Appliquer le RGPD dans le recrutement

Depuis le début des années 2000, l'essor du web et des nouvelles technologies a profondément transformé le métier de recruteur. Expansion des sites d'emploi et CVthèques, avènement des réseaux sociaux professionnels, des publicités ciblées, des entretiens en visioconférence ou vidéo, développement d'outils de sourcing digitalisés, recours à l'intelligence artificielle, … : les canaux de recrutement, comme les outils du recruteur, continuent d'évoluer chaque jour. Le résultat ? Un accès à un vivier de talents quasi infini et, en rebond, à des volumes de données candidats inconnus jusqu'alors. Or qui dit « données personnelles », dit également « risque élevé de porter atteinte à la vie privée ». Pour cette raison, il est primordial que les recruteurs respectent les droits et libertés des candidats en appliquant les recommandations du Règlement Général sur la Protection des Données, plus connu sous le nom de RGPD.

I - Qu'est-ce que le RGPD ?

Le RGPD est entré en vigueur le 25 mai 2018. Ce règlement crée un cadre légal sur le traitement des données personnelles au niveau européen. Il s'inscrit dans la continuité de la Loi Informatique et Libertés, appliquée en France depuis 1978. Le RGPD vise à renforcer le contrôle des citoyens européens sur l'utilisation de leurs données personnelles ; une question centrale aujourd'hui, à l'heure du tout numérique. Ainsi, tout organisme, public ou privé, établi sur le territoire de l'Union européenne ou traitant les données de résidents européens, est concerné par l'application du RGPD.

Le principal objectif du RGPD est de protéger la vie privée des citoyens européens en mettant à leur disposition les droits suivants, relatifs à leurs données personnelles : droit à l'information, droit d'accès, droit d'opposition, droit de rectification, droit à l'oubli, droit à la portabilité. Le RGPD vise également à responsabiliser les acteurs traitant les données personnelles et à renforcer la coopération avec les autorités de protection des données afin de prendre des décisions communes.

II - Les principaux points de conformité du RGPD dans le recrutement

Quelles sont les données qui peuvent être collectées lors d'un recrutement ?

Dans le cadre d'un recrutement, le recruteur est amené à collecter un certain nombre de données (coordonnées personnelles, lieux des expériences professionnelles, écoles

fréquentées, …). Les acteurs du recrutement doivent donc veiller à être en conformité avec le Règlement Général sur la Protection des Données.

Selon le guide à destination des recruteurs édité par la CNIL[1], le recruteur doit tout d'abord respecter le principe de minimisation des données. C'est-à-dire que les informations collectées doivent être adéquates, pertinentes et limitées à la sélection du candidat en vue d'un poste donné, et au bon déroulement de l'entretien d'embauche. Plus précisément, les données collectées ne doivent servir qu'à identifier le candidat le plus apte à occuper un poste, à mesurer ses compétences professionnelles et qualifications dans cette optique et à permettre la prise de contact. Dans le cadre d'un processus de recrutement, le recruteur pourra par exemple conserver les données relatives à l'expérience d'un candidat, ou encore des données telles que le numéro de téléphone et l'e-mail du candidat pour fixer un rendez-vous pour un entretien d'embauche.

L'autre principe à respecter est celui du respect de la vie privée du candidat. Enfreindre ce droit constitue une discrimination à l'embauche. D'ailleurs, l'article 226-1 du code pénal sanctionne l'atteinte à la vie privée d'autrui par une peine d'un an d'emprisonnement et 45 000 € d'amende. Durant la phase de sélection, le recruteur ne pourra par exemple pas demander certaines informations telles que le numéro de sécurité sociale, les coordonnées bancaires, des données concernant les membres de la famille du candidat ou sa situation familiale (marié ou non, avec ou sans enfants, orientation sexuelle, …). Cette liste n'est bien sûr pas exhaustive. Par ailleurs, les entreprises de travail temporaire ne doivent pas communiquer à leurs entreprises clientes les coordonnées bancaires des salarié.e.s et candidat.e.s à l'emploi telles que le relevé d'identité bancaire ou encore les bulletins de salaire mais aussi d'autres informations personnelles telles que l'origine, le lieu de naissance, le lieu de résidence d'un.e candidat.e.

Les obligations de l'employeur pour protéger les données des candidats

L'employeur est dans l'obligation de mener certaines actions pour protéger les données personnelles des candidats.

- **Informer les candidats**

Tout d'abord, le responsable du traitement des données doit informer les candidats de la collecte de leurs données personnelles, des modalités de traitement et de la manière d'exercer leurs droits selon les articles 12, 13 et 14 du RGPD. C'est le principe de loyauté et de transparence.

Il doit aussi informer sur l'identité et les coordonnées du responsable de traitement, la finalité du traitement, la base juridique du traitement, le caractère obligatoire ou facultatif de la communication des données, les destinataires des informations, la durée de

conservation des données, l'existence et les conditions d'exercice des droits applicables, ou encore la possibilité de faire une réclamation auprès de la CNIL.

Cette information doit être délivrée de manière concise, transparente, compréhensible et facilement accessible. Le candidat à l'emploi doit impérativement donner son consentement éclairé et univoque concernant l'entrée de ses informations dans la base de données du recruteur.

Si un candidat n'est pas retenu, le recruteur doit l'informer que ses données seront conservées pendant une durée maximum de deux ans. Si au contraire un candidat est retenu, ses données sont conservées pendant toute la durée de sa présence dans l'entreprise puis 5 ans après son départ de l'entreprise.

- **Limiter l'accès aux données**

Il incombe au.à la recruteur.euse de prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des informations personnelles collectées et empêcher que celles-ci soient déformées, endommagées ou que des tiers non autorisés y aient accès.

A titre d'exemple au sein des ressources humaines, seuls les agents en charge des processus de recrutement sont autorisés à accéder aux CV et lettres de motivation enregistrés dans le logiciel RH recrutement utilisé.

Le rôle de DPO (Data Protection Officer), personne déléguée à la protection des données, se développe massivement depuis la mise en œuvre du RGPD pour garantir l'intégrité et la protection des données collectées par l'entreprise.

- **Tenir un registre des activités de traitement**

Le recruteur doit mettre en place un registre des activités de traitement. Ce document a pour objectif de recenser la manière dont les données sont traitées. Le registre doit permettre d'identifier les acteurs qui interviennent dans le traitement des données, de visualiser les catégories de données traitées, de comprendre la visée des données collectées, leur destination et leur disponibilité (qui peut y accéder, sur quelle durée, comment sont-elles protégées, etc.).

Par ailleurs, depuis 2023, la CNIL propose un questionnaire[2] d'auto-évaluation aux recruteurs, qui permet à chaque recruteur d'évaluer sa méthode concernant la collecte, le partage, la réutilisation et la conservation des données personnelles des candidats.

- **Mener une Analyse d'Impact**

L'employeur doit mener une Analyse d'Impact relative à la Protection des Données (AIPD) lorsque le traitement des données personnelles collectées dans le cadre d'un recrutement présente un « risque élevé » pour les droits et libertés des candidats. Les recruteurs, qui collectent un large volume de données qu'ils sont amenés à croiser lors de recherches au sein de leurs bases de données, et peuvent avoir en leur possession des données dites sensibles, doivent utiliser l'outil qu'est l'AIPD pour sécuriser le traitement des données collectées. La CNIL propose un outil open source afin de réaliser son AIPD.

- **Contrôler et limiter l'utilisation des décisions automatisées,ou d'outils tels que la vidéo**

De nombreuses méthodes offrent aujourd'hui aux recruteurs la promesse de leur permettre d'évaluer les traits de personnalité et le « savoir-être » des candidat.e.s, d'identifier certains risques ou encore de prédire leurs performances futures. Tout comme les autres outils déployés dans le cadre de recrutement, ces méthodes doivent respecter la réglementation applicable tant au droit du travail qu'à la protection des données.

En particulier, elles ne peuvent être utilisées qu'à la condition de présenter un lien objectif, direct et nécessaire avec l'appréciation de la capacité à occuper l'emploi proposé ou les aptitudes professionnelles des candidats. Ces derniers bénéficient à cet égard d'un droit renforcé à la transparence, l'employeur ayant l'obligation de les informer expressément et préalablement à la mise en œuvre, des méthodes et techniques d'aide au recrutement utilisées conformément à l'article L.1221-9 du code du travail.

Par ailleurs, l'article 22 du RGPD interdit que la décision de recruter un candidat soit prise de manière entièrement automatisée (intelligence artificielle, test de personnalité). Il est possible que cela soit strictement nécessaire à l'exécution d'un contrat ou que le candidat ait donné son consentement, cependant même dans ce cas, il existe plusieurs obligations : les candidat.e.s doivent être informés de l'existence d'une décision automatisée lors de la collecte de leurs données. De plus, suite à la décision prise, le.la candidat.e peut demander à ce qu'elle soit réexaminée par un tiers ou la contester.

Par ailleurs, la CNIL alerte sur les algorithmes de traitement d'images vidéo qui analysent ensuite les micro-expressions (ou encore la morpho-psychologie) des candidats afin par exemple de les comparer à une liste de qualités déterminées par le recruteur (rigueur, agréabilité…). Aucune étude scientifique n'a pour l'instant assuré la fiabilité de ce type de résultats basées sur les micro-expressions. Dans le cadre d'un recrutement, la CNIL recommande d'écarter ce type d'analyse.

Les droits des candidats sur leurs données personnelles

Les candidats bénéficient d'un droit d'accès, de rectification, de suppression et de portabilité des données qui les concernent, ainsi que du droit d'opposition ou de limitation du traitement de leurs informations personnelles. Ces droits peuvent être exercés sur simple demande auprès de l'organisme collecteur, sur justification de l'identité du demandeur.

Pour que les candidats puissent exercer leurs droits, le recruteur doit prévoir un formulaire de contact spécifique, un numéro de téléphone ou une adresse e-mail dédiée et rendre l'information aisément accessible, par exemple par l'intermédiaire de son site web. Si l'entreprise effectue les recrutements via son site internet, le candidat devra pouvoir exercer ses droits à partir de son espace personnel.

Se conformer au RGPD est une obligation légale, qui conditionne également le respect de la vie privée de vos candidats dans le cadre du recrutement. Nous vous invitons à vous tenir régulièrement informés du cadre légal relatif à la collecte et à la protection des données à travers des formations et en vous référant au site de la CNIL. Par ailleurs, A Compétence Egale va publier un guide à destination des entreprises et des candidats à l'emploi concernant le RGPD, en octobre 2023, il sera accessible directement et gratuitement sur le site.

–

[1] "Guide Recrutement : les fondamentaux en matière de protection des données personnelles et questions-réponses", CNIL, 30 janvier 2023
[2] "Recruteurs : testez votre conformité au RGPD grâce à un questionnaire d'auto-évaluation", CNIL, 30 janvier 2023