aux évolutions de leurs outils métiers. De plus, ils vont devoir intégrer les conséquences liées à la conservation limitée dans le temps des données récoltées et à leur anonymisation une fois archivées.

II - COMPRENDRE LES NOUVEAUX PRINCIPES DE PROTECTION DES DONNÉES

LES NOUVELLES DÉFINITIONS INTRODUITES PAR LE RÈGLEMENT EUROPÉEN

Le texte adopté est un règlement européen, ce qui signifie que, contrairement à une directive, il est **directement applicable dans l'ensemble de l'Union** sans nécessiter de transposition dans les différents États membres. Le même texte s'applique donc à partir du 25 mai 2018 dans toute l'Union. Dès lors, les traitements déjà mis en œuvre à cette date doivent d'ici là être mis en conformité avec les dispositions du règlement.

Un champ d'application étendu

Le critère du ciblage
Le règlement s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler » (en anglais monitor).

En pratique, le droit européen s'applique chaque fois qu'un résident européen est directement visé par un traitement de données, y compris par Internet.

La responsabilité des sous-traitants
Par ailleurs, alors que le droit de la protection des données actuel concerne essentiellement les « responsables de traitements », c'est-à-dire les organismes qui déterminent les finalités et les modalités de traitement de données personnelles, le règlement étend aux sous-traitants une large partie des obligations imposées aux responsables de traitement.

Un guichet unique : le « one stop shop »

Les entreprises sont désormais en contact avec un « guichet unique », à savoir l'autorité de protection des données de l'État membre où se trouve leur « établissement principal », désignée comme l'autorité « chef de file ». Cet établissement est soit le lieu de leur siège central dans l'Union, soit l'établissement au sein duquel sont prises les décisions relatives aux finalités et aux modalités du traitement. Les entreprises bénéficient ainsi d'un interlocuteur unique pour l'Union européenne en matière de protection des données personnelles, lorsqu'elles mettent en œuvre des traitements transnationaux.

Une coopération renforcée entre autorités pour les traitements transnationaux

Toutefois, dès lors qu'un traitement est transfrontalier – donc qu'il concerne les citoyens de plusieurs États membres –, les autorités de protection des données des différents États concernées sont juridiquement compétentes pour s'assurer de la conformité des traitements de données mis en œuvre.

Afin d'assurer une réponse unique pour l'ensemble du territoire de l'Union, l'autorité « chef de file » coopère avec les autres autorités de protection des données concernées dans le cadre d'opérations conjointes. Les décisions sont adoptées conjointement par l'ensemble des autorités concernées, notamment en termes de sanctions.

Les autorités de protection nationales sont réunies au sein d'un Comité européen de la protection des données (CEPD), qui veille à l'application uniforme du droit sur la protection des données. Il remplace l'ancien G29.

En pratique, l'autorité « chef de file » propose les mesures ou décisions (constatant la conformité d'un traitement ou proposant une sanction, par exemple). Les autorités européennes concernées par le traitement disposent alors d'un délai de quatre semaines pour approuver cette décision ou, au contraire, soulever une objection. Si l'objection n'est pas suivie, la question est portée devant le CEPD qui rend alors un avis. Cet avis est contraignant et doit donc être suivi par l'autorité « chef de file ».

Que le CEPD soit ou non saisi, l'autorité « chef de file » porte la décision ainsi partagée par ses homologues. Il y a donc une décision conjointe, susceptible de recours devant le juge des décisions de l'autorité « chef de file ».

Par exemple, dans le cas d'une entreprise dont l'établissement principal est en France, la CNIL est le guichet unique de cette entreprise et lui notifie les décisions adoptées dans le cadre de ce mécanisme de cohérence. Ses décisions sont ensuite, si elles sont défavorables, susceptibles de recours devant le Conseil d'État.

Ce mécanisme permet ainsi aux autorités de protection des données de se prononcer rapidement sur la conformité d'un traitement ou sur un manquement au règlement et garantit une sécurité juridique élevée aux entreprises en leur assurant une réponse unique sur l'ensemble du territoire de l'Union.

NOUVEAUX DROITS POUR LES PERSONNES CONCERNÉES

Le règlement européen renforce les droits des personnes et facilite l'exercice de ceux-ci.

Consentement renforcé et transparence

Le règlement impose la mise à disposition d'une information claire, intelligible et aisément accessible aux personnes concernées par les traitements de données.
L'expression du consentement est définie : les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambigüe.

De nouveaux droits

Le droit à la portabilité des données : ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers. Il s'agit ici de redonner aux personnes la maîtrise de leurs données, et de compenser en partie l'asymétrie entre le responsable de traitement et la personne concernée.

Des conditions particulières pour le traitement des données des enfants : Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les mineurs de moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Les États membres peuvent abaisser cet âge par la loi, sans toutefois qu'il puisse être inférieur à 13 ans.

En France par exemple, l'âge retenu est de 15 ans. En deçà, la loi française prévoit que le consentement conjoint de l'enfant et du titulaire de l'autorité parentale doit être recueilli.

Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

Introduction du principe des actions collectives : Tout comme pour la législation relative à la protection des consommateurs, les associations actives dans le domaine de la protection des droits et libertés des personnes en matière de protection des données ont la possibilité d'introduire des recours collectifs en matière de protection des données personnelles.

Un droit à réparation des dommages matériel ou moral : Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

RISQUES JURIDIQUES ET SANCTIONS QUI PÈSENT

Des sanctions encadrées, graduées et renforcées

Les responsables de traitement et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement.

Les autorités de protection peuvent notamment :

- Prononcer un avertissement ;
- Mettre en demeure l'entreprise ;
- Limiter temporairement ou définitivement un traitement ;
- Suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- Ordonner la rectification, la limitation ou l'effacement des données.

S'agissant des nouveaux outils de conformité qui peuvent être utilisés par les entreprises, l'autorité peut retirer la certification délivrée ou ordonner à l'organisme de certification de retirer la certification.

S'agissant des amendes administratives, elles peuvent s'élever, selon la catégorie de l'infraction, de 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, **de 2% jusqu'à 4% du chiffre d'affaires annuel mondial**, le montant le plus élevé étant retenu.

Ce montant doit être rapporté au fait que, pour les traitements transnationaux, la sanction sera conjointement adoptée entre l'ensemble des autorités concernées, donc potentiellement pour le territoire de toute l'Union européenne.

Dans ce cas, une seule et même décision de sanction décidée par plusieurs autorités de protection sera infligée à l'entreprise.

NOUVELLES OBLIGATIONS POUR LE RESPONSABLE DES TRAITEMENTS ET LES SOUS-TRAITANTS

Une conformité basée sur la transparence et la responsabilisation

Alors que la directive de 1995 reposait en grande partie sur la notion de « formalités préalables » (déclaration, autorisations), le règlement européen repose sur une logique de conformité, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement du régulateur.

Une clé de lecture : la protection des données dès la conception et par défaut (privacy by design)

Les responsables de traitements doivent mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut. **Concrètement, ils doivent veiller à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »).**

Un allègement des formalités administratives et une responsabilisation des acteurs

Afin d'assurer une protection optimale des données personnelles qu'ils traitent de manière continue, les responsables de traitements et les sous-traitants devront mettre en place des mesures de protection des données appropriées et démontrer cette conformité à tout moment (accountability).

La conséquence de cette responsabilisation des acteurs est la suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes. Quant aux traitements soumis actuellement à autorisation, le régime d'autorisation est maintenu dans certains cas par le droit national (par exemple en matière de santé) ou est remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

De nouveaux outils de conformité :

- la tenue d'un registre des traitements mis en œuvre
- la notification de failles de sécurité (aux autorités et personnes concernées)
- la certification de traitements
- l'adhésion à des codes de conduites
- le DPO (délégué à la protection des données)
- les analyses d'impact relatives à la protection des données (AIPD)

Les « analyses d'impact relatives à la protection des données » (AIPD ou PIA)

Pour tous les traitements à risque, le responsable de traitement devra conduire une analyse d'impact complète, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Concrètement, il s'agit notamment des traitements de données sensibles (données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi, fait nouveau, les données génétiques ou biométriques), et de traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire notamment de profilage.

En cas de risque élevé, il devra consulter l'autorité de protection des données avant de mettre en œuvre ce traitement. Les « CNIL » pourront s'opposer au traitement à la lumière de ses caractéristiques et conséquences.

Une obligation de sécurité et de notification des violations de données personnelles pour tous les responsables de traitements

Les données personnelles doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées.

Lorsqu'il constate une violation de données à caractère personnel, le responsable de traitement doit notifier à l'autorité de protection des données la violation dans les 72 heures. L'information des personnes concernées est requise si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne.

Le Délégué à la Protection des données (Data Protection Officer)

Les responsables de traitement et les sous-traitants devront obligatoirement désigner un délégué :

- s'ils appartiennent au secteur public,

- si leurs activités principales les amène à réaliser un suivi régulier et systématique des personnes à grande échelle,

- si leurs activités principales les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

En dehors de ces cas, la désignation d'un délégué à la protection des données sera bien sûr possible.
Les responsables de traitement peuvent opter pour un délégué à la protection des données mutualisé ou externe.

Le délégué devient le véritable « chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. Il est ainsi chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que ses employés ;
- de contrôler le respect du règlement européen et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact (AIPD) et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci

NOUVELLES RÈGLES DE GESTION POUR LA CYBERSÉCURITÉ

Implicitement, ce règlement impose de mettre en place une politique de sécurité globale. L'objectif prioritaire est d'assurer la confidentialité, l'anonymisation, l'intégrité et la disponibilité de ce type d'information sensible.

Pour les entreprises, il s'agit de contraintes fortes. Mais le RGPD doit être l'occasion d'établir une cartographie précise des lieux de stockage de ce type d'informations et de s'appuyer sur des solutions mieux adaptées. Il s'agit notamment du Cloud. La protection des données étant une problématique complexe, « de nombreuses entreprises choisissent d'externaliser certains services ou de les migrer dans le Cloud », déclare Philippe Trouchaud, Associé responsable du département de cybersécurité de PwC.

Mais attention, déléguer la protection de ce type d'informations à un fournisseur dans le Cloud n'exonère pas les entreprises de mettre en place des outils de sécurité visant à contrôler, au niveau local, les accès à ces dossiers sensibles. En droit, elles en sont propriétaires. Même si elles les confient à des prestataires, c'est leur responsabilité qui sera en jeu.

Concrètement, comment faire ?

Les bonnes questions à se poser :

1 - Quels pourraient être les impacts sur les personnes concernées en cas :
- d'accès illégitime ?
- de modification non désirée ?
- de disparition ?

2 - Est-ce grave ?
3 - Comment chacun de ces scénarios pourrait-il arriver ?
4 - Est-ce vraisemblable ?
5 - Quelles mesures (de prévention, de protection, de détection, de réaction…) devrait-on prévoir pour réduire ces risques à un niveau acceptable ?

Le catalogue de bonnes pratiques aide à déterminer des mesures proportionnées aux risques identifiés, en agissant sur :

1 - les «éléments à protéger» : minimiser les données, chiffrer, anonymiser, permettre l'exercice des droits…
2 - les «impacts potentiels» : sauvegarder les données, tracer l'activité, gérer les violations de données…
3 - les «sources de risques» : contrôler les accès, gérer les tiers, lutter contre les codes malveillants…
4 - les «supports» : réduire les vulnérabilités des matériels, logiciels, réseaux, documents papier…

Pour traiter un risque identifié et le réduire à un niveau acceptable, l'utilisateur des guides peut sélectionner une ou plusieurs mesures appropriées.

III - DÉFINIR UN PLAN D'ACTIONS POUR SE METTRE EN CONFORMITÉ

GOUVERNANCE DES DONNÉES, RÔLES ET RESPONSABILITÉS

Le règlement européen sur la protection des données vise à responsabiliser les acteurs des traitements de données en uniformisant les obligations pesant sur les responsables de traitements et les sous-traitants.

Le représentant légal
C'est le point de contact de l'autorité. Il a mandat pour « être consulté en complément ou à la place du responsables de traitement sur toutes les questions relatives aux traitements »

Le sous-traitant
Le sous-traitant est tenu de respecter des obligations spécifiques en matière de sécurité, de confidentialité et en matière d'accountability. Il a notamment une obligation de conseil auprès du responsables de traitement pour la conformité à certaines obligations du règlement (PIA, failles, sécurité, destruction des données, contribution aux audits)

Il est tenu de maintenir un registre et de désigner un DPO dans les mêmes conditions qu'un responsable de traitement.

LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

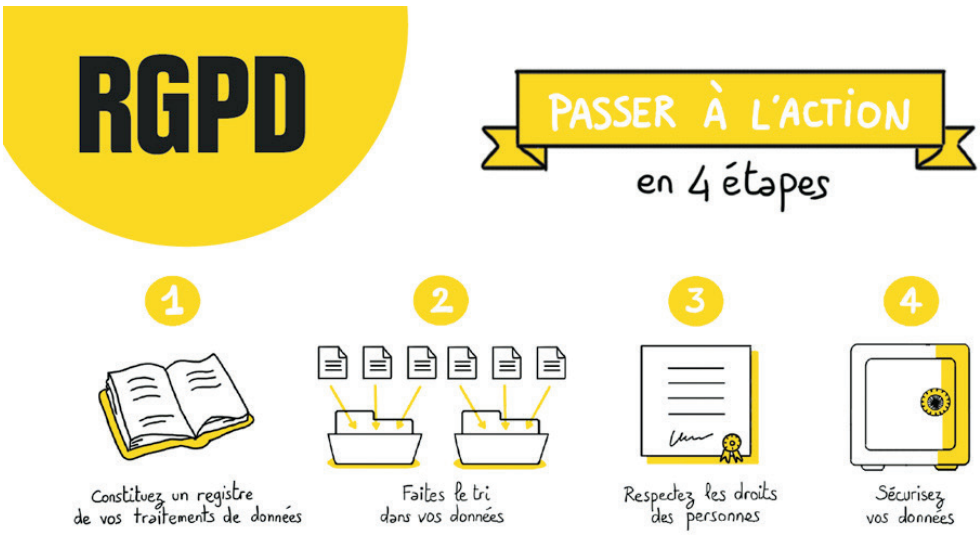
Pour vous aider à informer les personnes dans des conditions conformes au RGPD, voici quelques exemples pratiques de mentions d'information.

Il s'agit d'illustrations de base, à adapter ou compléter, et non de modèles de mentions valables dans toutes les hypothèses.

Vous pouvez trouver l'ensemble de ces exemples sur le site de la CNIL : https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation

Voici un exemple concret a consulter : https://www.inria.fr/informations-pratiques/donnees-personnelles

LES ACTIONS À PRÉVOIR POUR SE METTRE EN CONFORMITÉ



1. Constituer un registre

Un exemple de registre peut être téléchargé sur le site de la Cnil :
https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf

2. Structurez vos bases de données et documentez-les

Lorsqu'on parle de données collectées, on parle en premier lieu du nom, prénom, téléphone, email, adresse, date de naissance… Mais il ne faut pas oublier également les données bancaires collectées sur les sites e-commerce, les données personnelles collectées lorsqu'on s'inscrit à un événement, mais aussi les données de géolocalisation… Toutes les données qui parlent des internautes et de leurs habitudes de vie sont concernées.

Dès lors que vous récoltez des données, vous devez les organiser en tenant compte des points suivants :

- **L'objectif** (ex. la fidélisation client, la demande d'information, le recrutement) ;

- **Les catégories de données** (ex. Service commercial : nom, prénom, téléphone, email professionnel, société)

- **Qui a accès aux données** (ex. Service commercial, service informatique, direction, prestataires, partenaires, hébergeurs) ;

- **La durée de conservation de ces données** (durée durant laquelle ces données sont utiles). La loi vous oblige donc à créer des registres structurés, par service, avec les éléments mentionnés ci-dessus. Une personne de votre société doit d'ailleurs être désignée responsable des données.

3. Communiquez et informez vos clients/prospects

L'objectif de ce règlement est aussi d'apporter plus de transparence à l'utilisateur final. La confiance entre votre entreprise et vos clients et/ou salariés dont vous possédez les données est primordiale. Pour chaque donnée collectée, il sera donc important d'expliquer comment vous allez l'utilisez.

Exemple :
Vous proposez l'inscription à une newsletter : vous devez ajouter une case à cocher précisant que l'internaute qui dépose son email ne recevra rien d'autre que ce pour quoi il s'est inscrit et pourra se désinscrire à tout moment. Mais vous devez également ajouter un texte mentionnant l'usage qui sera fait de ces données (voir les modèles de mentions de la CNIL)

Une des bases de cette loi est également de donner un droit de regard à l'internaute sur la modification ou la suppression de ces données.
Ajoutez donc un lien à vos newsletters permettant de se désabonner ou de supprimer ses données de votre base. L'internaute doit également pouvoir vous contacter pour vous demander de supprimer ou modifier ses données.

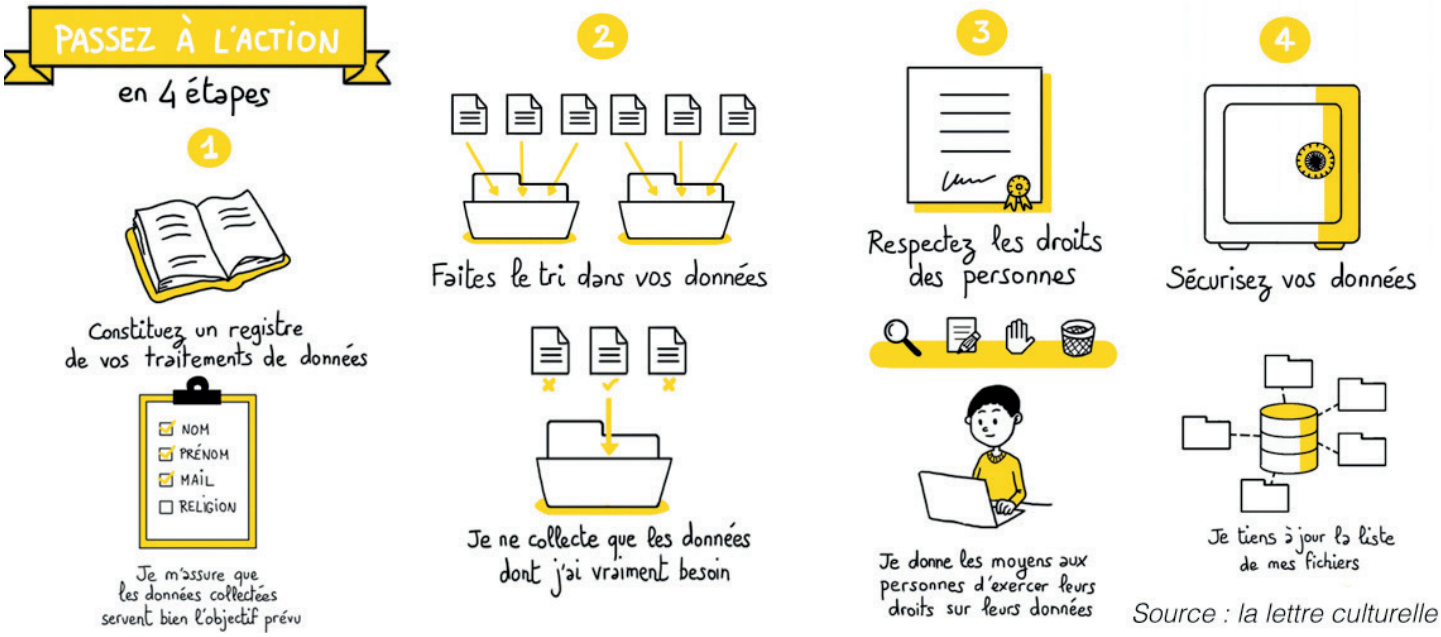
4. Sécurisez les données

On l'a constaté avec des exemples récents touchant des sites internet de renoms, la sécurité n'est pas toujours assurée et parfois, certains sites se font pirater leurs données au détriment de millions d'internautes.
Des réflexes de sécurité doivent être mis en place au sein de votre entreprise :

- Changez vos mots de passes régulièrement,
- Mettez à jour votre site, votre blog et vos différents logiciels,
- Chiffrez vos données si c'est possible.

Exemple donné par la CNIL :
Vous êtes restaurateur et vous livrez à domicile. Vos clients vous communiquent leur adresse précise et le code d'entrée de leur immeuble. Si ces informations sont piratées ou perdues, elles peuvent être utilisées pour s'introduire frauduleusement au domicile de votre client. Conséquence désastreuse pour vos clients, mais aussi pour vous !

LA DÉMARCHE POUR METTRE EN ŒUVRE LE PLAN D'ACTION



Source : la lettre culturelle

Les 6 étapes préconisées par la CNIL

SOURCE CNIL : https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

1) Choisir un DPO.

Il apparaît comme pertinent d'accompagner ses équipes et de désigner un "pilote" de la gouvernance des données personnelles de votre entreprise. Il doit vérifier la conformité de son organisation avec le RGPD par l'identification des actions de traitement réalisées, l'analyse et la vérification de leur conformité. Véritable conseiller de votre mise en conformité ses recommandations vous guideront dans la jungle du RGPD ! La nomination d'un DPO, n'est pas obligatoire pour toutes les entreprises mais elle est fortement conseillée. Etant un poste inédit, il peut être difficile de trouver un interlocuteur qualifié sur le marché de l'emploi. Recrutement en interne ou externalisation? Fonction à mi-temps ou à plein temps ? Embauche ou mutualisation ? Autant de questions qu'il va falloir vous poser !

Malgré son rôle central dans la stratégie de mise en conformité d'une entreprise, le DPO n'est cependant pas légalement responsable de la conformité de son entreprise. C'est elle seule qui prend la décision d'appliquer ou non ses recommandations !

2) Cartographiez vos données

Avant d'engager une refonte de ses processus, une étape clé va être de recenser tous les traitements de données actuels dans l'entreprise. Le but : dresser un registre des traitements pour être en mesure d'identifier et de quantifier l'impact du RGPD.

L'article 4 du règlement définit un taitement comme «toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des 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 communicationpar transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction».

Le registre doit englober les différents traitements de données personnelles, les différentes catégories de données traitées, les objectifs de chaque opération de traitement, les différents acteurs qui traitent ces données et les différents flux d'origine et destination des données. Vous serez ainsi en mesure d'identifier les zones de risques et de mettre en place des actions correctives.

3) Élaborez votre plan d'action

Vous possédez maintenant un état des lieux complet sur lequel vous appuyer pour développer votre plan d'action ! Voici quelques étapes essentielles à votre transition vers la conformité :

01 Nettoyez votre base

Assurez-vous que les données collectées et traitées sont strictement nécessaires à la poursuite des objectifs définis

02 Vérifier l'adéquation de vos traitements avec les grands principes RGPD

On entre ici dans une introduction concrète du concept de «Privacy by design»! Mettez en place des mesures proactives et préventives dans la gestion de vos données personnelles de même qu'une protection automatique de ces dites données. Les processus mis en place doivent permettre à chaque personne concernée d'exercer ses droits (accès, rectification, portabilité...)

03 Révisez toutes vos mentions d'informations pour être en adéquation avec le règlement

CGV, contrats... On justifie chaque collecte en s'appuyant sur une base juridique solide ! (consentement, contrat ...)

04 Engagez la responsabilité de vos sous-traitants

Vérifiez la mise en conformité de vos sous-traitants et formalisez des clauses contractuelles définissant les obligations de ces derniers en termes de sécurité, confidentialité et protection des données personnelles traitées.

4) Evaluez les risques

Identifier un traitement à risque ne suffit plus, il vous faudra réaliser pour chacun de ces traitements suspects une analyse d'impact de la protection des données (DPIA - Data Protection Impact Assessment). Cette étude visant à inciter les organismes à construire un processus plus respectueux de la vie privée repose sur deux grands piliers :

- L'évaluation du système de traitement actuel et sa mise en comparaison avec les grands principes et droits cités dans le RGPD (finalités, durées de conservation, droits des personnes…)
- L'étude de risque sur la sécurité des données (abus, violations, disparition des données…)

5) Repensez vos processus internes

Le déploiement de votre plan d'action passe avant tout par la refonte de vos processus actuels. Votre obligation : garantir un haut niveau de protection des données personnelles et ce en permanence.
Application des principes de "Privacy by default" et "Privacy by design" à chaque niveau de votre activité, sensibilisation de l'ensemble de vos collaborateurs pour les impliquer dans une démarche proactive et responsable de traitement de la donnée, traitement des réclamations et des demandes des personnes concernées, ou encore anticipation des violations de données sont des sujets qui vont vous demander de repenser globalement vos processus de traitement internes et externes des données personnelles. Privilégiez des outils "RGPD compliant" pour mettre en oeuvre votre stratégie, anticiper et automatiser au maximum chaque scénario.

6) Documentez votre conformité

Nous l'avons dit le principe d'accountability est un des grands changements induits par le RGPD. Être en mesure de fournir des preuves de sa conformité nécessite de tenir à jour une documentation complète sur chaque action mise en place.

Quels éléments archiver ?

- Le registre des traitements
- Les analyses d'impacts sur la protection des données (PIA)
- L'encadrement des transferts de données hors de l'UE
- Les mentions d'information
- Les modèles de recueil de consentement
- Les procédures mise en place pour l'exercice des droits des individus
- Les contrats avec ses sous-traitants
- Les procédures en cas de violation de données
- Les preuves de consentement

ETAPE 1
DÉSIGNER UN PILOTE

DÉSIGNER UN PILOTE
Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.
> En savoir plus

ETAPE 2
CARTOGRAPHIER

CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES
Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.
> En savoir plus

ETAPE 3
PRIORISER

PRIORISER LES ACTIONS À MENER
Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.
> En savoir plus

ETAPE 4
GÉRER LES RISQUES

GÉRER LES RISQUES
Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact relative à la protection des données (AIPD).
> En savoir plus

ETAPE 5
ORGANISER

ORGANISER LES PROCESSUS INTERNES
Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).
> En savoir plus

ETAPE 6
DOCUMENTER

DOCUMENTER LA CONFORMITÉ
Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.
> En savoir plus