RESSOURCES HUMAINES

5 RGPD : LES EXIGENCES DE LA MISE EN CONFORMITÉ DES ENTREPRISES AU NIVEAU RH

Article rédigé par :
Ludivine PONS,
avocat, Cabinet Coblence et Associés

Alors que le RGPD entre en vigueur le 25 mai 2018, la question de la mise en conformité des données RH des entreprises constitue l'un des points cruciaux de vigilance des chefs d'entreprises et de leurs experts-comptables au regard des exigences du règlement. Méthodologie, pragmatisme et rigueur sont de mise pour entrer dans ce cadre protégé et protecteur des droits des personnes.

Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (GDPR ou, ci-après "RGPD"), et abrogeant la directive 95/46/CE, met en place une véritable approche européenne de la sécurité des données à caractère personnel [1]. Cette approche régionale répond en premier lieu à un impérieux besoin de réguler le traitement à grande échelle de données personnelles, notamment par les groupes et sociétés récipiendaires de nombreuses données, tels que les gestionnaires de moteurs de recherche et de réseaux sociaux.

En 99 articles, le RGPD entend ainsi **réguler la gestion de données** par nature immatérielle, que ce soit dans les grands groupes pour lesquels il semble avoir été édicté, mais **également dans de petites et moyennes entreprises** qui semblent globalement désarmées face à l'ampleur de la tâche qu'induit les dispositions du RGPD : cartographie des données traitées, désignation pour certaines d'un délégué à la protection des données (ci-après "DPD") au statut particulier, tenue d'un registre obligatoire, gestion des sous-traitants, mise en place de procédures efficientes de gestion des données, réalisation dans certaines circonstances d'études d'impacts, etc.

La **gestion des ressources humaines de l'entreprise** est **en premier lieu concernée par les exigences du RGPD**. En effet, les **traitements de données à caractère personnel des salariés** sont, si ce n'est quotidiens, à tout le moins réguliers et/ou récurrents : embauche, recrutement, établissement de la paie, suivi du parcours professionnel, gestion des flottes d'outils professionnels et de voitures de fonction, gestion des arrêts, mutuelle et prévoyance, retraite, PEE, etc. Ces traitements ont lieu tout au long du parcours professionnel des salariés au sein de l'entreprise mais aussi, peut-être, auprès du nouvel employeur en application du droit à la portabilité des données [2].

L'expert-comptable, partenaire privilégié de nombreuses entreprises, sera au premier plan concerné par l'application rigoureuse des dispositions du RGPD, tant en interne, qu'en qualité de sous-traitant. Il lui est donc essentiel de maîtriser les impacts pour ses clients employeurs.

Dans ce contexte, il est essentiel de faire preuve de méthodologie, tout particulièrement en matière de gestion des données

1. V. *D.O Actualité 11/2018, n° 11 et s.* – V. égal., *Comm. com. électr. 2018, dossier 1 à 19*

2. *RGPD, art. 20*

à caractère personnels traitées dans le domaine des ressources humaines, thème de la présente étude. Sur la base des conseils et préconisations de la Commission Nationale Informatique et Libertés (CNIL) [3], il sera exposé ci-après des conseils pratiques pour que la mise en place du RGPD soit facilitée.

1. Étape 1 : choisir un délégué à la protection des données : quand ? qui ?

A. - Quel est son rôle ?

Selon les lignes directrices du G29 relatives aux délégués à la protection des données (DPD, ou DPO) [4], il est précisé que ces derniers « favorisent le respect des règles grâce à la mise en œuvre d'outils de responsabilité (comme la facilitation d'analyses d'impact relatives à la protection des données et à la facilitation ou la réalisation d'audits relatifs à la protection des données) ». En outre, les DPD « agissent comme intermédiaires avec les acteurs concernés », c'est-à-dire essentiellement avec la CNIL et les personnes dont les données sont traitées.

Le DPD a ainsi pour rôle de **garantir l'application constante des dispositions du RGPD au sein de l'entreprise.**

B. - Sa désignation est-elle obligatoire ?

L'article 37 du RGPD précise les **cas dans lesquels la désignation du DPD est obligatoire**. Ainsi, le responsable du traitement (l'employeur par exemple) doit désigner « *en tout état de cause un délégué à la protection des données lorsque* » :

- le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;
- **les activités de base** du responsable du traitement consistent en :

- des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un **suivi régulier et systématique à grande échelle** des personnes concernées ; **ou**
- **un traitement à grande échelle de catégories particulières de données** (qui relèvent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique) et de données à caractère personnel relatives à des condamnations pénales et à des infractions.

S'agissant du cas particulier des employeurs et **plus particulièrement de leur service des ressources humaines**, on constate qu'ils sont amenés à gérer très régulièrement notamment les traitements suivants :

- l'établissement de la paie ;
- la gestion des recrutements ;
- la gestion de performances professionnelles ;
- le suivi des horaires effectués par les salariés ;
- le suivi systématique de l'activité ou des déplacements des salariés ;
- la gestion des arrêts maladie ;
- le suivi des infractions routières lorsqu'un véhicule de fonction est mis à disposition.

Lors de ces traitements, des données sensibles seront collectées et traitées : handicap, situation familiale (notamment pour la mutuelle et la prévoyance), numéro de sécurité sociale, coordonnées bancaires, etc. En outre, la plupart des données ainsi collectés donneront lieu à un traitement régulier et systématique (la paie). Pour autant, ces types de traitement ne semblent pas nécessiter, à ce jour, la désignation d'un DPD au sein de la plupart des entreprises concernées dès lors qu'il ne s'agit pas de leur « activité de base » au sens du RGPD. Il nous semble toutefois que la désignation d'un DPD constitue une précaution non négligeable au regard de la sensibilité des données traitées.

Par contre, s'agissant des entreprises dont l'« activité de base » consiste à assurer ou sous-traiter la tout ou partie de la gestion des ressources humaines, comme la paie, il nous semble que la désignation d'un DPD s'impose. Cette désignation devrait par exemple s'imposer, selon nous, aux cabinets d'expertise-comptable traitant régulièrement et à grande échelle les données à caractère personnel des salariés de leurs clients.

L'article 35 du RGPD renvoyant aux lignes directrices du G29 concernant l'analyse d'impact précise que **le salarié, soumis à une relation de sujétion vis-à-vis de son employeur, doit être considéré comme une « personne vulnérable ».**

C. - Qui peut être DPD ?

Il est possible de recourir au service de tiers prestataires qui exerceront le rôle de DPD pour le compte de l'employeur. Il conviendra alors de prendre soin de s'assurer de la rédaction du cahier de charges du tiers prestataire et de vérifier au préalable qu'il ait toutes compétences pour exercer pleinement sa mission en justifiant du suivi de programme de formation reconnu.

Un salarié peut également être désigné DPD. Il doit être désigné « *sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39* » [5].

Il peut exercer sa mission « DPD » à côté d'autres fonctions. Dans ce cas, le salarié désigné ne doit pas être en conflit d'intérêt :

- il ne doit pas être amené à décider de constituer un traitement de données et d'en déterminer la ou les finalités ainsi que les moyens ;
- il ne peut généralement pas exercer des fonctions d'encadrement supérieur : directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines, responsable du service informatique, etc.

3. dlr : cette étude a été publiée in *D.O Actualité 2018, 20/2018, n° 21*. Elle a été mise à jour en vue de cette publication.
V. https ://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes.

4. V. *https ://www.cnil.fr/sites/default/files/atoms/files/wp243rev01_fr.pdf.*

5. *RGPD, art. 37 § 5*

Si le salarié exerce ses fonctions DPD à temps partiel, il doit bénéficier d'un temps suffisant pour exercer ses fonctions DPD mais aussi ses autres fonctions. Il est de bonne pratique de **fixer un pourcentage de temps consacré à la fonction DPP** après avoir déterminé le temps nécessaire à l'exécution de la fonction sur la base d'un plan de travail [6].

Il doit en outre [7] **:**

- bénéficier d'une **formation continue** pour garantir qu'il dispose des moyens nécessaires pour exercer ses fonctions ;

- bénéficier des **ressources nécessaires à l'exercice de ses missions** (financières, RH, moyens notamment).

D. - Est-il pertinent de désigner en qualité de DPD un salarié de l'entreprise ?

Cette question est récurrente au sein des entreprises qui s'inquiètent d'avoir un salarié bénéficiant d'un statut particulier. En effet, le salarié DPD doit être en mesure d'exercer ses fonctions et missions en toute indépendance et ne doit, à ce titre, recevoir « *aucune instruction en ce qui concerne l'exercice des missions* » DPD. En outre, il ne peut être licencié, discriminé ou sanctionné en raison de l'exercice de ses fonctions DPD [8]. Les lignes directrices du G29 précisent que le DPD « devrait avoir la possibilité d'indiquer clairement son avis divergent au niveau le plus élevé de la direction et aux décideurs » sans en être inquiété. Il doit également pouvoir décider seul de la façon dont il traite une affaire et les conclusions auxquelles il arrive.

Si le salarié DPD bénéficie en effet d'un **statut à part** au sein de l'organisation concernée, il n'est **pas pour autant un salarié protégé** au sens du Livre IV de la deuxième partie du Code du travail français. La CNIL confirme par ailleurs que le délégué « n'est pas un salarié protégé au sens du code du travail français et que dès lors, il pourrait être licencié légitimement, comme tout autre employé, pour des motifs autres que l'exercice de ses missions de délégué (par exemple, en cas de vol, de harcèlement physique, moral ou sexuel ou fautes graves similaires) » [9].

Ceci étant posé, le choix d'un DPD interne ou externe doit se faire **sur la base de considérations pratiques**, comme par exemple :

- Existe-t-il d'ores et déjà un **Correspondant Informatique et Libertés** ? Dans l'affirmative, ce dernier pourra naturellement devenir le DPD.

- **Souhait de l'entreprise d'être certifiée ou reconnue comme respectueuse des normes RGPD** et volonté de communiquer en interne et en externe à ce propos : un DPD en interne semble dès lors être plus indiqué ; ce positionnement peut constituer un avantage concurrentiel.

- **Volonté de l'entreprise de protéger la confidentialité des traitements opérés et des données traitées**. Peur de fuites en externe. Le DPD aura accès à des informations sensibles. Certaines entreprises préfèreront s'orienter en conséquence vers un DPD externe soumis au secret professionnel comme un avocat. D'autres choisiront la position opposée préférant garder totalement en interne la gestion de leurs traitements.

- **Crainte de l'entreprise de ne pouvoir occuper à temps plein un salarié en raison de l'absence de recul sur les impacts du RGPD**. Le recours à un DPD externe peut permettre de jouer plus facilement sur le volume de travail généré par l'implémentation du RGPD dans le temps.

E. - Quand est-il nécessaire de désigner un DPD ?

La **désignation du DPD doit intervenir au plus tôt et en tout état de cause au 25 mai 2018**, date d'entrée en vigueur du RGPD.

2. Étape 2 : lister l'ensemble des déclarations et autorisations CNIL existantes au sein de l'entreprise

Jusqu'au 24 mai 2018 inclus, la réalisation de traitements de données à caractère personnel était soumise à des **formalités préalables auprès de la CNIL et auprès des IRP**. Le **listing des formalités** ainsi accomplies constitue une **base essentielle pour identifier les traitements** en vigueur au sein de l'entreprise et permettre, par la suite, de compléter le registre des traitements.

À titre d'exemple, on peut citer les formalités suivantes qui sont les plus fréquentes au sein d'un service RH :

* NS 42 : badge sur le lieu de travail ;
* NS 46 : Gestion de personnel ;
* NS 47 : Gestion de la téléphonie sur le lieu de travail ;
* NS 51 : Géolocalisation des véhicules des employés ;
* NS 57 : Ecoute et enregistrement des conversations téléphoniques sur le lieu de travail ;
* DI 002 : Gestion de rémunérations ;
* DI 009 : listes d'initiés ;
* AU-010 : Recouvrement des contraventions routières ;
* AU-004 : Dispositif d'alerte professionnelle ;
* AU-052 et 053 : biométrie pour le contrôle d'accès sur le lieu de travail ;
* Déclarations : notamment vidéosurveillance ;
* Autres

3. Étape 3 : procéder à une cartographie à date des traitements de données à caractère personnel impliquant des salariés

La cartographie des traitements de données à caractère personnel concernant les salariés va notamment permettre :

- de **lister l'ensemble des traitements réalisés de façon exhaustive**,

- de **vérifier l'existence ou non de sous-traitance ou de transferts de données** et de **contrôler l'existence et le contenu des contrats de sous-traitance** en matière de protection des données à caractère personnel,

- d'**identifier la finalité du traitement opéré et les personnes pouvant y avoir accès**,

6. *RGPD, art. 38*
7. *RGPD, art. 38*
8. *RGPD, art. 38 § 3*
9. V. *https ://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees.*

- le **respect de l'information ou l'information-consultation préalable des instances représentatives du personnel** lorsque cela est légalement requis,

- de **contrôler la présence de mesures de sécurité suffisantes** pour garantir la protection des données collectées.

Exemples de traitements mis en place pouvant concerner des salariés :

* Paie* Administration du personnel
* Formation – OPCA
* Procédure de recrutement
* Mise à disposition d'outils informatiques
* Procédure d'alerte
* Badge d'entrée/sortie
* Mutuelle et prévoyance
* Retraite complémentaire
* Gestion des amendes routières
* Plan d'épargne d'entreprise – Participation/intéressement
* Etc.

Un **exemple de cartographie pour une paie externalisée auprès d'un prestataire tiers** :

Réalisé le :	Commentaires / actions	
Nom du traitement	Paie	
Description du traitement	Gestion de la paie du personnel de l'ensemble de la société	
Personnes concernées	Salariés	
Intervenants dans la gestion du traitement : en interne et en externe	*Interne* : responsable de paie / DRH en approbation / DAF en contrôle	*Interne* : vérifier les accès / mettre en place une procédure de renouvellement des mots de passe
	Externe : société XX (n° RCS – adresse siège social) – contrat de sous-traitance signé le XXX.	*Externe* : vérifier les termes du contrat – renégocier par voie d'avenant les engagements du sous-traitant en matière de protection des données / mesures de sécurité / audits / etc.
Catégories de données concernées / Données sensibles traitées	État civil / identité / rémunération / statut / fonctions / ancienneté / lieu de travail / nature du contrat de travail / retenues opérées par l'employeur / taux et base des cotisations sociales / congés et absences (dont AT/MP) / frais professionnel / mode de règlement / identité bancaire / taux invalidité / durée du temps de travail	Appliquer le principe de minimisation des données collectées / À compléter avec le prélèvement à la source depuis janvier 2019
Finalités du traitement	Calcul et paiement des rémunérations et accessoires Réalisation des opérations résultant de dispositions légales, CCN et contrats de travail Tenue des comptes individuels relatifs à l'intéressement et à la participation Statistiques non nominatifs Fourniture des écritures de paie à la comptabilité	
Destinataire(s) des données	Service chargé de l'administration et de la paie du personnel Service chargé du contrôle financier Organismes gérant les différents systèmes d'assurances sociales, d'assurances chômage, de retraite et de prévoyance, les caisses de CP, les organismes publics et administrations légalement habilitées à les recevoir	
Information / Consentement des salariés	Salariés	Données recueillies requises légalement : information Attention au droit à l'image en cas de collecte d'une photo du salarié

Réalisé le :	Commentaires / actions	
Information et/ou consultation des IRP	Fait par PV du XXX	L. 2323-29 / L. 2323-46 (CE / DUP) et L. 2312-8 et L. 2312-38 (CSE) – Information et/ou consultation selon l'impact (externalisation paie / changement de prestataire de paie par ex.)
Meures de sécurité mises en place	*Techniques* : en interne, mot de passe individuel régulièrement modifié / chez la société XXX, à documenter	Documenter les mesures de sécurité en place chez la société XXX
	Organisationnelles : procédure SOX et management des autorisations d'accès / modification / validation de la paie	
Transfert hors UE ?	Non / Oui : de quel type, finalité ?	Vérifier la localisation des serveurs d'hébergement des données chez la société XXX
Si la sous-traitance est autorisée, demander la liste des sous-traitants et prendre toutes garanties utiles.		

Cette cartographie doit être réalisée pour chaque traitement de données à caractère personnel.

4. Étape 4 : mener, lorsque cela est nécessaire, une étude d'impact

La *Privacy Impact Assessment* ou étude d'impact (ci-après « PIA ») n'a pas vocation à être mise en œuvre pour l'ensemble des traitements RH. Elle est **requise uniquement lorsque le traitement** « ***est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques*** » [10]**. Dans ses lignes directrices, le G29 liste 9 critères à prendre en compte pour identifier, de manière générale, un traitement à risque concernant les salariés** :

- Évaluation ou notation du salarié (rendement au travail, état de santé, établissement de profil ou prédiction).

- Surveillance systématique du salarié dans les locaux professionnels ou de son activité, y compris son poste de travail et son activité sur internet.

- Collecte de données sensibles ou hautement personnel (appartenance syndicale du salarié, email non professionnel, par exemple).

- Traitement de données à large échelle (combinant le nombre de personnes concernées, la zone géographique, le volume de données et à la durée du traitement).

- Combinaison ou croisement de plusieurs jeux de données entre elles.

- Traitement de données relatives à des personnes vulnérables (les salariés sont considérés par le G29 comme des personnes vulnérables en raison du déséquilibre des pouvoirs accrus entre salariés/employeur).

- Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles (système de reconnaissance d'empreintes digitales ou reconnaissance faciale des salariés pour l'entrée dans les locaux).

- Traitement qui empêche le salarié d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

Au-delà de deux critères sur les 9 énumérés : la PIA devrait en principe être effectuée selon le G29. **Si la PIA révèle un risque élevé, l'entreprise devra consulter au préalable la CNIL avant la mise en œuvre du traitement** (avis sous 8 semaines).

Dans le cadre de la cartographie des traitements réalisée par l'entreprise, si cette dernière constate que l'un des traitements est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, il nous semble indispensable de réaliser une PIA préalable, tout particulièrement si l'entreprise n'avait pas procédé auparavant à une formalité de déclaration normale ou d'autorisation auprès de la CNIL l'autorisant à réaliser un tel traitement. Il conviendrait également de stopper le traitement « litigieux » dans l'attente de la réalisation de cette PIA et, le cas échéant, jusqu'à ce que la CNIL se soit prononcée à ce propos.

5. Étape 5 : mettre en place des processus internes pour gérer l'évolution et le suivi efficient des traitements en place au sein de l'entreprise

La mise en conformité de l'entreprise aux dispositions du RGPD est une première étape. Il convient par la suite de **garantir le maintien de cette conformité dans le temps**.

À cet effet, l'entreprise peut :

- **Mettre en place une procédure claire et précise de collecte des données des candidats et salariés** : quelles données collectées, quelles finalités, quels destinataires, durée de conservation, information/consentement et modalités concrètes d'exercice de leur droit d'accès, rectification, effacement, limitation, portabilité par les salariés (prévoir par exemple de remettre une fiche d'information et de consentement aux candidats leur expliquant les caractéristiques des traitements de leurs données à caractère personnel qu'ils soient retenus pour le poste ou non).

- **Instituer une procédure claire et précise de notification des violations de données à caractère personnel** : notification

10. *RGPD, art. 35 § 1*

à la CNIL au plus tard dans les 72 h après avoir pris connaissance de la notification de la violation / actions mises en œuvre (en urgence, en curatif, de fond) / établir un formulaire type de déclaration de violation dont aurait connaissance un tiers ou un salarié.

- Créer une **veille sur la durée de conservation des données.**

- **Mettre en place un plan de formation régulier des salariés pour garantir le respect des processus internes et leur application effective** : à ce titre, les salariés ont à la fois des droits et des devoirs en matière de respect du RGPD. Si l'employeur doit garantir aux salariés que les traitements de leurs données à caractère personnel sont conformes au RGPD, les salariés eux-mêmes doivent respecter le RGPD dès lors qu'ils ont accès à des données à caractère personnel, qu'il s'agisse des données de leurs collègues ou de celles des clients et prospects.

- En cas de **sous-traitance, mettre en place un cahier des charges très précis** s'agissant de la protection des données à caractère personnel confiées au sous-traitant permettant ainsi de garantir, dès la conception d'une plateforme/application/traitement de données, la protection des données à caractère personnel (*Privacy by Design*). Mettre également en place des clauses types garantissant la protection et la sécurité des données traitées par un sous-traitant.

- **Mettre en place des modèles de recueil du consentement des personnes concernées** lorsque cela est requis.

6. Étape 6 : documenter la conformité des traitements réalisés au RGPD

L'entreprise doit être capable à tout moment de démontrer qu'elle respecte les dispositions du RGPD en tous ses aspects. À cet effet, elle doit absolument **se ménager la preuve des actions entreprises** et **garantir que la protection des données à caractère personnel, en particulier de ses salariés, est opérationnelle et régulièrement contrôlée**.

Ainsi, l'entreprise doit :

- **Tenir un registre des traitements** : l'implémentation de ce registre est **fortement conseillée même pour les structures de moins de 250 salariés** et il doit en outre **être complet et avoir une date certaine** ; en effet, en cas de contentieux, notamment prud'hommal, il conviendra que l'employeur puisse démontrer que le traitement opéré, et support de la sanction disciplinaire contestée, est licite :

- par exemple, si un licenciement est basé sur une faute du salarié constatée dans le cadre d'un enregistrement audiovisuel (télésurveillance), l'employeur devra démontrer qu'au moment où l'infraction a été constatée, ce type de traitement était consigné au préalable dans le registre, que les moyens, la finalité poursuivie, les destinataire, la durée de conservation notamment y étaient précisés et régulièrement contrôlés par l'employeur, que les instances représentatives du personnel avaient été au préalable consultées et qu'une information claire et préalable des salariés sur ce procédé avait été faite. À défaut, la faute support du licenciement pourrait être écartée et le licenciement considéré comme étant sans cause réelle et sérieuse ;

- il peut être **opportun de faire un point annuel avec les instances représentatives du personnel sur le contenu du registre**, permettant ainsi d'acter, avec date certaine, que l'employeur est à jour de ses obligations ;

- de même, les **échanges par emails avec le DPD s'il en existe un ou en interne et contenant en pièce jointe copie du registre à jour, devront être conservés** pour documenter la preuve de la tenue dudit registre.

- **Tenir un registre des PIA réalisés, des avis formulés en interne et par la CNIL et préciser si le traitement a été mis en place et quelles mesures de contrôle et de sécurité** ont été déployées pour en assurer la protection.

- **Documenter les transferts hors Union européenne et préciser la base légale** permettant un tel transfert (clauses types, *Binding Corporate Rules*, *Privacy Shield*).

- **Collecter les preuves que les personnes concernées ont été informées et/ou ont donné leur consentement** lorsque le traitement de leurs données repose sur un consentement préalable.

- **Tenir un listing des sous-traitants gérant des données à caractère personnel** pour le compte du responsable de traitement et indiquer qu'une vérification de clauses du contrat a été faite, les conclusions de cette vérification et le plan d'actions mis en place.

- **Tenir un listing des audits réguliers opérés au sein de l'entreprise et auprès des sous-traitants gérant des données à caractère personnel** – préciser les conclusions des audits et le plan d'actions mis en place.

- **Tenir un registre des violations de données constatées et documenter la résolution du problème**.

7. Étape 7 : adapter les « outils » RH de l'entreprise

Par « outils », il faut notamment entendre le **règlement intérieur et la charte informatique** (annexée de préférence au règlement intérieur), les **documents informatifs remis aux candidats à un poste au sein de l'entreprise** concernant le traitement de leurs données à caractère personnel, le **plan de formation** pour **s'assurer que les salariés sont pleinement informés de leurs droits mais également de leurs obligations en matière de RGPD**.

Sur le cas particulier de la **charte informatique**, il est essentiel par exemple, si tel n'est pas déjà le cas de, notamment :

- définir ce qu'est une donnée à caractère personnel et un traitement de telles données ;

- rappeler les principes mis en place par le RGPD : transparence, recueil du consentement lorsque cela est nécessaire, la limitation des finalités, la minimisation des données collectées, la limitation de la conservation, la confidentialité et la sécurité ;

- expliquer les bonnes pratiques de recueil et de traitement des données à caractère personnel par les salariés auprès de tiers, clients, patients, prospects : loyauté, neutralité, précaution, transparence, sécurité de la collecte des données et de leur traitement ;

- rappeler les conditions d'usage des outils informatiques.■