NUMERIQUE

Protection des données personnelles :

Quelles obligations pour l'employeur vis-à-vis des salariés ?

Janvier 2020

A retenir :

- Le Règlement général de la protection des données (RGPD) entré en application en mai 2018 vient compléter le code du travail sur ce sujet. Les règles du code du travail continuent à s'appliquer.

- Le RGPD pose le principe de la Responsabilisation de l'employeur dans le traitement des données personnelles des salariés. Nous passons d'une notion de « *formalités préalables* » (déclaration, demande d'autorisations par l'employeur) à une logique de conformité, sous le contrôle et avec l'accompagnement du régulateur qui est la Commission Nationale Informatique et Libertés (CNIL).

- Les obligations faites à l'employeur découlent des exigences imposées par le RGPD à tout responsable de traitement de données. Elles prennent la forme de Responsabilité (Accountability) conféré au responsable de traitement, de respect de principes édictés par le RGPD devant être mis en œuvre pour chacun des traitements, ou enfin d'obligations directement inscrites dans un des 99 articles du RGPD.

- Nous recensons dans cette fiche qui vient compléter la Charte CFE-CGC Ethique et Numérique RH, les obligations de l'employeur devant particulièrement être suivie syndicalement. Elles sont au nombre de 5 :
  - Une obligation d'informer les salariés du traitement de leurs données ;
  - Une obligation de tenir un registre des traitements ;
  - Une obligation de préserver les salariés d'un risque élevé pour leurs droits et libertés ;
  - Une obligation d'assurer la confidentialité et la sécurité des données à caractère personnel des salariés ;
  - Une obligation d'informer en cas violation des données à caractère personnel des salariés.

- Cette fiche vient compléter la Charte Ethique et Numérique RH réalisée par la CFE-CGC et le Lab RH, présentée en janvier 2018, actualisée en novembre 2018 suite à la relecture par la CNIL. Elle est également le pendant de la Fiche « protection des données personnelles : quels droits pour les salariés vis-à-vis de l'employeur ? ».

INTRODUCTION

Avec l'entrée en application du depuis mai 2018, le cadre français de la protection des données personnelles au travail a été renforcé. La loi Informatique et Liberté du 6 janvier 1978 ainsi que **le Code du travail** prescrivaient déjà des règles de protection dans l'utilisation des données personnelles des salariés sur leur lieu de travail ou dans le cadre de leur contrat de travail. Le RGPD vient compléter ce cadre. Ainsi, en matière de RH et de contrôle du travail, la protection des données est à la fois prévue par le code du travail et le RGPD.

Le grand changement apporté par le RGPD au regard de loi Informatique et Liberté de 1978 est la **responsabilisation** de l'employeur dans le traitement des données personnelles des salariés. Nous passons ainsi d'une notion de « *formalités préalables* » (déclaration, demande d'autorisations par l'employeur en amont du traitement) à une logique de conformité, sous le contrôle et avec l'accompagnement du régulateur qui est la Commission Nationale Informatique et Libertés (CNIL).

Considéré désormais comme Responsable de Traitement, l'employeur est garant de la protection des données des salariés. Il doit être en capacité de prouver à tout moment que les traitements qu'il organise sont justifiés, et qu'il respecte les règles relatives à la protection des données.

Eclairage sur la notion de Responsabilité
Un employeur a été jugé indirectement responsable de la fuite des données de plus de 5.000 de ses employés, alors même que cette fuite avait été provoquée par un autre employé sur la base d'une vengeance (Jugement de la *Haute cour de justice d'Angleterre et Pays de Galles ;* 1er décembre 2017 *"Morrisons").*
L'employeur a été tenu responsable de la conduite de cet employé dont la responsabilité civile voire pénale pourra le moment venu être engagée, sous certaines conditions.

Eclairage sur la notion d'employeur : tout employeur, quel que soit son secteur ou sa taille est soumis à ces obligations. La loi n° 2018-493 du 20 juin 2018 prévoit que la Cnil doit prendre en considération les besoins spécifiques des micro-entreprises, petites entreprises et moyennes entreprises.

Les obligations faites à l'employeur découlent des exigences imposées par le RGPD au responsable de traitement. Elles prennent la forme :

- de Responsabilité (Accountability) conférée au responsable de traitement,
- de principes édictés par le RGPD et qui doivent être mis en œuvre pour chacun des traitements,
- ou enfin d'obligations directement inscrites dans un des 99 articles du RGPD.

Parmi les obligations posées par le RGPD, 5 doivent particulièrement retenir une attention syndicale en raison des risques qu'elles engendrent pour le salarié en cas de dérive :

- une obligation d'informer les salariés du traitement de leurs données ;
- Une obligation de tenir un registre des traitements ;
- Une obligation de préserver les salariés d'un risque élevé pour leurs droits et libertés ;
- Une obligation d'assurer la confidentialité et la sécurité des données à caractère personnel des salariés ;
- Une obligation d'informer en cas violation des données à caractère personnel des salariés.

L'OBLIGATION D'INFORMATION DES SALARIES (PRINCIPE D'INFORMATION ET DE TRANSPARENCE)[1]

L'employeur a l'obligation d'informer les collaborateurs sur l'utilisation qu'il fait de leurs données personnelles, mais aussi du pourquoi il le fait, pour qui et comment.

Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance[2]. Le RGPD impose que cette information soit « **concise, transparente, compréhensible et aisément accessible ».**

Attention

Cette obligation d'information est la contrepartie au fait qu'en principe l'employeur n'a pas à recueillir le consentement du salarié sur le traitement de ses données dans le cadre du travail, celui étant dans un lien de subordination, obstacle à un consentement libre et éclairé. De ce fait, l'absence de recueil de consentement oblige l'employeur à fournir aux collaborateurs l'ensemble des informations donnant lieu à une collecte et un traitement.

Quelles sont les informations que l'employeur doit faire auprès des salariés ?

L'employeur doit notamment informer les collaborateurs des éléments suivants :

- La source des données personnelles lorsque celles-ci n'ont pas été recueillies directement ;
- La finalité des traitements pour lesquelles il utilise leurs données personnelles ;
- La base juridique du traitement, sans laquelle un traitement ne peut être licite (recueil du consentement, intérêt légitime du responsable de traitement, exécution du contrat de travail, obligation légale). Dans le cas où le fondement du traitement repose sur un intérêt légitime, l'employeur doit le faire connaître ;
- La durée de conservation des données personnelles.

Si l'employeur a recours à une prise de décision automatisée, il doit obligatoirement en mentionner l'existence ainsi que les conséquences prévues de ce traitement pour le collaborateur concerné.

En cas de transfert des données personnelles hors UE, l'employeur doit en informer les collaborateurs.

L'employeur doit faciliter l'exercice des droits des collaborateurs, et les informer des droits dont ils disposent (accès, rectification, effacement, portabilité, et possibilité d'introduire une réclamation auprès d'une autorité de contrôle) et leur communiquer les coordonnées du responsable de traitement et du délégué à la protection des données (DPD) lorsque ce dernier a été désigné.

[1] Article 14 du RGPD
[2] Article L.1222-4 du code du travail

Ainsi la CNIL a reconnu licite la mise en place par un employeur d'un traitement automatisé de données à caractère personnel ayant pour finalité la détection des anomalies concernant les paiements et remboursements des frais professionnels. La CNIL a vérifié notamment les mesures d'information des salariés[3].

Quelles sont les modalités d'information auprès des salariés ?

L'information doit être délivrée individuellement et par écrit, pour faciliter la preuve de la délivrance de l'information. L'information du CSE sur les moyens ou les techniques d'aide au recrutement, sur les traitements automatisés de gestion du personnel et la consultation sur les moyens et techniques permettant un contrôle de l'activité des salariés prévues par le Code du travail[4], ne se substituent pas à cette information individuelle

La CNIL préconise une information des salariés à chaque fois qu'il est demandé au salarié une information. Cela recouvre notamment les hypothèses de mises à jour de données administratives, d'entretien d'évaluation ou encore de demande de formation…Cela vise aussi l'hypothèse de la mise en place d'un dispositif de surveillance, selon des modalités qui relèvent de la détermination de l'employeur.

S'agissant du **support d'information**, il pourra s'agir d'un avenant au contrat de travail, d'une note de service, d'une information sur l'intranet, d'un courrier joint au bulletin de paye, etc.

S'agissant de la **collecte indirecte de données personnelles** (informations collectées par l'employeur au sujet du salarié auprès d'organismes tiers, comme l'Urssaf par exemple), la notice d'information devra reprendre les informations mentionnées ci-avant et être complétées par les catégories de **données personnelles collectées de manière indirecte** ainsi que la **source** de ces données.

Le plus syndical

Comme indiqué dans la Charte CFE-CGC Ethique et Numérique RH, il appartient aux représentants CFE-CGC de s'assurer que cette obligation d'information individuelle a bien été respectée. Nous vous invitons à voir les exemples d'informations types donnés par la CNIL et qui sont accessibles sur son site https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation. Sur cette base, il est important de savoir comment l'employeur assure en pratique cette information auprès des salariés (lettre d'information adressée à chacun des salariés, règlement intérieur, mention dans les contrats de travail…).

***Réflexe militant CFE-CGC** : l'obligation d'information du salarié découle du principe de loyauté dans l'exécution du contrat de travail. Dans le cadre d'accompagnement de personnes en passe d'être sanctionnée ou d'être licenciée pour un motif où l'employeur aurait eu connaissance d'information via des traitements cités ci-dessus, il est important de s'assurer que le salarié en question a bien été*

[3] Délibération du 3 mai 2018

[4] Article L.2312-38 du code du travail

informé de ce traitement spécifique des données, les éléments collectés pouvant être irrecevables si ce n'est pas le cas[5].

Nous préconisons également de susciter une discussion lors d'une réunion du CE ou du CSE sur la notion « d'intérêt légitime de l'employeur » pour aider à préciser les cas où ce motif serait invoqué pour justifier une collecte et un traitement de données.

Enfin, il peut être intéressant pour les représentants CFE-CGC de rencontrer le délégué à la protection des données (DPD DPO) désigné par l'entreprise (lorsqu'il y a plus de 250 salariés) pour au moins 2 raisons :

- ce dernier est en charge d'informer et de conseiller le responsable de traitement, l'employeur en l'occurrence, ainsi que ces employés. Il est donc utile de connaître la personne qui sera saisie de questionnement de l'employeur ou des salariés ;

- le DPD DPO présente chaque année son rapport d'activité au Conseil d'administration ainsi qu'au CSE. Il est donc utile de rencontrer en amont de ce rapport la personne qui le rédigera.

L'OBLIGATION DE TENIR UN REGISTRE DES ACTIVITES DE TRAITEMENT[6]

L'employeur d'une entreprise de plus de 250 salariés, en tant que Responsable de traitement, a l'obligation de tenir un registre. Selon le « principe de documentation » décrit dans la charte CFE-CGC Ethique et Numérique RH, l'employeur a l'obligation de consigner chaque traitement dans le registre des activités de traitement complétées, le cas échéant, de l'étude d'impact relative à la protection des données si celle-ci a été réalisée.

Véritable document de recensement et d'analyse, le registre participe à la documentation de la conformité au RGPD. Il permet d'identifier précisément :

- les parties prenantes (représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données,
- les catégories de données traitées,
- à quoi servent ces données (ce qui en est fait), qui accède aux données et à qui elles sont communiquées,
- combien de temps elles sont conservées,
- comment elles sont sécurisées.

A noter : La CNIL met à disposition sur son site un exemple de registre.

Ni le code du travail ni le RGPD ne prévoit l'accès au registre aux salariés ou à leurs représentants. La seule obligation est de le tenir à la disposition de la CNIL en cas de contrôle.

[5] Cass. Soc. 3 octobre 2018
[6] Article 30 du RGPD

Le plus syndical

Dans le cadre de la consultation de la CNIL en mai 2019 sur son projet de référentiel Gestion des Ressources Humaines, la CFE-CGC a répondu selon l'architecture proposée des différents types de données, en indiquant sa position sur les bases légales que pouvaient justifier chaque type de traitement (cf. infographie ci-dessous) :

De plus, comme indiqué dans la Charte Ethique et Numérique RH, la CFE-CGC préconise de demander la présentation annuelle du registre des traitements en CSE ainsi que les éventuelles études d'impact. Cela permet d'avoir une visibilité sur les règles utilisées dans les algorithmes et ce qu'il résulte de leur traitement, par le biais d'audit, si nécessaire, lors d'une commission du suivi des traitements des données que la confédération préconise dans la Charte, par exemple.

Cette demande de présentation annuelle au CSE du registre peut être fondée sur la compétence générale du CSE d'information et consultation sur la situation économique et financière qui comprend le développement technologique de l'entreprise[7]. Un refus de la part de l'employeur serait difficilement recevable dans la mesure où le registre correspond aux informations communiquées aux salariés et donc il n'y a aucun enjeu de confidentialité. De plus, la Charte CFE-CGC Ethique Numérique RH ayant été relue par la CNIL sans remarque de sa part sur ce point, nous pouvons affirmer que la CNIL entérine cette préconisation comme une bonne pratique.

[7] Article L.2312-25 du code du travail

L'OBLIGATION DE PRESERVER LES SALARIES D'UN RISQUE ELEVE POUR LEURS DROITS ET LIBERTES[8] (ANALYSE D'IMPACT A LA PROTECTION DES DONNEES)

Dès lors qu'un traitement de données personnelles est **susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées**, le RGPD impose une analyse d'impact à la protection des données (AIPD).

Concrètement, la CNIL a dressé une liste de types d'opérations de traitement pour lesquels elle estime obligatoire de réaliser une AIPD. Parmi les types d'opérations listées, certaines concernent potentiellement les salariés, telles que :

- Les traitements établissant des profils de personnes physiques à des fins de gestion des ressources humaine.
- Les traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés.
- Les traitements ayant pour finalité la gestion des alertes et des signalements en matière professionnelle
- Les traitements mutualisés de manquements contractuels constatés, susceptibles d'aboutir à une décision d'exclusion ou de suspension du bénéfice d'un contrat.

Le plus syndical

Ce point est à garder en mémoire dans le cas de défense de salarié faisant l'objet d'une sanction ou d'un licenciement à la suite de ce type de traitement. Il convient de vérifier que l'employeur a bien procédé à l'étude d'impact et de la demander.

Pour les autres traitements non listés, la CNIL considère qu'une AIPD doit être effectuée, si au moins **deux des neuf critères ci-dessous** sont concernés :

- Evaluation/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.

L'exemple que nous citons dans la charte CFE-CGC Ethique et Numérique RH est le cas suivant : une entreprise qui met en place un contrôle de l'activité de ses salariés doit réaliser une étude d'impact relative à la protection des données car le traitement remplit le critère de la surveillance systématique et celui des données concernant des personnes vulnérables (une entreprise recensant au moins une personne reconnue RQTH).

[8] Article 35 du RGPD

La réalisation de l'étude d'impact repose sur la double approche :

- une évaluation juridique du traitement algorithmique (analyse de la nécessité et de la proportionnalité par rapport aux principes et droits fondamentaux) ;
- une évaluation technique du traitement algorithmique (analyse des risques concernant la sécurité des données).

Si l'étude d'impact démontre que le traitement présente un risque élevé pour les salariés concernés par le traitement, l'employeur est tenu de consulter la CNIL afin d'étudier les mesures visant à en atténuer les risques[9].

Le Plus syndical

La CFE-CGC préconise que les analyses d'impact soient présentées en CSE en vue d'une consultation des élus. Cette consultation sera l'occasion de vérifier si toutes les données exigées sont nécessaires, si le traitement proposé prévaut sur les droits généraux à la vie privée (dont jouissent également les collaborateurs sur le lieu de travail) et si les mesures prises pour garantir que les atteintes au droit à la vie privée et au droit au secret des communications sont limitées au minimum.

Cette consultation peut être invoquée au titre de la consultation générale sur la gestion et l'évolution économique et financière de l'entreprise, à l'organisation du travail, à la formation professionnelle et aux techniques de production ainsi que sur toute introduction de nouvelles technologies10. Elle peut être aussi demandée au titre de la compétence spécifique du CSE sur la mise en œuvre de moyens de contrôle des salariés11.

La présentation annuelle du rapport du DPD DPO au CSE et au CA peut être l'occasion pour les représentants du personnel CFE-CGC de poser les questions sur l'existence des études d'impacts, les cas de recours et leurs résultats.

***Réflexe militant CFE-CGC** : Dans le cadre d'accompagnement de personnes en passe d'être sanctionnée ou d'être licenciée pour un motif où l'employeur aurait eu connaissance d'information via des traitements cités ci-dessus, il est important de réclamer auprès de l'employeur l'étude d'impact.*

[9] Article 36 du RGPD
[10] Article L. 2312-8 du code du travail
[11] Article L. 2312-38 du code du travail

L'OBLIGATION DE CONFIDENTIALITE ET DE SECURITE DES DONNEES A CARACTERE PERSONNEL DES SALARIES[12] (SUR LA SECURITE DES TRAITEMENTS)

L'employeur est tenu de garantir la confidentialité et la sécurité appropriées des traitements des données à caractère personnel qu'il organise. L'employeur doit s'assurer de la bonne protection des données, en particulier au regard de traitement inapproprié, de perte ou vol, et pouvoir démontrer la mise en place de mesures de sécurité appropriées. L'enjeu est de veiller à ce que les données à caractère personnel soient mises à l'abri de la curiosité des autres salariés ou de tiers.

Quelles sont les modalités de confidentialité et de sécurité ?

Selon le principe de sécurité du traitement que nous décrivons dans la charte Numérique et Ethique RH (repris du RGPD), l'employeur doit mettre en œuvre les moyens qui lui permette de garantir la confidentialité et la sécurité des traitements des données à caractère personnel, après avoir identifié les risques et les conséquences que ledit traitement peut engendrer sur la vie privée des collaborateurs.

La confidentialité peut passer par des droits d'accès strictement définis dans le cadre d'une politique d'habilitation. La CNIL recommande fortement le recours pour chaque salarié à un mot de passe individuel régulièrement changé et un mécanisme de verrouillage systématique des postes informatiques au-delà d'une courte durée de veille.

La sécurisation peut s'appuyer sur la technique de chiffrement ou encore de pseudonymisation[13].

Le défaut de respect de cette obligation conduira à des sanctions financières (amendes)[14] voire pénale si un délit est constitué, en cas de violation du secret professionnel (exemple divulgation d'un taux de prélèvement à la source)[15] et de non-respect des règles visant à assurer la protection des données à caractère personnelle[16].

Cette obligation de confidentialité et de sécurité des données est-elle une obligation de résultat ?

La question est légitime dans la mesure où, avec la mise en place du RGPD, le système statique de déclaration et de demandes d'autorisations est remplacé par un système dynamique d'auto-certification qui s'accompagne d'un renforcement de la responsabilité des responsables de traitement et sous-traitants. Il est précisé le responsable de traitement est responsable de toutes les violations de données à caractère personnel.

---

[12] Article 32 du RGPD

[13] Au sens du RGPD, la pseudonymisation est un principe qui énonce que le traitement des données à caractère personnel doit être effectué de telle façon que celui-ci ne puisse plus être attribué à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

[14] Délibération CNIL formation restreinte n° SAN-2019-006 du 13 juin 2019

[15] Article L.226-13 du code pénal

[16] Article L.226-21 du code pénal

Avant l'entrée en vigueur du RGPD, la CNIL estimait que cette obligation était une obligation de moyen[17].

Avec le changement de logique découlant du RGPD, il est possible de considérer que cette obligation tend à devenir une obligation de résultat[18].

Le plus syndical

Comme nous y faisons référence dans la charte Ethique et Numérique RH, La CNIL et l'Agence national de sécurité des systèmes d'information (ANSSI) rassemblent respectivement dans un guide et un Kit l'ensemble des mesures permettant de garantir la sécurité des données personnelles.

L'OBLIGATION D'INFORMATION EN CAS VIOLATION DES DONNEES A CARACTERE PERSONNEL DES SALARIES[19]

En cas de constatation de violation des données à caractère personnel des salariés, **l'employeur a l'obligation de notifier une violation de données à caractère personnel**, c'est-à-dire lorsqu'il a constaté une perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, et ce de manière accidentelle ou illicite.

Une information obligatoire à la CNIL

L'employeur dispose après constatation d'une violation d'un délai de 72h pour la notifier auprès de la CNIL selon la procédure prévue à cet effet. Il doit documenter sur un registre l'incident constaté, en y consignant les informations telles que la nature de la violation, le nombre d'enregistrement et de personnes concernées, les catégories de personnes touchées, décrire les conséquences liées à cette violation et les mesures prises pour éviter la reproduction d'une telle violation.

Une information sous condition du salarié concerné

Lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés du salarié, celui-ci, concerné par cette violation, doit également être prévenu à moins que l'employeur ait pris des mesures permettant la non exploitation des données (par un chiffrement par exemple) ou permettant la non réalisation du risque élevé d'atteinte aux droits et libertés.

Le plus syndical

La CFE-CGC préconise que l'obligation de sécurité incombant à l'employeur s'accompagne d'actions de sensibilisation et de formation des salariés sur ces enjeux de sécurité, qualifiés pour la CNIL de « précautions élémentaires » et qui y consacre une fiche spécifique .

[17] Délibération n°2014-298 du 7 août 2014
[18] Analyse Préventica du 15 mai 2018
[19] Articles 33 et 34 du RGPD

Comme nous l'indiquons dans la charte Ethique et Numérique RH, la formation des salariés permet d'acquérir une « culture de la donnée » mais également d'être sensibilisés aux enjeux de sécurité, à l'heure où les cyberattaques touchent de plus en plus d'entreprises. Cette formation peut être mise en place au titre de l'adaptation des salariés à l'évolution du poste de travail et à la veille au maintien de leurs capacités à occuper un emploi au regard des évolutions des technologies et des organisations, au regard des compétences numériques requises[20].

LES ACTIONS POSSIBLES EN CAS DE NON-RESPECT DES REGLES DE LA PROTECTION DES DONNEES PERSONNELLES PAR L'EMPLOYEUR

Lorsqu'un salarié ou un représentant du personnel constate une irrégularité dans le traitement des données personnelles, plusieurs actions sont possibles :

- **le signalement auprès du DPD DPO** désigné par l'entreprise. Indépendant de l'employeur (même s'il est salarié de l'entreprise), il est le conseil de l'employeur mais aussi des salariés dans la bonne application des règles de protection des donnés ;
- **le droit d'alerte** de la délégation des membres du CSE : si un délégué constate, notamment par l'intermédiaire d'un salarié, qu'il existe une atteinte aux droits des personnes ou aux libertés individuelles dans l'entreprise qui ne serait pas justifiée par la nature de la tâche à accomplir ni proportionnée au but recherché, il en saisit immédiatement l'employeur[21] ;
- Le signalement auprès de l'inspection du travail ;
- Le signalement auprès de la CNIL : https://www.cnil.fr/fr/plaintes/travail. La CNIL dispose d'un large arsenal de mesures destinées à vérifier que les employeurs respectent leurs obligations en matière de protection des données : effectuer un contrôle sur place, convoquer le responsable de traitement à une audition, contrôler en ligne. A l'issue de ses interventions, elle peut décider des sanctions.

[20] Article L. 6321-1 du code du travail

[21] Articles L.2312-5 et L.2312-59 du code du travail