Proposition Formation Mallette du Dirigeant

Appel d'offre AGEFICE – Millésime 2019

MODULE n°7:

Protection des Données Personnelles (1jr)

Thématique : Nouvelles Technologies et compétences numériques

Protection des Données Personnelles – RGPD (Documentation CNIL)

Et autres outils et supports :

https://www.cnil.fr/fr/rgpd-par-ou-commencer

https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_fiche-1_que-faire-quand-votre-entreprise-communique-vend-en-ligne.pdf

https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_fiche_3_protegez-les-donnees-de-vos-collaborateurs.pdf

https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_fiche_2_ameliorez-maitrisez-votre-relation-client_0.pdf

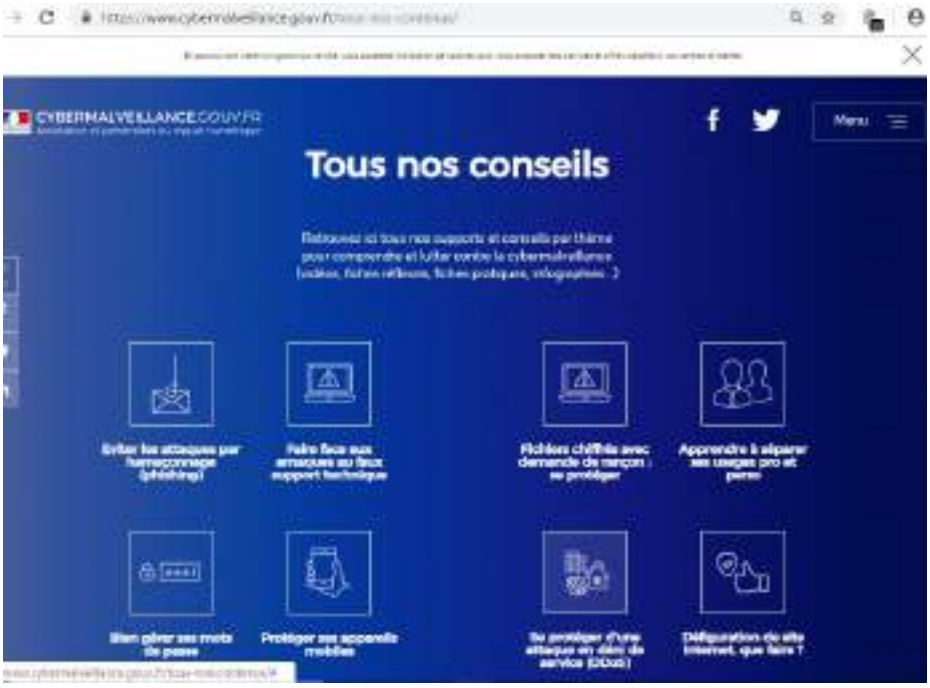
RGPD POUR VOUS :

https://www.cnil.fr/fr/comprendre-le-rgpd

- Tableau-loi-Informatique-libertes-1978

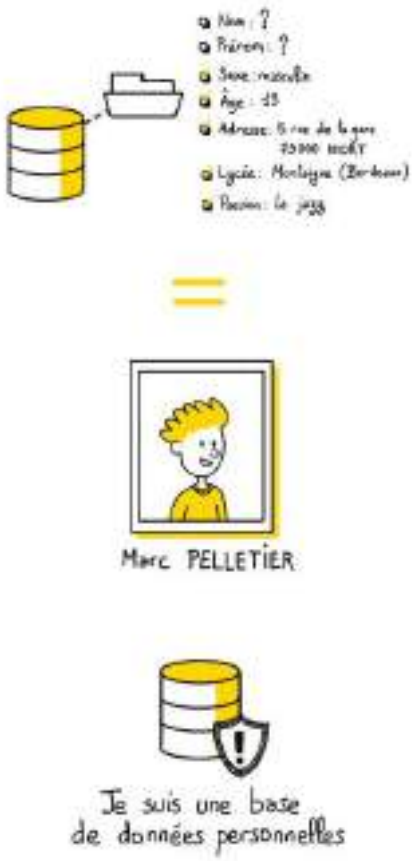
MISE EN PRATIQUE durant le module :

- Auto diagnostic : https://www.agencergpd.eu/diagnostic-rgpd-en-ligne/
- registre_rgpd_basique à remplir avec bénéficiaire et https://www.technologia.fr/actualites/rgpd-modeles-de-messages-dinformation-a-utiliser/
- Connection sur :



1- Définitions et périmètre

1.1. Qu'est-ce qu'une donnée personnelle ?



La notion de « données personnelles » est à comprendre de façon très large

Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ».

Une personne peut être identifiée :

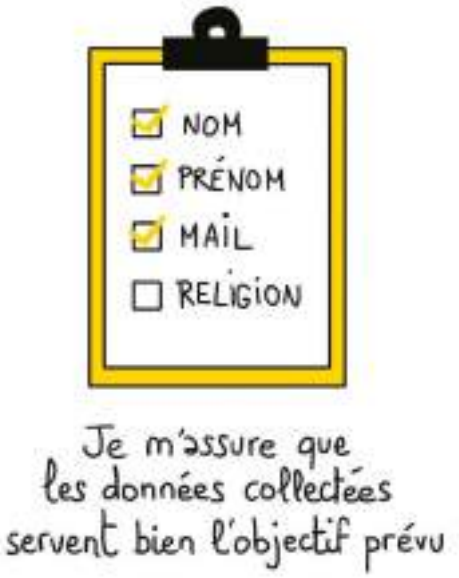
- **Directement** (exemple : nom, prénom)
- **Ou indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- **À partir d'une seule donnée** (exemple : numéro de sécurité sociale, ADN)
- **À partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

Exemple : une base marketing contenant de nombreuses informations précises sur la localisation, l'âge, les goûts et les comportements d'achats de consommateurs, y-compris si leur nom n'est pas stocké, est considérée comme un traitement de données personnelles, dès lors qu'il est possible de remonter à une personne physique déterminée en se basant sur ces informations.

1.2. Qu'est-ce qu'un traitement de données personnelles ?



Un traitement de données doit avoir **un objectif**, une finalité, c'est-à-dire que vous ne pouvez pas collecter ou traiter des données personnelles simplement au cas où cela vous serait utile un jour. A chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de votre activité professionnelle.

Exemple : vous collectez sur vos clients de nombreuses informations, lorsque vous effectuez une livraison, éditez une facture ou, proposez une carte de fidélité. Toutes ces opérations sur ces données constituent votre traitement de données personnelles ayant pour objectif la gestion de votre clientèle.

Cette notion est également très large.

Un « traitement de données personnelles » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).

Exemple : tenue d'un fichier de ses clients, collecte de coordonnées de prospects via un questionnaire, mise à jour d'un fichier de fournisseurs, etc.

Par contre, un fichier ne contenant que des coordonnées d'entreprises (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « compagnieA@email.fr ») n'est pas un traitement de données personnelles.

Un traitement de données personnelles n'est **pas nécessairement informatisé :** les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

2- Principes et précautions

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 respectueuses de la vie privée des personnes concernées :

2.1. NE COLLECTEZ QUE LES DONNÉES VRAIMENT NÉCESSAIRES

Posez-vous les bonnes questions : Quel est mon objectif ? Quelles données sont indispensables pour atteindre cet objectif ? Ai-je le droit de collecter ces données ? Est-ce pertinent ? Les personnes concernées sont-elles d'accord ?

2.2. SOYEZ TRANSPARENT

Une information claire et complète constitue le socle du contrat de confiance qui vous lie avec les personnes.

2.3. PENSEZ AUX DROITS DES PERSONNES

Vous devez répondre dans les meilleurs délais, aux demandes de consultation, de rectification ou de suppression des données.

2.4. GARDEZ LA MAÎTRISE DES DONNÉES

Le partage et la circulation des données personnelles doivent être encadrées et contractualisées, afin de leur assurer une protection à tout moment.

2.5. IDENTIFIEZ LES RISQUES

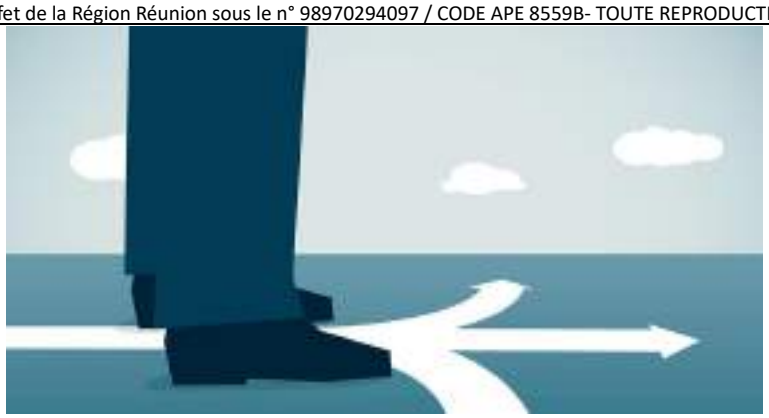
Vous traitez énormément de données, ou bien des données sensibles ou avez des activités ayant des conséquences particulières pour les personnes, des mesures spécifiques peuvent s'appliquer.

2.6. SÉCURISEZ VOS DONNÉES

Les mesures de sécurité, informatique mais aussi physique, doivent être adaptées en fonction de la sensibilité des données et des risques qui pèsent sur les personnes en cas d'incident.

3- Qu'est ce qui change ?

Le nouveau règlement européen sur la protection des données personnelles est entré en application le 25 mai 2018.



LA RÉFORME DE LA PROTECTION DES DONNÉES POURSUIT TROIS OBJECTIFS :

1. **Renforcer les droits des personnes**, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;
2. **Responsabiliser les acteurs traitant des données** (responsables de traitement et sous-traitants) ;
3. **Crédibiliser la régulation** grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées.

3.1. Un cadre juridique unifié pour l'ensemble de l'UE

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 compétents 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.

3.2. Un renforcement des droits des personnes

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.

3.3. 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 amènent à réaliser un suivi régulier et systématique des personnes à grande échelle,
- Si leurs activités principales les amènent 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

3.4. Des responsabilités partagées et précisées

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 responsable 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 responsable 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.

3.5. Le cadre des transferts hors de l'Union mis à jour

Les responsables de traitement et les sous–traitants peuvent transférer des données hors UE seulement s'ils encadrent ces transferts avec des outils assurant un niveau de protection suffisant et appropriés des personnes.

Par ailleurs, les données transférées hors Union restent soumises au droit de l'Union non seulement pour leur transfert, mais aussi pour tout traitement et transfert ultérieur.

Ainsi, et hormis les transferts fondés sur une décision d'adéquation de la Commission Européenne, les responsables de traitement et les sous-traitants peuvent mettre en place :

- Des règles d'entreprises contraignantes (BCR) ;
- Des clauses contractuelles types approuvées par la Commission Européenne ;
- Des clauses contractuelles adoptées par une autorité et approuvées par la Commission européenne.

De nouveaux outils sont également prévus :

- Pour les sous-traitants : la possibilité de mettre en place des règles d'entreprises contraignantes ;
- Pour les autorités publiques : le recours à des accords contraignants ;
- Pour les responsables de traitement et les sous-traitants : l'adhésion à des codes de conduite ou à un mécanisme de certification. Ces deux outils doivent contenir des engagements contraignants.

Enfin, une autorisation spécifique de l'autorité de protection basée sur ces outils n'est plus requise.

3.6. 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.

4- Quelles-sont ces obligations ?

Les sous-traitants qui traitent des données personnelles pour le compte de leurs clients ont de nouvelles responsabilités au regard du Règlement européen sur la protection des données (RGPD). La CNIL publie un guide pour les sensibiliser et les accompagner dans la mise en œuvre concrète de leurs obligations.

3.7. Qui est concerné ?

Applicable à compter du 25 mai 2018, le RGPD impose des obligations spécifiques aux sous-traitants dont la responsabilité sera susceptible d'être engagée en cas de manquement.

Ces obligations concernent **tous les organismes qui traitent des données personnelles pour le compte d'un autre organisme, dans le cadre d'un service ou d'une prestation**. Sont notamment concernés :

- Les prestataires de services informatiques (hébergement, maintenance, …),
- Les intégrateurs de logiciels,
- Les sociétés de sécurité informatique,

- Les entreprises de service du numérique ou anciennement sociétés de services et d'ingénierie en informatique (SSII) qui ont accès aux données,
- Les agences de marketing ou de communication qui traitent des données personnelles pour le compte de leurs clients

3.8. Que doivent faire les sous-traitants ?

Les sous-traitants sont tenus de respecter des obligations spécifiques en matière de sécurité, de confidentialité et de documentation de leur activité. Ils doivent prendre en compte la protection des données dès la conception du service ou du produit et par défaut et mettre en place des mesures permettant de garantir une protection optimale des données.

Les sous-traitants ont notamment une obligation de conseil auprès des clients pour le compte desquels ils traitent des données. Ils doivent les aider dans la mise en œuvre de certaines obligations du règlement (étude d'impact sur la vie privée, notification de violation de données, sécurité, contribution aux audits).

Les sous-traitants devront tenir un registre des activités de traitement effectuées pour le compte de leurs clients.

Dans certains cas, ils devront désigner un délégué à la protection des données (DPD) dans les mêmes conditions qu'un responsable de traitement.

Présenté sous forme de questions-réponses, le guide propose également un exemple de clauses de sous-traitance à adapter et préciser selon la prestation de sous-traitance concernée.

Ce guide est un outil vivant qui pourra être enrichi compte tenu des bonnes pratiques remontées auprès de la CNIL par les professionnels

5- Plan d'actions

Le 25 mai 2018, le règlement européen est entré en application. De nombreuses formalités auprès de la CNIL disparaissent. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité :

ETAPE 1 : DÉSIGNER UN PILOTE

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exerce une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données.

La désignation d'un délégué à la protection des données (DPO) est obligatoire si :

- Vous êtes un organisme public ;
- Vous êtes une entreprise dont l'activité de base vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

Même si votre organisme n'est pas formellement dans l'obligation de désigner un délégué à la protection des données, il est fortement recommandé de désigner une personne disposant de relais internes, chargée de s'assurer de la mise en conformité au règlement européen. Le délégué constitue un atout majeur pour comprendre et respecter les obligations du règlement, dialoguer avec les autorités de protection des données et réduire les risques de contentieux.

Le rôle du délégué à la protection des données

« Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé :

- **D'informer et de conseiller** le responsable de traitement ou le sous-traitant, ainsi que leurs employés
- **De contrôler le respect du règlement** et du droit national en matière de protection des données
- **De conseiller l'organisme** sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution
- **De coopérer avec l'autorité de contrôle** et d'être le point de contact de celle-ci

Pour vous accompagner dans la mise en place des nouvelles obligations imposées par le règlement européen, le délégué doit notamment :

- **S'informer** sur le contenu des nouvelles obligations

- **Sensibiliser** les décideurs sur l'impact de ces nouvelles règles
- **Réaliser l'inventaire** des traitements de données de votre organisme
- **Concevoir** des actions de sensibilisation
- **Piloter** la conformité en continu

ETAPE 2 : CARTOGRAPHIER

Pour mesurer concrètement l'impact du règlement européen sur la protection des données de votre activité, commencez par recenser de façon précise les traitements de données personnelles que vous mettez en œuvre. La tenue d'un registre des traitements vous permet de faire le point.

Dans le cadre de leur plan d'action pour se mettre en conformité au règlement européen sur la protection des données (RGPD), les organismes doivent tenir une documentation interne complète sur leurs traitements de données personnelles et s'assurer qu'ils 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, vous devez au préalable 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. Vous devrez 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 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 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 ?

ETAPE 3 : PRIORISER

Sur la base du registre des traitements, 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.

Après avoir identifié les traitements de données personnelles mis en œuvre au sein de votre organisme, vous devez, pour chacun d'eux, identifier les actions à mener pour vous conformer aux obligations actuelles et à venir.

Cette priorisation peut être menée au regard des risques que font peser vos traitements sur les libertés des personnes concernées. Certaines tâches seront faciles à mettre en œuvre et vous permettront de progresser rapidement.

Points d'attention quels que soient vos traitements

1. Assurez-vous que **seules les données strictement nécessaires** à la poursuite de vos objectifs sont collectées et traitées.
2. Identifiez **la base juridique** sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale)
3. Révisez vos **mentions d'information** afin qu'elles soient conformes aux exigences du règlement (articles 12, 13 et 14 du règlement)
4. Vérifiez que vos **sous-traitants** connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées.
5. Prévoyez les modalités d'exercice des **droits des personnes** concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...)
6. Vérifiez les **mesures de sécurité** mises en place.

Points d'attention nécessitant une vigilance particulière

VOUS TRAITEZ CERTAINS TYPES DE DONNÉES

- Des données qui révèlent l'origine prétendument raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale,
- Des données concernant la santé ou l'orientation sexuelle,
- Des données génétiques ou biométriques,
- Des données d'infraction ou de condamnation pénale,
- Des données concernant des mineurs.

VOTRE TRAITEMENT A POUR OBJET OU POUR EFFET

- La surveillance systématique à grande échelle d'une zone accessible au public ;
- L'évaluation systématique et approfondie d'aspects personnels, y compris le profilage, sur la base de laquelle vous prenez des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.

VOUS TRANSFÉREZ DES DONNÉES HORS DE L'UNION EUROPÉENNE

- Vérifiez que le pays vers lequel vous transférez les données est reconnu comme adéquat par la Commission européenne ;
- Dans le cas contraire, encadrez vos transferts.

Si vos traitements répondent à ces caractéristiques, des mesures particulières peuvent s'appliquer (exemple : analyse d'impact relative à la protection des données (AIPD), information renforcée, recueil du consentement, autorisation préalable, clauses contractuelles,). Une analyse approfondie de la loi informatique libertés et du règlement est nécessaire pour déterminer les mesures à mettre en œuvre.

ETAPE 4 : 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 (en anglais, Data Protection Impact Assessment).

Qu'est-ce qu'une analyse d'impact relative à la protection des données (AIPD) ?

C'est une analyse aidant à construire des traitements de données respectueux de la vie privée et permettant de démontrer la conformité de son traitement au RGPD. Une AIPD est un outil d'évaluation d'impact sur la vie privée. Elle repose sur 2 piliers :

1. Les principes et droits fondamentaux, « non négociables », fixés par la loi. Ils ne peuvent faire l'objet d'aucune modulation, quelles que soient la nature, la gravité et la vraisemblance des risques encourus
2. La gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriée pour protéger les données personnelles

Une AIPD contient :

- Une description du traitement étudié et de ses finalités
- Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités
- Une évaluation des risques pour les droits et libertés des personnes concernées les mesures envisagées pour faire face aux risques

Quand mener une analyse d'impact relative à la protection des données (AIPD)?

De manière générale, réaliser une AIPD est une bonne pratique pour s'assurer de créer un traitement conforme au RGPD et respectueux de la vie privée, que celui-ci soit susceptible ou non d'engendrer des risques élevés sur la vie privée.

L'AIPD doit être réalisée avant la mise en œuvre du traitement. C'est un processus itératif, les analyses doivent être revues et corrigées de manière régulière, en particulier lors de changements majeurs des modalités d'exécution du traitement.

Mener une AIPD est obligatoire pour tout traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes concernées (Article 35 du RGPD). Pour vous aider à déterminer si votre traitement est susceptible d'engendrer des risques élevés, les 9 critères suivants sont définis dans les lignes directrices du G29 :

1. Evaluation ou notation ;

2. Décision automatisée avec effet juridique ou effet similaire significatif ;
3. Surveillance systématique ;
4. Données sensibles ou données à caractère hautement personnel ;
5. Données personnelles traitées à grande échelle ;
6. Croisement d'ensembles de données ;
7. Données concernant des personnes vulnérables ;
8. Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles ;
9. Exclusion du bénéfice d'un droit, d'un service ou contrat.

Si votre traitement rencontre au moins 2 de ces critères, alors il est vivement conseillé de faire une AIPD.

Qui participe à l'élaboration de l'analyse d'impact ?

- **Le responsable de traitement** : valide l'AIPD et s'engage à mettre en œuvre le plan d'action défini dans l'AIPD ;
- **Le délégué à la protection des données :** élabore le plan d'action et se charge de vérifier son exécution ;
- **Le(s) sous-traitant(s) :** fournit les informations nécessaires à l'élaboration de l'AIPD ;
- **Les métiers** (RSSI, maîtrise d'ouvrage, maîtrise d'œuvre) : aident à la réalisation d'AIPD en fournissant les éléments adéquats ;
- **Les personnes concernées** : donnent leurs avis sur le traitement.

Les outils pour vous aider

La CNIL a élaboré une méthode et un catalogue de bonnes pratiques qui vous aident à mener une AIPD et déterminer les mesures proportionnées aux risques identifiés.

Un logiciel PIA, en version Beta, facilite la formalisation de cette analyse.

ETAPE 5 : ORGANISER

Pour garantir un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent 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 demandes de rectification ou d'accès, modification des données collectées, changement de prestataire).

Organiser les processus implique notamment :

- **De prendre en compte de la protection des données personnelles dès la conception** d'une application ou d'un traitement (minimisation de la collecte de données au regard de la finalité, cookies, durée de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données s'assurer du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de traitements de données). Pour cela, appuyez-vous sur les conseils du délégué à la protection des données
- **De sensibiliser et d'organiser la remontée d'information** en construisant notamment un plan de formation et de communication auprès de vos collaborateurs
- **De traiter les réclamations et les demandes des personnes concernées quant à l'exercice de leurs droits** (droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement) en définissant les acteurs et les modalités (l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen)
- **D'anticiper les violations de données** en prévoyant, dans certains cas, la notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais

ETAPE 6 : DOCUMENTER

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.

Votre dossier devra notamment comporter les éléments suivants :

LA DOCUMENTATION SUR VOS TRAITEMENTS DE DONNÉES PERSONNELLES

- **Le registre des traitements** (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants)
- **Les analyses d'impact relatives à la protection des données** (AIPD) pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes
- **L'encadrement des transferts** de données hors de l'Union européenne (notamment, les clauses contractuelles types, les BCR et certifications)

L'INFORMATION DES PERSONNES

- **Les mentions d'information**
- Les modèles de **recueil du consentement des personnes concernées**,
- Les procédures mises en place pour **l'exercice des droits**

LES CONTRATS QUI DÉFINISSENT LES RÔLES ET LES RESPONSABILITÉS DES ACTEURS

- **Les contrats avec les sous-traitants**
- Les procédures internes **en cas de violations de données**
- Les preuves que les personnes concernées **ont donné leur consentement** lorsque le traitement de leurs données repose sur cette base.

VOUS AUREZ FRANCHI CETTE ÉTAPE SI

- **Votre documentation démontre que vous respectez les obligations prévues par le règlement européen**