Les obligations de l'employeur en matière de protection des données personnelles

Mise à jour de la fiche suite à la publication de la loi française sur la protection des données personnelles et réorganisation de la fiche sur la base « d'actions » à réaliser.

Pour s'adapter aux enjeux du numérique et garantir une meilleure maîtrise des données personnelles, le droit européen a créé le **Règlement Général sur la Protection des Données** (« RGDP »)[1], qui s'applique directement en France depuis le **25 mai 2018**, complété par la **loi française n° 2018-493 du 20 juin 2018**[2], avec pour objectif de se substituer la loi informatique et libertés du 6 janvier 1978.

Pour rappel, depuis la loi de 1978 dite Informatique et Libertés, le législateur a souhaité **encadrer l'utilisation des données personnelles (informatiques ou manuscrites),** par exemple les noms, prénoms et autres informations à caractère personnel… **afin de protéger la vie privée des personnes**, y compris **les salariés dans l'entreprise.**

Dans nos secteurs, **nos entreprises** manipulent quantité de données personnelles relatives aux salariés et à leurs adhérents pour le fonctionnement de leur activité.

Le RGPD ne vient pas modifier les principes de base applicables au traitement de ces données (notamment que les données doivent être conservées dans une **finalité particulière**, que la collecte doit être **nécessaire** au regard de cette finalité …, cf. ci-après) ; **il vient plus modifier les modalités de gestion et de contrôle de ces données.**

En effet, le système de déclaration à la Cnil est remplacé depuis mai 2018 par un système **d'auto-contrôle continu et de responsabilisation des entreprises et des sous-traitants** (tels que les éditeurs de logiciel de paie et de gestion RH), ces derniers étant aussi concernés par le dispositif.

Si l'entreprise ne satisfait pas aux obligations d'auto-évaluation, elle pourra être sanctionnée par la Cnil.

1. Les 5 actions à mettre en place pour protéger les données personnelles

1.1. La mise en place d'un registre de vos traitements de données

Vous devez faire vous-même **l'évaluation de la compatibilité entre le traitement** envisagé et les règles européennes et nationales, en passant par la première étape de mise en place d'un registre.

Dans les **entreprises d'au moins 250 salariés**, l'employeur devra tenir un registre interne des traitements de données à caractère personnel qui devra contenir certaines mentions (RGPD, art. 30), à savoir :

- - l'identité (nom, prénom et coordonnées) du responsable du traitement, co-responsables de traitement, sous-traitants et destinataires intervenant dans le traitement ;
- - les finalités du traitement des données ;
- - les catégories de personnes concernées et les catégories des données traitées ;
- - le cas échéant, les transferts de données personnelles hors UE et les données communiquées ;
- - une description générale des mesures de sécurité techniques et organisationnelles ;

[1] L'objectif du règlement européen (UE) n°2016/679 du 27 avril 2016 (dit Règlement général sur la protection des données - RGPD) est de redonner aux citoyens le contrôle de leurs données personnelles tout en unifiant les réglementations relatives à la protection des données de la vie privée dans l'Union européenne.

[2] Il est prévu que dans les 6 mois suivant la promulgation de la loi, une ordonnance soit prise. Cette ordonnance portera sur la réécriture de l'ensemble de la loi informatique et libertés de 1978 afin d'apporter les corrections et adaptation nécessaires à la législation européenne sur la protection des données à caractère personnelle.

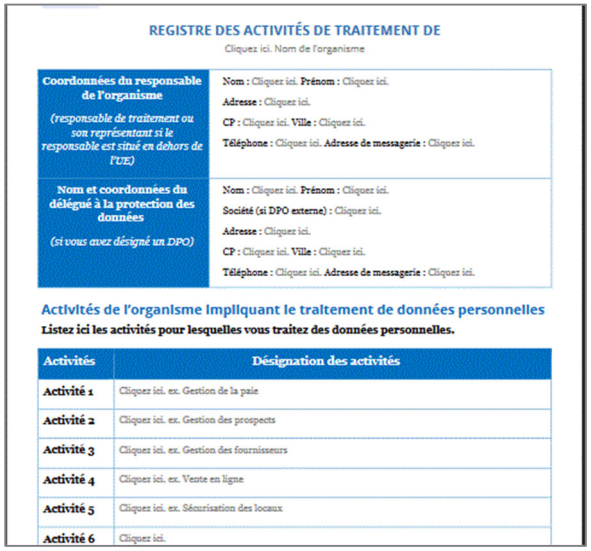
- - les limites de durée de conservation et les délais prévus pour l'effacement des données.

Dans les autres entreprises, ce document n'est pas obligatoire **mais nous vous recommandons de le mettre en place au moins de manière simplifiée,** car il vous permet d'avoir un **support écrit pour votre auto-évaluation**, et un support de vérification pour la Cnil. Si vous ne faites pas de registre, il faudra quand même respecter la démarche de contrôle qui suit :

La démarche est la suivante :

1) Identifiez les activités principales de votre entreprise qui nécessitent la collecte et le traitement de données.

Exemples : recrutement, gestion de la paye, formation, gestion des badges et des accès, statistiques de ventes, gestion des adhérents, etc.



REGISTRE DES ACTIVITÉS DE TRAITEMENT DE

Cliquez ici. Nom de l'organisme

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	**Nom :** Cliquez ici. **Prénom :** Cliquez ici. **Adresse :** Cliquez ici. **CP :** Cliquez ici. **Ville :** Cliquez ici. **Téléphone :** Cliquez ici. **Adresse de messagerie :** Cliquez ici.
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	**Nom :** Cliquez ici. **Prénom :** Cliquez ici. **Société (si DPO externe) :** Cliquez ici. **Adresse :** Cliquez ici. **CP :** Cliquez ici. **Ville :** Cliquez ici. **Téléphone :** Cliquez ici. **Adresse de messagerie :** Cliquez ici.

Activités de l'organisme impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités
Activité 1	Cliquez ici. ex. Gestion de la paie
Activité 2	Cliquez ici. ex. Gestion des prospects
Activité 3	Cliquez ici. ex. Gestion des fournisseurs
Activité 4	Cliquez ici. ex. Vente en ligne
Activité 5	Cliquez ici. ex. Sécurisation des locaux
Activité 6	Cliquez ici.

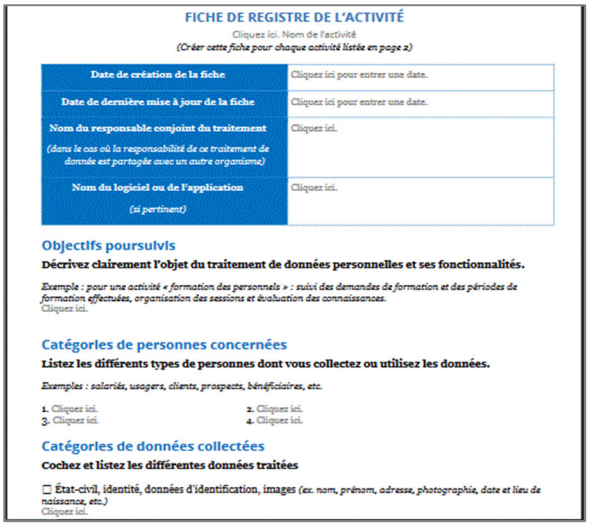
Exemple de modèle de registre : https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf

Concernant les données RH :

Les tâches pour lesquelles il est nécessaire de collecter, traiter et stocker des données personnelles sont notamment le recrutement (données personnelles des candidats, lettres de motivation, les contrats de travail…°, la gestion des carrières (dans le cadre de la formation, des évaluations annuelles et professionnelles, du droit disciplinaire, des arrêts de travail …), la paie et plus globalement la politique de rémunération et d'avantages sociaux (des données personnelles sont collectées pour la gestion des bulletins de paie (et du logiciel de paie), et pour la prévoyance/frais, lors des déclarations sociales et fiscales…), les relations sociales (données collectées dans le cadre des élections des représentants du personnel ou pour la BDES, les informations/consultation du CSE…), la sécurité et la gestion des accès (par exemple les dispositifs de badgeage ou de videosurveillance), la rupture du contrat de travail (documents de fin de contrat, solde de tout compte…)…

2) Dans votre registre, créez une fiche pour chaque activité recensée, en précisant :

- **L'objectif poursuivi** (la finalité - exemple : la gestion des paies) ;
- **les catégories de données utilisées** (exemple pour la paie : nom, prénom, date de naissance, salaire, etc.) ;
- **Qui a accès aux données** (le destinataire - exemple : service du personnel, service informatique, direction, prestataires, partenaires, hébergeurs) ;
- La **durée de conservation** de ces données (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive).



FICHE DE REGISTRE DE L'ACTIVITÉ

Cliquez ici. Nom de l'activité

(Créer cette fiche pour chaque activité listée en page 2)

Date de création de la fiche	Cliquez ici pour entrer une date.
Date de dernière mise à jour de la fiche	Cliquez ici pour entrer une date.
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	Cliquez ici.
Nom du logiciel ou de l'application *(si pertinent)*	Cliquez ici.

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.
Cliquez ici.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

Catégories de données collectées

Cochez et listez les différentes données traitées

☐ État-civil, identité, données d'identification, images *(ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)*
Cliquez ici.

S'agissant des données traitées dans le cadre d'un **logiciel** (paie, …), indiquez qu'il s'agit de données établies par un prestataire, et il faudra vérifier auprès de ce prestataire qu'il respecte lui-même la réglementation sur le traitement des données personnelles (cf. ci-après).

Le registre est placé sous la responsabilité du dirigeant de l'entreprise.

Pour avoir un registre exhaustif et à jour, il faut en discuter et être en contact avec toutes les personnes de l'entreprise susceptibles de traiter des données personnelles.

1.2. Faites le tri dans vos données : l'auto contrôle

La constitution du registre vous permet de **vous interroger sur les données dont votre entreprise a réellement besoin** (ce qui correspond aux principes de **finalité et de pertinence**).

Pour chaque fiche de registre créée, **vérifiez que** (démarche très importante) :

- les **données que vous traitez sont nécessaires** à vos activités (par exemple, il n'est pas utile de savoir si vos salariés ont des enfants, si vous n'offrez aucun service ou rémunération attachée à cette caractéristique) ;
- vous ne traitez **aucune donnée dite « sensible »** ou, si c'est le cas, que vous avez bien le droit de les traiter (voir partie 1.6 sur l'analyse d'impact) ;
- **seules les personnes habilitées ont accès** aux données dont elles ont besoin ; **vous ne conservez pas vos données au-delà de ce qui est nécessaire**. Par exemple, les données relatives à la gestion de la paie ou le contrôle des horaires des salariés ne peuvent être conservés que 5 ans maximum, et doivent ensuite être effacées. Il n'existe pas de liste des durées de conservation, ces durées devant être adaptées à la finalité.

La réglementation sur la protection des données personnelles prévoit en effet le respect des principes fondamentaux suivants (base de toute de cette législation) :

- tout traitement de données à caractère personnel doit être prescrit dans le cadre d'une **finalité** particulière (exemple : le recueil de données personnelles du type nom/prénom/adresse peut être recueilli dans le but de la gestion du recrutement)
- la collecte de ces données doit être nécessaire et **pertinente** au regard de la finalité (exemple : la situation professionnelle de l'entourage du candidat n'est pas pertinente au regard du process de recrutement)
- les données personnelles doivent être impérativement **conservées seulement le temps nécessaire pour l'accomplissement de l'objectif**
- les personnes concernées doivent être informées de manière claire et précise des objectifs poursuivis, du caractère obligatoire ou facultatif de leurs réponses, des destinataires des données et des modalités d'exercice de leurs droits **(principe de respect du droit des personnes)**.
- et empêcher notamment qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès (exemple : mise en place de mot de passe pour chaque personne ayant accès à ces données) **(principe de garantie de sécurité des données)**

Exemple : collecter des informations sur l'entourage familial d'un candidat dans un formulaire est inadéquat puisque ces données ne permettent pas d'évaluer ses compétences professionnelles ni d'apprécier sa capacité à occuper le poste proposé. Rappelons également que les CV et lettres de motivation ne peuvent être conservés plus de 2 ans à compter du dernier contact avec le candidat.

A cette occasion, améliorez vos pratiques : Minimisez la collecte de données, en éliminant de vos formulaires de collecte et vos bases de données toutes les informations inutiles. Redéfinissez qui doit pouvoir accéder à quelles données dans votre entreprise. Pensez à poser des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications.

Ainsi, au niveau RH, lors du travail d'identification des données collectées, les gestionnaires du personnel **doivent vérifier qu'ils ne collectent que les données adéquates, pertinentes et strictement nécessaires à la finalité du traitement**.

S'agissant des données traitées dans le cadre d'un logiciel (paie, …), le RGPD impose un **réexamen des contrats entre responsables de traitement et sous-traitants**. Les contrats devront préciser notamment la finalité du traitement, la durée de conservation des données et les obligations du sous-traitant. Dans ce cadre, **l'entreprise devra s'assurer que ses sous-traitants présentent des garanties techniques et organisationnelles suffisantes** au regard des exigences du règlement et de l'objectif de protection des données.

1.3. Respectez les droits des personnes

Le RGPD renforce l'obligation d'information et de transparence à l'égard des personnes dont vous traitez les données (salariés, adhérents, etc.).

- **Informez les personnes et les salariés et recueillez leur consentement**

A chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.

Vérifiez que **l'information comporte les éléments suivants** :

- pourquoi vous collectez les données (« la finalité » ; par exemple pour gérer une inscription en ligne) ;
- ce qui vous autorise à traiter ces données (le « fondement juridique » : il peut s'agir du consentement de la personne concernée, de l'exécution d'un contrat, du respect d'une obligation légale qui s'impose à vous, de votre « intérêt légitime ») ;
- Qui a accès aux données (indiquez des catégories : les services internes compétents, un prestataire, etc.) ;
- Combien de temps vous les conservez (exemple : « 5 ans après la fin de la relation contractuelle ») ;
- Les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (via leur espace personnel sur votre site internet, par un message sur une adresse email dédiée, par un courrier postal à un service identifié) ;
- Si vous transférez des données hors de l'UE (précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données).

Pour ce qui concerne **les salariés,** l'information est à délivrer au moment où les données sont collectées dans les documents de collecte (ex. : contrat de travail, fiche de renseignement) ou en pièce jointe.

Nous vous conseillons donc de remettre au salarié un dossier explicatif type avec la preuve de la remise du document à son embauche.

Le Règlement durcit également considérablement le régime du consentement : **ce consentement doit se manifester par une déclaration ou un « acte positif clair »** (pas de consentement par défaut). Il faudra donc veiller à insérer dans le système de collecte un dispositif permettant de recueillir ce consentement (ex. : système de case à cocher, autorisation écrite ou encore clause dans le contrat de travail).

- **Permettez aux personnes d'exercer facilement leurs droits**

Les personnes dont vous traitez les données (adhérents, salariés prestataires, etc.) ont des **droits sur leurs données**, qui sont d'ailleurs **renforcés par le RGPD** : droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement.

Vous devez leur donner les moyens d'exercer effectivement leurs droits. Dans les documents de communication avec ces personnes, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée. Si vous proposez un compte en ligne, donnez à vos clients la possibilité d'exercer leurs droits à partir de leur compte.

Mettez en place un **processus interne** permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois au maximum).

- **Sécurisez vos données**

Vous devez prendre les mesures nécessaires pour garantir au mieux la sécurité des données. Vous êtes en effet tenu à une obligation légale d'assurer la sécurité des données personnelles que vous détenez en minimisant les risques de pertes de données ou de piratage.

Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas de d'incident.

Des réflexes doivent être mis en place : mises à **jour de vos antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes, ou chiffrement de vos données dans certaines situations**. En cas de perte ou vol d'un outil informatique, il sera plus difficile pour un tiers d'y accéder.

Au titre des mesures organisationnelles pouvant être prises, l'entreprise peut mettre à la disposition de son personnel une **documentation interne** pour, par exemple, le sensibiliser aux cyber-attaques.

Les failles de sécurité ont également des conséquences pour ceux qui vous ont confié des données personnelles : Ayez à l'esprit les conséquences pour les personnes de la perte, la divulgation, la modification non souhaitée de leurs données, et prenez les mesures nécessaires pour minimiser ces risques.

Pour évaluer le niveau de sécurité des données personnelles dans votre entreprise, voici quelques questions à se poser :

- Les comptes utilisateurs internes et externes sont-ils protégés par des mots de passe d'une complexité suffisante ?
- Les accès aux locaux sont-ils sécurisés ?
- Des profils distincts sont-ils créés selon les besoins des utilisateurs pour accéder aux données ?
- Avez-vous mis en place une procédure de sauvegarde et de récupération des données en cas d'incident ?

Pour en savoir plus :

Guide des bonnes pratiques de l'informatique réalisé par l'ANSSI et la CPME sur le site internet www.cybermalveillance.gouv.fr et Guide sécurité des données personnelles de la CNIL

Pour vous aider en cas de difficultés (un sinistre, une attaque informatique, etc.), le site gouvernemental www.cybermalveillance.gouv.fr vous propose de l'aide en ligne ainsi qu'une liste de prestataires approuvés.

Cette démarche d'anticipation sur le niveau global de sécurité peut être complétée par une approche assurantielle. Renseignez-vous auprès de ces professionnels sur le contenu possible des polices d'assurance (responsabilité civile, dommages couverts…) et surtout sur les services à l'assuré (notamment l'assistance en cas de sinistre, de gestion de crise…).

- **Signalez à la CNIL les violations de données personnelles**

Votre entreprise a subi une violation de données (des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées ou vous avez constaté un accès non autorisé à des données) ?

Vous devez la **signaler à la CNIL dans les 72 heures** si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées (RGPD, art. 33). Cette notification s'effectue en ligne sur le site internet de la CNIL.

Si ces risques sont élevés pour « pour les droits et libertés » de ces personnes, vous devrez les en informer.

À l'issue de cette étape, vous serez en capacité d'assurer une protection des données personnelles en continu et de faire face aux incidents.

1.4. Désignation d'un DPO obligatoire dans certaines entreprises

Les actuels correspondants informatique et libertés (CIL) sont remplacés par des délégués à la protection des données (DPO ou *Date protection officer*) qui devront répondre à des critères de désignation stricts.

La présence du DPO sera **obligatoire pour les organismes privés dont l'activité de base les amène à réaliser un suivi des personnes régulier, systématique et à grande échelle, les organismes privés dont les activités de base les amènent à traiter de grandes quantités de données sensibles**[3] ou relatives à des condamnations pénales ou à des infractions.

A priori, ces activités concerneront peu de nos structures. Si vous ne savez pas si vous devez mettre en place un DPO, nous vous conseillons de contacter directement la CNIL.

Le DPO reprendra les attributions du CIL avec des missions élargies. Ainsi, il informera et conseillera l'entreprise ou le sous-traitant sur l'observation du RGPD, contrôlera la conformité des traitements au RGPD et au droit national, conseillera l'organisme sur la réalisation d'une analyse d'impact et en vérifiera l'exécution, servira d'interlocuteur à la Cnil et coopérera avec elle. Il ne sera pas personnellement responsable en cas de non-conformité, cette obligation incombant à l'entreprise ou au sous-traitant. Il peut être interne ou externe à l'organisme et peut même être mutualisé.

1.5. Analyse d'impact

Une **analyse d'impact** sur la protection des données personnelles pourra être demandée aux entreprises lorsque le traitement induira un **risque élevé pour les droits et libertés de la personne**. C'est le cas si l'entreprise est amenée à traiter de grandes quantités de données sensibles. A priori, la Cnil n'exigera pas immédiatement la réalisation d'une étude d'impact pour les traitements ayant régulièrement fait l'objet d'une formalité préalable auprès de la Cnil avant le 25 mai 2018. En revanche, une telle étude devra être réalisée dans les 3 ans à compter de cette date pour les traitements susceptibles de présenter un risque élevé.

Nous vous conseillons de demander directement à la CNIL si vous avez un doute sur l'obligation de mettre en œuvre cette analyse dans votre structure.

De manière générale, la Cnil met à disposition des entreprises sur son site **plusieurs outils pratiques** : un logiciel facilitant la réalisation des études d'impact, un modèle de registre et, bientôt, des référentiels (sectoriels pour certains), des modèles-type de mentions d'information, de formulaires de recueil de consentement, d'un formulaire de désignation du DPO

Vous pourrez retrouver tous ces outils via le lien suivant, à l'intérieur de chaque étape correspondante : https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

2. Le nouveau rôle de la CNIL : réguler et accompagner

Désormais la CNIL n'a plus vocation à délivrer des autorisations ni à recevoir de déclaration. Par contre, elle peut réaliser des contrôles a postériori. En effet, si un traitement peut engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable de traitement doit effectuer une analyse d'impact par rapport à la protection des données à caractère personnel. Il doit également au préalable, consulter la CNIL[4]. A cet effet, la CNIL peut établir une liste des traitements susceptibles de créer un risque élevé. Le responsable des données doit la consulter au préalable.

Attention : pour les données les plus sensibles – données biométriques nécessaires à l'identification ou au contrôle de l'identité des personnes, les données génétiques ou encore pour les traitements utilisant le numéro

[3] Ces données sensibles n'ont pas changé. On y retrouve l'appartenance politique, syndicale, les origines ethniques, l'appartenance à une religion, la santé, etc. Seules les données biométriques (ex. : authentification par empreinte digitale ou reconnaissance de l'iris) ont été ajoutées au RGPD

[4] Règlement UE n°2016/679 27 avril 2016, article 35

d'inscription au répertoire national d'identification des personnes physiques (NIR), des formalités préalables sont nécessaire préalablement à leurs traitements.

La CNIL conserve néanmoins un rôle **d'information et de certification**. Elle continue à établir et à mettre à disposition des textes pour faciliter la mise en conformité des traitements de données à caractère personnel avec les nouveaux textes relatifs à la protection des données (notamment concernant les données sensibles) notamment à destination des TPE/PME. Elle peut également agréer des organismes et certifier des personnes, produits ou encore procédures de traitements de données.

Son pouvoir **d'enquête** est maintenu. Elle peut notamment ordonner la communication de toute information utile, mener des enquêtes sous forme d'audits, notifier une violation constatée, accéder à toutes les données et informations nécessaires à l'accomplissement de ses missions[5], accéder aux locaux des entreprises.

Remarques : les agents de contrôle de la Cnil pourront recueillir sur place ou sur convocation tout renseignement et toute justifications utiles et demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie. Ils pourront accéder, dans des conditions préservant la confidentialité à l'égard des tiers, aux programmes informatiques et aux données ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle. Le secret ne pourra leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou par le secret médical.

Même chose concernant son **pouvoir de sanction**. Si le responsable de traitement ou son sous-traitant ne respecte pas les dispositions du RGPD ou de la loi, le président de la CNIL peut exiger une mise de demeure de : satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, mettre les opérations de traitement en conformité avec la législation applicable, communiquer à la personne concernée la violation de ses données à caractère personnel ou encore de rectifier ou d'effacer les données concernées [6].

[5] Le secret professionnel ne peut pas lui être opposé sauf concernant les informations couvertes par le secret professionnel (avocat, journaliste ou médecin)

[6] Selon le projet de loi relatif à la protection des données personnelles, le président de la Cnil pourra avertir le responsable de traitement de possibles violations aux dispositions européennes de ses opérations de traitement. Il pourra aussi décider de saisir la formation restreinte de la Cnil qui, elle, pourra rappeler le responsable à l'ordre, mettre en demeure l'entreprise de se mettre en conformité (dans le délai qu'elle fixera et qui pourra, en cas d'urgence, être de 24 heures), prononcer une injonction de mettre en conformité le traitement avec les dispositions européennes ou légales sous astreinte, limiter temporairement ou définitivement un traitement ou suspendre les flux de données, ordonner de répondre favorablement aux demandes d'exercice des droits des personnes, ordonner la rectification, la limitation ou l'effacement des données, ou retirer la certification délivrée ou ordonner à l'organisme de certification de la retirer. En complément ou à la place de ces mesures, la Cnil pourra condamner les entreprises à une amende qui devra être "effective, proportionnée et dissuasive".