Projet – Conformité réglementaire pour traiter et analyser des données

Membres du groupe :

- Manon BONNAUD-DUBOIS
- Christie NTOLANI
- Maël CHAINE
- Nathan BIGOT
- Thibault DAGUIN

Annexe : Fichier Excel recensant les données traitées par le service RH avec les informations suivantes : validité du traitement, finalité, base légale du traitement, temps de conservation (si connu)

Nous venons d'être nommés DPO au sein d'une société industrielle d'une centaine de salariés.

Rôle du DPO :

- Informer et conseiller l'entreprise sur ses obligations en matière de protection des données.
- Contrôler la conformité aux règles de protection des données.
- Coopérer avec la CNIL.
- Être le point de contact pour les personnes concernées et l'autorité de contrôle.
- Sensibiliser le personnel de l'organisme à la protection des données.
- Participer à l'évaluation des risques liés au traitement des données

Aujourd'hui notre priorité est la mise en conformité des traitements existants avec le RGPD.

1) Identifier les données personnelles collectées

Pour commencer, nous nous intéressons à une catégorie de données spécifique : les données personnelles. Le RGPD s'applique dès lors qu'une entreprise collecte et traite des informations permettant d'identifier une personne physique directement ou indirectement.

Dans le cas présent, nous avons une liste de traitements du service ressources humaines permettant :

- L'identification de l'employé
- Le suivi de la carrière et de la formation de l'employé

Vous trouverez en annexe l'intégralité des données traitées par le service RH avec les informations suivantes : validité du traitement, finalité, base légale du traitement, temps de conservation (si connu)

Nous reviendrons ici, essentiellement sur les données collectées qui posent ou peuvent poser problème dans le cadre de l'application du RGPD.

Comme ces informations peuvent être confidentielles nous considérons que seul le service RH aura accès aux données personnelles relatives aux ressources humaines.

Données relatives à l'identité :

- **Photographie** : Il est possible de demander une photographie au salarié c'est une donnée facultative, le salarié peut refuser ce traitement et l'employeur doit recueillir son consentement libre et éclairé.
- **Références du passeport** : Ce traitement est possible mais uniquement pour les personnels amenés à se déplacer à l'étranger (comme pour les commerciaux par exemple si l'entreprise à une clientèle internationale)

- **Situation familiale, situation matrimoniale, enfants à charge** : Ce traitement est possible mais est conditionné au principe de pertinence (ces données peuvent être utiles si l'employé bénéficie de la mutuelle d'entreprise, de la prévoyance et/ou du CSE)
- **Nature des études suivies par les enfants** : Le principe de pertinence s'applique ici, la nature des études suivies par les enfants n'est pas pertinente dans un registre du personnel
- **Profession des parents** : Idem, le principe de pertinence s'applique également, cette information n'est pas pertinente.

Données relatives à la situation professionnelle, au titre d'autorisation de travail et aux personnes à prévenir en cas d'urgence

Les données collectées sont valides et pertinentes, toutefois comme précisé précédemment ces données ne pourront être accessible qu'aux personnes autorisées au sein du service RH. Certaines de ces données sont également des données sensibles (comme la RQTH) et un soin particulier à la sécurité du fichier peut être apporté.

Données relatives à la gestion de la carrière du salarié

Les données collectées sont valides, toutefois les données de recrutements d'un employé ne peuvent être conservées indéfiniment.

Si la finalité est atteinte (emploi en CDI par exemple), les données doivent être supprimées. Sinon, avec le consentement de la personne la candidature peut être conservée pendant 2 ans en vivier.

Données relatives à l'évaluation professionnelle du salarié

Ici, nous avons 2 données interdites de collecte : l'appartenance syndicale et le nombre de jours de grève. Ces données présentent un caractère sensible qui en restreint la collecte.

Une exception toutefois existe, l'employeur peut avoir accès aux informations des salariés élus représentants du personnel (nature du mandat et syndicat d'appartenance autorisés à la collecte). La conservation de cette donnée est limitée dans le temps, jusqu'à 6 mois en base active après la fin du mandat et 6 ans en archivage intermédiaire (prescription pénale pour un délit).

Données relatives au suivi administratif des visites médicales des employés

Ici une donnée pose problème, l'indication des pathologies des salariés. C'est une donnée sensible que la médecine du travail ne communique pas à l'employeur et que l'employeur ne peut pas collecter.

Il existe toutefois une exception, l'employeur est en droit de connaitre les informations liées aux accidents du travail causés dans l'entreprise et/ou aux maladies professionnelles contractées dans l'entreprise.

2) Constitution du registre des activités de traitement (RAT)

Une fois les traitements de données identifiés, nous conseillons de supprimer l'intégralité des données interdites et non pertinentes. Nous conseillons également de mettre en place un registre des activités de traitement (RAT) pour consigner ces informations. Cela permettra d'identifier clairement la finalité de chaque traitement et le temps de conservation des données.

En effet les informations indispensables à inscrire dans le RAT sont :

- l'identité (nom, prénom, coordonnées) du responsable de traitement : ici le responsable légal de l'entreprise

- l'identité du DPO (Nous)

- les finalités de chaque traitement

- une description des personnes concernées et de données personnelles traitées

- les catégories de destinataires auxquels les données personnelles seront communiquées

- le cas échéant, les transferts de données vers un pays tiers et les données communiquées

- dans la mesure du possible, les délais de conservation des données

- une description générale des mesures de sécurité techniques et organisationnelles

3) Veiller à la sécurité des données

Dans le RAT nous avons dû décrire les mesures de sécurité apportées pour sécuriser les traitements, nous pouvons ici détailler nos préconisations en la matière.

Nous avons déjà dit que les fichiers liés aux données des ressources humaines ne devaient être accessible qu'aux personnes habilitées au sein de ce service.

Nous recommandons également de mettre en place plusieurs mesures à prendre tel que :

- Changer régulièrement des mots de passe, en utilisant des mots de passe dit "fort"
- Mettre à jour fréquemment ses logiciels et antivirus, avoir un pare-feu
- Déterminer une charte informatique à respecter au sein de l'entreprise
- Informer et sensibiliser les personnes
- Déterminer un identifiant et des habilitations propres à chaque utilisateur. C'est à dire limiter l'accès à certaines données uniquement pour certains utilisateurs.
- Sécuriser le matériel utilisé et le réseau informatique, les postes de travail, les serveurs, les sites web, les locaux, chiffrage des données, sauvegardes régulières ...
- Détruire les archives obsolètes et avant leur mise au rebut

Une étude d'impact permet d'évaluer les risques probables au traitement de données personnelles et déterminer les mesures nécessaires afin de diminuer les risques.

-> L'étude doit normalement être effectué avant la récolte des données
-> Si le niveau de risque est élevé, l'étude doit être soumise à la CNIL ou en cas de demande de la CNIL.

Nous conseillons donc de réaliser une "étude d'impact" quand le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées :

- Soit le traitement apparait dans la liste des types d'opération de traitement dans lesquelles la CNIL impose la réalisation d'une analyse d'impact.
- Soit le traitement correspond au moins à 2 des 9 critères suivant :
    - Évaluation/scoring (y compris le profilage)
    - Décision automatique avec effet légal ou similaire
    - Surveillance systématique
    - Collecte de données sensibles ou données à caractère hautement personnel
    - Collecte de données personnelles à large échelle
    - Croisement de données

- Personnes vulnérables (patients, personnes âgées, enfants, etc.)
- Usage innovant (utilisation d'une nouvelle technologie)
- Exclusion du bénéfice d'un droit/contrat

4) Informer les personnes sur leurs droits vis-à-vis des données personnelles

- **Permission, opposition et rectification**

Pour la collecte des données sensibles et la réutilisation des données à d'autres fins il faut le consentement préalable des salariés ou des clients. De plus, le responsable de traitement ne doit traiter que des données pertinentes.

Toute personne a le droit de s'opposer, **pour des motifs légitimes**, au traitement de ses données, sauf si celui-ci répond à une obligation légale (ex : fichiers des impôts). C'est le droit à l'opposition.

Toute personne a le droit d'exiger que ses données soient, selon les cas, complétées, mises à jour, supprimées ou rectifiées. C'est le droit de rectification. Par exemple un salarié de votre entreprise peut demander à retirer sa photo de la base de données. Un client peut demander la rectification de son adresse email.

- **Droit d'accès et de portabilité**

Vous devez donner l'accès à ses données à toute personne qui demande les données qui la concerne. Elle peut très bien les réutiliser ou les transmettre à un autre responsable de traitement (article 20 du RGPD). C'est le droit à la portabilité. Par exemple, un salarié voulant changer de société peut demander à récupérer toutes les données la concernant pour les confier à une autre entreprise.

Toute personne liée à votre entreprise peut demander à votre responsable de traitement sur quelles informations il s'est fondé pour prendre une décision la concernant. C'est le droit d'accès (article 15 du RGPD). Par exemple, un employé peut demander les données qui auraient servi au responsable de traitement motivant le refus de sa promotion. S'il constate que cette décision a été influencé par sa pathologie, il peut poursuivre votre entreprise pour préjudice moral.

- **Droit de recours et de réparation du dommage matériel ou moral**

Des personnes liées à votre entreprise, ayant subi des dommages matériels ou moraux, peuvent porter plainte contre vous. Soit auprès de la CNIL ou auprès des associations de consommateurs nationales agréées. C'est le droit de réparation du préjudice subi (article 82 du RGPD). Prenons un exemple, un salarié peut porter demander réparation d'un préjudice s'il constate que la société inclue dans sa base de données le nombre de jours de grève suivis au cours des 10 dernières années, car ces données peuvent être utilisées à l'encontre du salarié.

- **Les limites d'accès**

Cependant, en tant que responsable de traitement vous pouvez limiter les droits d'accès. Vous pouvez refuser à une personne qui demande de manière abusive, répétitive ou systématique les données (par exemple, un client qui demande une copie intégrale d'un enregistrement toutes les semaines).