Application du RGPD en matière sociale

Le règlement général sur la protection des données personnelles (RGPD), en application depuis le 25 mai 2018, impose aux entreprises et associations de nouvelles obligations notamment sur la protection des données à caractère personnel des salariés, et augemente les sanctions encourues par elles. Quelles sont les nouvelles règles que doit respecter l'employeur ? Quels sont les droits des salariés ? Présentation.

La loi n° 2018-493 du 20 juin 2018, promulguée le 21 juin 2018, a modifié la loi « informatique et libertés » du 6 janvier 1978 conduisant à l'entrée en vigueur du règlement européen général sur la protection des données personnelles du 27 avril 2016 (RGPD).

En pratique, le nouveau règlement européen sur la protection des données personnelles a dû nécessairement conduire les entreprises et les associations à modifier leurs pratiques en termes de gestion des données tant à l'égard des salariés embauchés qu'à l'égard des clients ou bénéficiaires des différentes structures.

En effet, le règlement européen connaît un impact conséquent en droit interne et a instauré de nombreuses nouvelles modifications et obligations à la charge des employeurs.

Le présent dossier juridique vise à balayer ces obligations précisément en matière sociale.

I. La mise en place d'outils au service du RGPD

La mise en place du RGPD, suite à la loi du 20 juin 2018 relative à la protection des données personnelles, a conduit à supprimer les déclarations préalables auxquelles étaient soumis les employeurs. Il s'agit dorénavant d'un système que l'on pourrait nommer d'« autocontrôle » qui doit conduire les entreprises et associations à démontrer à tout moment leur conformité quant au traitement de données avec le règlement général de protection des données.

Le RGPD consacre à ce titre deux points principaux concernant la protection des données personnelles. Il s'agit, d'une part, de la protection relative à la vie privée par défaut qui peut conduire l'employeur à ne recueillir que la quantité de données personnelles strictement nécessaires au but poursuivi et à prévoir l'étendue du traitement et une accessibilité limitée. Il s'agit par ailleurs, d'autre part, de la protection de la vie privée dès la conception qui exige des employeurs que les systèmes de traitement des données personnelles soient conçus dans le strict respect de la vie privée des salariés et des partenaires ou clients de la structure.

A. Le registre obligatoire des activités de traitement des données

En premier lieu, le respect du RGPD doit conduire toutes les structures à mettre en place et tenir à jour un registre des activités de traitement des données : cette formalité est obligatoire pour toutes les entreprises ou associations qui traitent des données à caractère personnel.

La notion de traitement de données personnelles a posé question quant à son étendue. La Commission nationale de l'informatique et des libertés (CNIL) donne une définition très large et précise. Il s'agit de « *toutes opérations ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction…)* ».

L'obligation de tenue du registre des activités de traitement des données personnelles est cependant différente en fonction de la taille de la structure. Ainsi, dans les entreprises ou associations d'au moins 250 salariés, l'employeur a l'obligation de tenir un registre complet listant l'intégralité des activités de traitement automatisé des données personnelles.

Dès lors que la structure emploie moins de 250 salariés, l'employeur conserve l'obligation de tenir le registre de traitement des données mais son contenu est limité aux situations où le traitement des données est susceptible de comporter un risque pour les droits et les libertés des personnes concernées si ce dernier n'est pas occasionnel ou s'il porte sur des données à caractère sensible.

Il est à noter que le registre doit être mis à la disposition de la CNIL à sa demande : les employeurs n'ont pas à transmettre le registre de manière préalable automatique.

Le document peut se présenter sous la forme d'un écrit ou sous une forme électronique.

Il devra en toute hypothèse comporter un nombre minimal d'informations et a pour objectif de recenser et d'analyser les modalités de traitement des données personnelles de la structure. A cet effet, il devra identifier notamment les noms et les coordonnées du responsable du traitement et, le cas échéant, du délégué à la protection des données, l'ensemble des acteurs intervenant dans le traitement des données, les différentes catégories de données traitées par l'entreprise, les finalités de traitement, la durée de conservation de données et les moyens dont la structure dispose afin de les sécuriser.

En pratique, en matière sociale et plus précisément de ressources humaines, le registre devra intégrer nécessairement l'intégralité des systèmes de gestion de la paie, les fichiers relatifs au recrutement ou à la gestion du personnel, les dispositifs d'évaluation et de contrôle de l'activité des salariés mais également les messageries électroniques professionnelles pouvant être mises en place dans la structure.

Au sein du registre, la CNIL recommande la création de fiches dédiées à chaque activité recensée précisant l'objectif poursuivi, les catégories de données utilisées et les personnes ayant accès à ces dernières ainsi que la durée de conservation prévue pour chacune des données. Dans un second temps, la constitution du registre doit avoir pour finalité de permettre à l'entreprise ou l'association de s'interroger sur l'intérêt de la collecte des données effectuée : l'identification de traitement de données inutiles doit conduire à abandonner la pratique alors que l'identification de

traitement de données sensibles mais utiles doit avoir pour effet de hiérarchiser les risques encourus et mettre en place un plan d'action adapté aux besoins de la structure.

B. L'obligation de mener une analyse d'impact

Lorsque l'employeur identifie des traitements susceptibles d'engendrer un risque élevé pour les droits et les libertés des salariés, la personne nommée comme responsable dy traitement a l'obligation de mener une analyse d'impact intégral afin de recenser les caractéristiques du traitement, les risques afférents mais surtout les mesures adoptées afin de protéger les données de l'ensemble du personnel. Il s'agira notamment, toujours en matière sociale, des informations recueillies concernant la vie privée des salariés et notamment à titre d'exemple leur appartenance syndicale, l'état de santé ou encore la situation familiale.

La CNIL a fixé par délibération du 11 octobre 2018(1) une liste non limitative des différents types d'opérations de traitement devant conduire à une analyse d'impact de manière impérative. On pourra citer à titre d'exemple les traitements établissant des profils de personnes physiques à des fins de gestion des ressources humaines, les traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés, ou encore les traitements ayant pour finalité la gestion des alertes et des signalements en matière professionnelle.

On relèvera par ailleurs que l'analyse d'impact est également obligatoire lorsque le traitement remplit au moins deux des neuf critères prévus par la CNIL(2) permettant de caractériser un traitement susceptible d'engendrer un risque élevé devant conduire l'employeur à mettre en place une analyse d'impact. Les critères sont les suivants :

• traitement de données à grande échelle ;

• données sensibles à caractère hautement personnel ;

• données concernant des personnes vulnérables ;

• croisement ou combinaison des données ;

• évaluation ou « scoring » ;

• prise de décision automatisée avec un effet juridique ou similaire ;

• surveillance systématique de personnes ;

• traitement pouvant exclure du bénéfice d'un droit, d'un service ou d'un contrat ;

• utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles.

La délibération CNIL fixe de manière utile les contours des données déterminées comme sensibles et précise qu'il s'agira notamment de données relatives à l'origine raciale ou ethnique, des opinions politiques ou des convictions religieuses ou philosophiques, de l'appartenance syndicale, des données génétiques ou relatives à la santé, des données biométriques ou concernant l'avis ou l'orientation sexuelle des salariés.

Quant aux données déterminées comme étant à caractère hautement personnel, la CNIL précise

qu'il s'agira notamment de données relatives à la communication électronique ou encore de localisation ou relatives à la situation financière de la personne.

Attention : L'analyse d'impact doit en principe être menée avant toute mise en œuvre du traitement car il s'agit en réalité d'éviter au maximum un traitement inutile de certaines données. Cependant, lorsque le traitement est mis en place car nécessaire à l'entreprise ou l'association, l'analyse d'impact devra être mise à jour de manière régulière afin de vérifier le niveau du risque pendant l'intégralité de la durée du processus de traitement des données, intégrant une adaptation des mesures au regard des évolutions informatiques et électroniques.

II. La nomination d'un responsable de traitement des données

La mise en place d'un responsable de traitement est obligatoire quelle que soit la taille de la structure et qu'il s'agisse d'une entreprise ou d'une association. Ainsi, tout employeur doit pouvoir justifier de l'existence et de la réalité du responsable de traitement des données. La CNIL précise à ce titre que le responsable de traitement est une personne morale ou physique « *qui détermine les finalités et les moyens d'un traitement, c'est-à-dire l'objectif et la façon de le réaliser. En pratique et en général il s'agit de la personne morale incarnée par son représentant légal* ».

Le rôle du responsable du traitement est, en premier lieu, de recenser tous les cas de traitement existant au sein de la société et, en second lieu, de mettre en œuvre pour chaque traitement les mesures adaptées. Il appartiendra également à ce dernier d'accomplir l'ensemble des formalités déclaratives auprès de la CNIL lorsque ces dernières sont obligatoires.

Ainsi, en pratique, l'employeur peut prendre lui-même les fonctions de responsable de traitement au sein de sa structure. Il est également possible de confier cette tâche à un autre salarié. Cependant, il conviendra alors de prévoir expressément un avenant au contrat de travail précisant les fonctions et les responsabilités inhérentes à la désignation du responsable de traitement. Dans la mesure où cette nouvelle mission entraînera une augmentation de la charge de travail du salarié, l'avenant au contrat devra nécessairement comprendre la prise en compte, en termes de rémunération, de cette désignation.

Comme évoqué précédemment, un registre des activités de traitement des données doit impérativement être mis en place au sein des différentes structures. Cette obligation incombera au responsable de traitement sur lequel reposera l'obligation de veiller à éviter la violation des données personnelles et de notifier les violations qui pourraient présenter un risque pour les droits et les libertés des personnes à la CNIL.

L'ensemble du personnel devra être informé de l'existence du responsable de traitement des données et des coordonnées auxquelles les salariés pourront contacter ce dernier.

A. En cas de violation des données à caractère personnel

Le responsable de traitement doit identifier toute violation de données à caractère personnel et aura l'obligation d'intégrer l'incident au registre des activités de traitement. Un document récapitulatif indépendant devra également être rédigé intégrant la nature de la violation, les catégories et le nombre approximatif de personnes concernées par cette violation ainsi que le nombre d'enregistrements de données à caractère personnel concernés. Plus important, le responsable de traitement devra intégrer une description des conséquences probables de la

violation des données précitées et expliciter les mesures prises afin d'éviter que l'incident ne se reproduise.

D'autre part, dès lors que l'incident constitue un risque pour la vie privée des personnes concernées, et ici précisément des salariés, l'incident devra être notifié à la CNIL dans un délai de 72 heures après sa constatation.

Attention, en cas de dépassement du délai de 72 heures, le responsable du traitement devra expliquer, lors de la notification, les motifs du retard afin d'éviter toute condamnation par la CNIL.

A noter : La CNIL a mis en place un téléservice spécifique dédié aux responsables de traitement permettant de notifier à la commission la violation présentant un risque pour les droits et libertés des personnes.

B. Les données traitées par des sous-traitants

En pratique, il arrive régulièrement que l'employeur sous-traite une partie de la gestion de données à caractère personnel, par exemple en recourant à un cabinet d'expertise comptable, à un organisme de traitement de la paie, de conseil en recrutement ou encore un prestataire de vote électronique pour les élections des représentants du personnel.

L'employeur ne peut se déresponsabiliser en recourant à ces sous-traitants et conserve l'obligation de vérifier que les contrats de sous-traitance respectent la réglementation européenne et le règlement général de protection des données. On conseillera à ce titre aux structures de vérifier, suite à la mise en œuvre du RGPD et de la loi du 20 juin 2018, de solliciter l'ensemble des sous-traitants ou prestataires extérieurs afin de vérifier le contenu des clauses contractuelles. Elles devront dorénavant nécessairement intégrer les obligations du sous-traitant, la finalité du traitement et la durée de conservation des données dans le respect du RGPD.

Ce n'est que dans cette hypothèse que l'employeur sera réputé avoir rempli ses obligations en matière de traitement des données personnelles.

III. la désignation d'un délégué à la protection des données

La nomination d'un délégué à la protection des données est réservée de manière obligatoire dans trois situations particulières :

• organismes publics et autorités publiques ;

• structures dont l'activité de base en tant que responsable ou sous-traitant exige un suivi régulier systématique à grande échelle des personnes concernées ;

• structures ayant la qualité de responsable ou de sous-traitant dont l'activité consiste en un traitement à grande échelle de données caractérisées comme sensibles.

On précisera que la CNIL conseille de nommer un délégué à la protection des données en toute hypothèse même si la structure n'entre pas dans les situations considérées ci-dessus, compte tenu des sanctions encourues en cas de manquements.

A noter : La CNIL ne définit pas précisément les notions d'« activité de base » ou de « traitement

à grande échelle des données ». Il est donc difficile de déterminer quels types de structures entrent dans ces catégories. Ainsi, on pourra considérer que les entreprises de travail temporaire intègrent aisément cette catégorie car elles traitent de données à caractère personnel à grande échelle au vu de leur activité principale. Dans le cadre du secteur des services à la personne, la question peut également être valablement posée. En effet, les besoins structurels de main-d'œuvre, comme le fait d'exécuter une prestation de travail auprès de publics âgés, handicapés ou d'enfants au domicile de ces derniers, conduisent à accéder à un nombre de données à caractère sensible ou personnel important pouvant par ailleurs relever également de l'état de santé des personnes.

La nomination du délégué à la protection des données (DPO – Data Protection Officer) ne doit pas être prise à la légère. En effet, le RGPD fixe des obligations bien plus exigeantes que celles qui étaient prévues pour l'ancien correspondant à la protection des données. Ainsi, la structure devra pouvoir justifier de l'expertise du délégué à la protection des données : le DPO doit avoir des connaissances spécialisées en droit et sur les pratiques en matière de protection des données. Il a également l'obligation d'entretenir ses connaissances. On retrouvera à ce titre sur le site de la CNIL les conditions permettant la désignation du DPO réparties en trois catégories :

• compétences requises ;

• moyens suffisants ;

• capacité d'agir en toute indépendance.

Il n'est donc pas question de nommer un salarié de l'entreprise ou de l'association sans vérifier qu'il dispose des compétences spécifiques. On relèvera également que la notion d'« indépendance du délégué » est une condition essentielle du RGPD, ce qui doit conduire l'employeur à envisager la désignation d'un délégué extérieur à l'entreprise ou l'association ou encore le recrutement d'un salarié dans le but exclusif d'assurer cette mission.

Dès lors que l'indépendance est une condition essentielle à l'exercice des missions du DPO, le RGPD rappelle que le délégué ne peut recevoir d'instructions concernant ses missions.

Ainsi, le responsable du traitement des données devra veiller à la conservation d'indépendance du DPO.

Il est toutefois intéressant de relever que le code du travail n'a pas intégré de protection spécifique pour le délégué à la protection des données qui pourrait être nommé à l'intérieur de la structure. Ainsi, les salariés exerçant les fonctions de délégué à la protection des données, malgré le bénéfice d'une indépendance, ne disposent pas du statut de salarié protégé. Il n'est pas utile de prévoir, par exemple en cas de licenciement, de solliciter l'autorisation de l'inspection du travail. Il est difficile de comprendre l'articulation entre l'indépendance et la protection contre toute sanction infligée en raison de l'exercice de sa mission avec l'absence totale de procédure dédiée comme cela peut être le cas pour un représentant du personnel ou encore un délégué syndical(1).

IV. L'information des salariés

La mise en conformité des entreprises et associations avec le règlement général de protection des données implique également une information des salariés présents dans la structure. En effet, l'employeur est par nature amené à collecter et traiter de nombreuses données personnelles

relatives aux salariés.

Le respect du RGPD impose à l'employeur d'informer les salariés mais également de recueillir leur consentement. En pratique, cela signifie que les employeurs doivent être obligés de modifier leurs pratiques.

En effet, ne serait-ce qu'en matière de recrutement, des employeurs collectent des données personnelles et il devient indispensable de vérifier l'utilité de la collecte des données et d'obtenir l'accord des candidats à l'embauche. Afin de satisfaire aux prescriptions du RGPD, il sera nécessaire de prévoir une fiche de recrutement intégrant l'autorisation de traitement des données et ses limites, outre une fiche d'informations concernant les droits relatifs à la collecte des données personnelles.

Il est à noter que le process de recrutement doit également être modifié quant aux documents qui seront conservés par l'employeur, que le candidat soit retenu ou non. A ce titre, le responsable du recrutement devra, pour chaque document, s'interroger sur l'utilité réelle de sa conservation. De surcroît, certains documents ne pourront demeurer en la possession de l'employeur. On pourra soulever la problématique de la demande de l'extrait de casier judiciaire. Ce n'est que lorsque le salarié sera amené à exercer des fonctions dites « sensibles » que l'employeur pourra, par exemple dans le cadre de l'autorisation de certaines activités de services à la personne, vérifier le casier judiciaire du salarié et le conserver mais uniquement dans les délais fixés par les textes.

En l'absence de texte spécifique, l'employeur aura la faculté de solliciter l'extrait de casier judiciaire du candidat afin d'en vérifier les antécédents mais ne pourra alors en conserver une copie.

Le RGPD ne fait pas mention des modalités pratiques à mettre en place afin d'en respecter les termes. On peut cependant penser qu'un formulaire à remplir par le candidat devrait permettre le respect de la réglementation. Le formulaire devra alors comprendre *a minima* des informations permettant de fixer la finalité du traitement des données personnelles, son fondement juridique et les destinataires de ces données, leur durée de conservation et l'ensemble des droits des salariés intégrant la demande de rectification ou d'effacement de données, le droit d'opposition et les coordonnées des personnes à contacter concernant le traitement de leurs données.

Une fois la phase de recrutement achevée, l'employeur aura l'obligation d'informer de manière plus précise le salarié du traitement de ses données dans le cadre de la relation de travail. A ce titre, on pourra penser naturellement à l'introduction d'une clause dans le contrat de travail du salarié informant ce dernier du traitement des données à caractère personnel.

Cependant, si la clause semble indispensable pour tout nouveau contrat de travail, elle demeure insuffisante au regard de la finalité du règlement intérieur de protection des données et des obligations mises à la charge de l'employeur. On conseillera la mise en place d'une notice ou d'un formulaire détaillé paraphé et signé par le salarié qui permettra de garantir au mieux le consentement de ces derniers.

Quant aux salariés déjà embauchés, l'introduction d'une clause contractuelle ne semble pas envisageable et on préférera alors mettre en place une lettre d'information relative au RGPD qui comprendra en annexe la notice fournie à tout salarié nouvellement embauché.

Comme dans le cadre de la fiche explicative relative au recrutement, la notice d'information aura

l'obligation de préciser la finalité du traitement des données personnelles, le fondement juridique et les destinataires des données ainsi que leur durée de conservation. Les droits des salariés devront être repris par ailleurs de manière détaillée.

V. Les droits des salariés

En premier lieu, tout salarié ou ancien salarié bénéficie du droit d'accès et de copie quant à l'ensemble des données personnelles qui ont été collectées par l'employeur.

En principe, la notice d'information ayant pris le soin de préciser le responsable du traitement, la demande devra lui être adressée. La loi du 20 juin 2018 prévoit que l'employeur dispose d'un délai de 1 mois pour donner suite à la demande du salarié.

Les employés bénéficient par ailleurs d'un droit de rectification et la loi fixe pour l'entreprise ou l'association l'obligation de rectifier les données personnelles inexactes dans les meilleurs délais. Il est intéressant de relever que le RGPD n'a pas fixé de délai spécifique à ce titre. On conseillera à l'employeur de respecter le délai prévu pour le droit d'accès et de copie.

Les salariés continuent à bénéficier d'un droit d'opposition (présent au sein de l'ancienne loi « informatique et libertés ») à un traitement des données personnelles, notamment lorsqu'ils contestent la légitimité des motifs poursuivis par l'employeur et plus précisément le responsable de traitement ou le délégué à la protection des données.

Le RGPD consacre également un droit à l'oubli, aussi dénommé « droit à l'effacement », qui permet au salarié de demander un effacement de l'ensemble des données qui ont été collectées par l'employeur. Une exception sera retenue lorsque l'employeur est en mesure de justifier du caractère d'intérêt général du traitement des données ou que ce dernier est nécessaire dans le cadre d'un litige juridique.

Enfin, en complément de ses autres droits, le salarié dispose d'un droit à la limitation. A ce titre, en cas de contestation de l'exactitude des données personnelles ou d'opposition au traitement de données personnelles, le salarié peut demander à son employeur de ne plus utiliser les données concernées mais toutefois de les conserver jusqu'à ce qu'il formule une réponse au problème soulevé.

Une portabilité des droits des salariés a été mise en place par le RGPD et devra permettre de récupérer les données et de les réutiliser à titre personnel. On pourra penser dans le cadre du droit social, et plus précisément de la gestion des ressources humaines, à des données relatives au recrutement du salarié ou à la paie. Le RGPD fixe un délai maximal de 1 mois à compter de la réception de la demande en principe. Le responsable du traitement des données a la faculté de rejeter la demande si les conditions du droit à la portabilité ne sont pas réunies. Cependant, dans cette hypothèse, le responsable aura l'obligation d'informer le demandeur du refus, du motif et de son droit de porter un recours auprès de la CNIL.

VI. Les sanctions encourues par l'employeur

La CNIL joue un rôle essentiel dans la mise en œuvre et le respect du RGPD. Elle dispose à cet effet de pouvoirs spécifiques. En premier lieu, elle intervient en tant que conseil afin d'accompagner les entreprises et les associations dans leurs démarches de conformité à la réglementation en vigueur.

Elle est également chargée de traiter les réclamations portées par les salariés et d'effectuer des contrôles des différentes structures. En ce sens, suite à un dépôt de plainte ou un contrôle, elle peut être amenée à prononcer des sanctions.

Les sanctions pouvant être prononcées par la CNIL ont été modifiées suite à l'entrée en vigueur du RGPD et de la loi rectificative du 20 juin 2018. Ainsi, la CNIL conserve une partie des pouvoirs dont elle disposait auparavant mais en obtient des supplémentaires.

Auparavant, la CNIL avait la faculté de prononcer des avertissements, mises en demeure, injonctions de cessation de traitements automatisés mais encore des sanctions pécuniaires. En cas de menace pour les libertés ou d'urgence, la CNIL disposait également de la faculté de recourir à une procédure d'interruption de la mise en œuvre du traitement des données ou d'un verrouillage des données traitées. Cette procédure ne pouvait toutefois intervenir qu'après respect du principe du contradictoire et pour une durée maximale de 3 mois. Dans cette hypothèse, la CNIL pouvait également saisir le juge des référés en cas d'atteinte grave et immédiate aux droits et libertés.

Au-delà de l'éventail des pouvoirs de sanction que possédait la CNIL, le RGPD renforce ces derniers et la commission dispose dorénavant de nouvelles mesures. Ainsi, la CNIL a la faculté de condamner les entreprises à une amende administrative en cas de violation du RGPD. La loi du 20 juillet 2018 précise que l'amende et son montant devront être fixés en tenant compte de la nature, de la gravité et de la durée de la violation mais également de la finalité du traitement concerné, du nombre de personnes qui auront été concernées ainsi que du niveau de dommages subi par ces dernières.

En pratique, le RGPD dresse une liste de violations pouvant être punies d'une amende limitée soit à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent ou 10 millions d'euros (la CNIL retiendra le montant le plus élevé des deux), soit, pour la seconde liste de violations, à une amende pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires.

La première amende limitée à 2 % du chiffre d'affaires annuel mondial ou 10 millions d'euros peut être prononcée en cas de violation des obligations générales à la sécurité des données, de l'obligation d'analyse d'impact ou de la désignation d'un délégué à la protection des données. L'amende pouvant atteindre 4 % du chiffre d'affaires ou 20 millions d'euros est quant à elle applicable en cas de violation des droits des personnes ou du non-respect d'une injonction émise par la CNIL.

Conseils pratiques pour sécuriser le stockage des données

La CNIL recommande vivement aux entreprises de mettre en place des mesures adaptées afin de garantir la sécurité des données personnelles des salariés.

On conseillera ainsi à chacun d'observer des réflexes simples : mettre à jour les antivirus, opérer des changements des mots de passe en utilisant notamment des chiffres, des majuscules et des caractères spéciaux, sauvegarder régulièrement les données sur des équipements fiables et sécurisés et veiller à ne pas mettre des données professionnelles sur des équipements personnels (ex. : clé USB).

La place du CSE dans le traitement des données à caractère personnel

Le code du travail a mis en place l'obligation d'information du comité social et économique (CSE) préalablement à l'introduction dans l'entreprise ou l'association de traitements automatisés de gestion du personnel et de toute modification de ces derniers. Il est donc impératif pour l'employeur de respecter cette obligation fixée par l'article L. 2312-38 du code du travail, sous peine de voir caractériser un délit d'entrave au fonctionnement de l'institution représentative du personnel.

Modèle de clause à insérer au contrat de travail RGPD – traitement des données personnelles

La loi n° 2018-493 du 20 juin 2018, promulguée le 21 juin 2018, a modifié la loi « informatique et libertés » du 6 janvier 1978 conduisant à l'entrée en vigueur du règlement général de protection des données (RGPD).

Dans le cadre de la gestion du personnel et aux fins du traitement de la paie, la société < *à compléter* > est conduite à solliciter des données personnelles concernant le salarié, intégrant notamment sa situation familiale, coordonnées bancaires, numéro de téléphone, numéro de sécurité sociale, date et lieu de naissance, adresse et adresse mail. Ces données font l'objet d'un traitement par la société représenté par < *Nom, Prénom du responsable des traitements* >, < Adresse mail dédiée >, en sa qualité de < *Fonction / Poste* > considéré comme étant le responsable de ces traitements.

En signant le présent contrat, le salarié autorise la société à collecter, enregistrer et stocker ces données qui ne seront traitées et utilisées que dans la mesure de ce qui est nécessaire à l'exécution du contrat de travail, à l'accomplissement par la société des obligations qui lui incombent et dans la limite des délais de prescription applicables en matière sociale.

Outre les services de la société habilités à les traiter en raison de leur rôle, les destinataires de ces données sont strictement limités à ce jour aux organismes et personnes suivantes : < *à compléter en fonction des destinataires réels de traitement des données dans l'entreprise ou l'association concernée* >.

Une notice explicative relative aux traitements des données à caractère personnel et à la protection de ces dernières est remise en annexe au présent contrat. En outre, en cas de difficultés liées à la gestion de ses données, le salarié a enfin la possibilité d'introduire une réclamation auprès de la CNIL : tél. 01 53 73 22 22 – site Internet www.cnil.fr.

Modèle de lettre d'information RGPD

Fait à < *lieu* >, le < *date* >

Objet : Protection de vos données à caractère personnel

Madame, Monsieur,

Compte tenu de l'entrée en vigueur depuis le 25 mai 2018 du règlement général sur la protection des données (RGPD) issu du règlement communautaire n° 2016/678 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, la société < *à compléter* > effectue une mise à jour de ses pratiques concernant la protection des données à caractère personnel traitées.

Dans ce cadre, vous trouverez joint ci-après une notice explicative permettant de vous informer quant à l'utilisation de vos données à caractère personnel ainsi que de vos droits à cet égard. Vous trouverez également, au terme de cette notice, les obligations en tant que salarié de l'entreprise dans la protection des données des clients auxquelles vous avez accès dans le cadre de vos fonctions et compte tenu de l'activité spécifique de la société dans le secteur des services à la personne.

Vous trouverez également ci-joint un mandat d'affiliation aux organismes sociaux.

Vous souhaitant bonne réception des présents documents.

Je vous prie de croire, Madame, Monsieur, en l'expression de mes sincères salutations.

< Qualité / Nom / Prénom >

Signature

Notes

(1) Délibération CNIL n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise, J.O. du 6-11-18.

(2) Délibération CNIL n° 2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données prévues par le RGPD, J.O. du 6-11-18.

(1) Voir notamment Rép. min. à QE n° 2000896, J.O. Sén. [Q.] du 7-02-19, p. 712.

Auteur

- Alison Dahan