DONNÉES PERSONNELLES

DRH connectée : son rôle et sa responsabilité dans la conformité RGPD

La question de la conformité au RGPD des données personnelles des salariés doit être au cœur des préoccupations des DRH désormais obligés d'appréhender sur le plan juridique cette règlementation.

Alors que les ressources humaines (RH) ne cessent de recourir aux moyens informatiques dans le cadre de leurs activités (notamment pendant la phase de recrutement, la gestion des carrières et le suivi du temps de travail), que les dispositifs de contrôle des salariés se multiplient, que le recours au télétravail s'institutionnalise depuis la crise sanitaire et que la possibilité laissée aux salariés d'utiliser leurs propres outils dans le cadre du BYOD (Bring Your Own Device ou « *prenez vos appareils personnels* ») se démocratise, la question des données personnelles des salariés est au cœur des préoccupations des entreprises qui doivent appréhender sur le plan juridique cette question délicate.

En effet, l'employeur est amené à recueillir un nombre important de données personnelles des salariés pour traiter notamment des questions relatives à la rémunération, aux déclarations sociales obligatoires, à la tenue du registre unique du personnel, à la gestion administrative du personnel, à l'organisation du travail, ou encore à l'action sociale qu'il prend en charge.

Ces données doivent être traitées dans le respect du règlement européen sur la protection des données (RGPD) qui encadre depuis plusieurs années tout traitement des données personnelles, en ce inclus le traitement par l'employeur des données personnelles de ses salariés, pour assurer le respect du principe de protection de la vie privée.

À défaut de respect, l'employeur s'expose notamment à de lourdes sanctions administratives (jusqu'à 4 % du chiffre d'affaires annuel mondial ou 20 millions d'euros, le montant le plus élevé étant retenu) et à une médiatisation forte de toute violation, portant ainsi atteinte de manière irrémédiable à la réputation et l'attractivité de l'entreprise.

Dans le cadre de la conformité du RGPD, la direction des ressources humaines a un rôle clé qui doit la conduire à prêter une attention particulière aux traitements des données personnelles des salariés de l'entreprise.

Données des salariés et RGPD

Les données des salariés protégées par le RGPD

Le RGPD s'appliquant à tout traitement des données personnelles, les données personnelles des salariés, des apprentis, des stagiaires et des intérimaires sont donc également concernées par le RGPD. Pour rappel, une donnée personnelle est définie par le RGPD comme étant « *toute information se rapportant à une personne physique identifiée ou identifiable* » (« *personne concernée* »). A titre d'exemples, il s'agira du nom, prénom, numéro de sécurité sociale, adresse email (personnelle ou professionnelle), numéro de téléphone personnel, numéro du poste téléphonique, date de naissance, date d'arrivée dans l'entreprise, etc.

L'employeur pourrait également être amené à traiter des données sensibles de ses salariés (données concernant la santé, la vie sexuelle, données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale). Le traitement de ces données est par principe interdit sauf exceptions encadrées par un régime de protection renforcé.

Un traitement est défini de manière très large par le RGPD et peut ainsi recouvrir la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Les données personnelles des salariés doivent donc être traitées en conformité avec le RGPD. Si toutes les règles du RGPD s'appliquent

sans exception, dans ce cadre, il existe néanmoins des spécificités du simple fait que les traitements portent sur des données de salariés. Nous en relèverons trois, étant entendu qu'elles ne sont pas exhaustives et que d'autres spécificités s'appliquent aux données personnelles des salariés.

Les spécificités du RGPD s'agissant des données des salariés

D'abord, en matière RH, les bases légales que l'on retiendra plus facilement pour traiter des données des salariés sont la nécessité d'exécuter le contrat de travail (notamment pour la gestion de la paie), de respecter une obligation légale (par exemple avec l'obligation de communiquer des informations salariales à l'administration fiscale) ou encore la poursuite d'un intérêt légitime par l'employeur (par exemple, la conservation de documents en cas de contentieux). Le consentement est quant à lui considéré comme une base légale à éviter pour les salariés sauf lorsqu'aucune conséquence négative ne résultera de leur refus de donner leur consentement. Les traitements effectués dans le cadre des opérations de recrutement ne pourront, par exemple, pas être fondés sur le consentement des candidats, un refus de leur part pouvant affecter leurs chances d'obtenir un emploi (ou certains types d'emplois). A l'inverse, l'enregistrement de l'image ou de la voix d'employés pour la production d'un clip promotionnel dans un espace de travail, pourra être fondé sur leur consentement, mais à la condition que le refus n'ait aucun impact à leur égard.

Ensuite, l'employeur ne peut pas collecter toutes les données et doit être particulièrement vigilant à certaines données qui ont un régime de protection spécifique. A titre d'exemple, l'usage du numéro de sécurité sociale (« *NIR* »), contenant de nombreuses informations personnelles (date et lieu de naissance, numéro unique), est limité par décret (n°2019-341 du 19 avril 2019) à certains secteurs (protection sociale, santé, travail, fiscalité) et pour des finalités limitativement énumérées. L'employeur n'est donc en principe pas autorisé à collecter et traiter cette donnée, sauf dans certains cas, notamment pour lui permettre de remplir ses obligations déclaratives nécessitant l'utilisation du NIR ou de réaliser les opérations de traitement de la paie. En revanche, le NIR n'a notamment pas à figurer sur un contrat de travail ou sur le registre du personnel et ne doit pas être demandé au stade du recrutement de la personne concernée.

Enfin, s'agissant des durées de conservation, elles devront nécessairement être établies à l'aune de certains délais de conservation imposés par le droit du travail, les délais de prescription légale, sans oublier les durées recommandées par la Cnil dans ses référentiels portant sur certains traitements de données. Or, une même donnée peut parfois avoir plusieurs utilités successives ce qui implique donc des durées de conservation différentes. Dans cette perspective, si des données ne sont plus utilisées au quotidien, mais qu'elles sont conservées en cas de contentieux ou afin de respecter une obligation légale, elles devront être archivées. Cet archivage devra être fait en bonne et due forme et l'entreprise ne devra pas se contenter de conserver les données en base active en mentionnant simplement qu'elles sont archivées. Au contraire, les données archivées ne devront être accessibles qu'aux services spécifiques qui doivent y accéder. En outre, un processus de gestion des archives devra être défini, tout comme le mode opératoire de destruction de celles-ci.

Conformité au RGPD : quel rôle et quelle responsabilité pour le DRH ?

Le RGPD a érigé un principe général de responsabilité pour rendre effective la protection des données personnelles. En vertu de ce principe, toute entité traitant de telles données est contrainte de mettre en œuvre des mécanismes et procédures internes afin d'être en mesure de s'assurer et de démontrer, à tout instant, le bon respect des règles relatives à la protection des données. Il convient dès lors de déterminer les acteurs et coresponsables de l'application du RGPD et en particulier le rôle du DRH.

Le rôle central du DRH dans la conformité au RGPD

Contrairement au DPO et aux services juridiques et informatiques, la direction des RH ne pilote pas, à proprement parler, la mise en œuvre des obligations du RGPD. Pour autant, le DRH conserve un rôle central dans la conformité du traitement des données personnelles des salariés.

Il doit généralement faire le lien entre les différents acteurs (en particulier entre les salariés et le DPO, ou référent RGPD si aucun DPO n'est désigné). Il a dans ce cas un rôle de coordinateur, d'assistant et de conseil. Pour les entreprises qui n'ont pas désigné de DPO ni de référent RGPD, le DRH sera alors généralement celui en charge du respect du RGPD dans le cadre du traitement des données personnelles des salariés. Il devient dans ce cas le véritable acteur de mise en conformité.

Son rôle vis-à-vis des salariés. Le salarié est à la fois sujet, puisque ce sont ses données qui font l'objet d'un traitement, ce qui lui confère des droits, et acteur du respect des règles internes mises en place par son employeur en matière de données personnelles. Le DRH doit donc s'assurer de la bonne information des salariés sur leurs droits et sur leurs obligations en matière de données personnelles. Les informations pourront être fournies aux salariés par tous les moyens utiles, et notamment par le contrat de travail, la formalisation de chartes, de notes de services ou encore des procédures écrites. Les informations doivent être concises, transparentes, compréhensibles et aisément accessibles.

Lorsqu'un salarié invoque un droit, le DRH doit également s'assurer que la demande est bien prise en compte dans les délais impartis par le RGPD. L'employeur est, en effet, contraint de répondre « *dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes* » (article 12(3) du RGPD). En l'absence de réponse, l'employeur pourra, soit faire l'objet d'une sanction administrative de la part de la Cnil, soit d'une procédure juridictionnelle dans la mesure où cette carence pourra être qualifiée de fautive et emporter la réparation de l'intégralité du dommage subi.

Un salarié peut, par exemple, être amené, sur le fondement de son droit d'accès, à exiger que lui soit communiqué l'ensemble des données de connexion à son poste de travail, ce qui lui permettrait d'établir la preuve, à l'occasion d'un éventuel contentieux, de son temps de travail et ainsi de solliciter le paiement d'heures supplémentaires.

Il doit également veiller à ce que les instances représentatives du personnel soient informées ou consultées avant toute décision d'installer un dispositif de contrôle des horaires ou d'accès aux locaux. Conformément à l'article L. 2312-8 du code du travail, l'employeur ne manquera pas de consulter et d'informer les instances représentatives du personnel avant la mise en œuvre de toute mesure relative à l'organisation, la gestion et la marche générale de l'entreprise (et notamment concernant « *l'introduction de nouvelles technologies, tout aménagement important modifiant les conditions de santé et de sécurité ou les conditions de travail* »).

Son rôle vis-à-vis de l'employeur dans la conformité au RGPD. Le DRH doit s'assurer que les procédures mises en place par l'entreprise seront bien respectées par les salariés et qu'elles seront suffisamment coercitives (et donc avec un pouvoir de sanction de l'employeur à l'égard du salarié en cas de non-respect) pour permettre leur effectivité. A défaut, l'employeur pourrait être en violation de ses obligations en ne mettant pas en œuvre les moyens suffisants pour assurer l'effectivité du RGPD. A ce titre, il devra identifier le meilleur moyen pour rendre opposables aux salariés ces règles mises en place par l'entreprise (tel que le contrat de travail ou le règlement intérieur).
Le DRH devra également, lorsque ce sera le cas, sanctionner le salarié qui a bafoué les règles relatives au RGPD qui lui sont opposables.
Dans le cadre d'une action disciplinaire, les données personnelles collectées au moyen de traitements conformes au RGPD constituent d'ailleurs un moyen de preuve essentiel à la défense de l'employeur dans le cadre des contentieux prud'homaux (comme la vidéosurveillance ou encore l'archivage de mails). Lorsqu'un salarié invoque le RGPD pour contester la recevabilité des preuves apportées par l'employeur, même lorsque la preuve est obtenue au travers d'un traitement de données illicites, la Cour de cassation a estimé que celles-ci pouvaient être admises dans la mesure où la production est indispensable à l'exercice du droit à la preuve et que l'atteinte est proportionnée au but recherché.

Vers une responsabilité du DRH en matière de conformité RGPD ?

Il ressort des précédents développements que même si la direction des ressources humaines a, dans le cadre de l'exercice de ses fonctions, pour mission d'encadrer et de protéger les données personnelles des salariés de son entreprise, son rôle dans l'application des principes énoncés par le RGPD n'est pas toujours clairement défini et délimité. Son rôle ne sera pas tout à fait le même si l'entreprise n'a pas désigné de DPO ni de référent RGPD, car il devrait assez naturellement être celui en charge du respect du RGPD dans le cadre du traitement des données personnelles des salariés, devenant dans ce cas le véritable acteur de la mise en conformité.

En tout état de cause, le DRH doit prendre conscience que le caractère particulier du traitement des données personnelles des salariés lui confère un rôle spécifique pour lequel une responsabilité propre peut lui être dévolue.

D'abord, du fait de sa position, le DRH peut mettre en place les règles relatives à la protection des données personnelles. Pour aider son entreprise à se conformer au RGPD et assurer aux salariés un traitement licite de leurs données personnelles, le DRH doit donc bien connaître et comprendre le contenu des règles relatives à la protection des données et jouer un rôle proactif en ce qui concerne les traitements des données personnelles des salariés.

En plus de cette responsabilité « *morale* » du fait de son rôle clé dans l'entreprise, le DRH pourrait aussi être responsable civilement et pénalement si l'employeur lui confie une mission plus importante et lui délègue ses pouvoirs à ce sujet. Lors de la répartition des pouvoirs au sein des délégations de pouvoirs, il est possible d'inclure dans le périmètre de la délégation concernant le DRH, une responsabilité en matière d'application du RGPD aux données à caractère personnel des salariés, à condition de fournir au DRH les moyens, les compétences, l'autorité et l'indépendance nécessaire.

Sabine DE PAILLERETS-MATIGNON
Avocate associée en droit social

Caroline GOUPIL
Avocate associée en IT / Data

Cabinet BCTG Avocats