Leto

CABINET DE RECRUTEMENT ET RGPD : QUELS ENJEUX ?

NOS CONSEILS

LETO. LEGAL

SOMMAIRE

LES POINTS CLÉS

L'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) a eu un impact important sur l'ensemble des entreprises européennes, quelle que soit leur taille ou leur domaine d'activité.

Les cabinets de recrutement ne font pas exception à la règle. Au contraire, ils sont particulièrement visés par le champ d'application de cette réglementation en raison du volume de données personnelles qu'ils collectent naturellement pour les besoins de leurs activités.
Si vous travaillez dans ce secteur d'activité et que vous vous interrogez sur la manière d'aborder efficacement le sujet de la conformité RGPD, ce guide est pour vous.

INTRODUCTION

Qu'est-ce que le RGPD ?

Entré en vigueur en mai 2018, le Règlement Général sur la Protection des Données (RGPD) est le texte européen qui pose le cadre réglementaire en matière de protection des données personnelles.
Si vous manipulez ce type de données en provenance de l'Union européenne (UE) ou depuis le sol européen, vous devez vous conformer à cette réglementation.

A quoi ca sert ?

Le Règlement Général sur la Protection des Données a deux objectifs principaux :

- Accorder des droits aux individus sur leurs données personnelles. Grâce au RGPD, ces personnes physiques pourront accéder à leurs données personnelles, décider de les rectifier ou de les effacer, et solliciter leur portabilité.
- Encourager les organismes à protéger les informations qu'ils détiennent sur les personnes pour prévenir tout abus dans la manipulation des données et garantir leur sécurité contre toute fuite, vol ou incident.

Pour cela, le RGPD impose un certain nombre d'obligations aux acteurs de l'économie.

Pourquoi le RGPD est une nouvelle opportunité ?

Contrairement aux idées reçues, le RGPD n'est pas seulement une nouvelle sous-couche réglementaire qui vient s'ajouter à la liste de vos obligations. Au contraire, le RGPD a dépassé le statut de simple contrainte administrative pour devenir porteur de nouvelles opportunités business :

- Les questionnaires “Privacy” au cours d’un appel d’offres ou d’un audit se sont largement généralisés. Les entreprises qui démontrent leur conformité au RGPD renforcent leur image auprès de leurs partenaires et clients potentiels. La capacité des entreprises à montrer "patte blanche" dans ce domaine est dorénavant un critère essentiel pour s'associer à une entreprise.
- Il constitue un argument marketing puissant : la protection des données personnelles est un sujet de préoccupation croissant pour les citoyens européens. Selon un sondage Eurobaromètre, 92 % des Européens considèrent la protection des données personnelles comme un droit fondamental. Les entreprises qui prennent au sérieux la confidentialité et la sécurité des données gagnent en confiance auprès de leurs clients et partenaires.
- Votre image de marque est sécurisée : se mettre en conformité au RGPD permet de vous prémunir contre une amende de la CNIL, des plaintes déposées par les personnes concernées, une procédure judiciaire engagée par un concurrent, et en définitive une mauvaise réputation.

Par où commencer ? Nous vous proposons un guide qui vous accompagne dans les étapes indispensables de la mise en conformité du RGPD pour votre activité, de manière pragmatique et pédagogique.

Leto

CARTOGRAPHIEZ VOS DONNÉES PERSONNELLES

Cette première étape est primordiale : faire l'inventaire des données personnelles que vous collectez sur les candidats, vos clients, vos employés etc.

Qu'est-ce qu'une donnée personnelle ?

Le RGPD ne s'applique qu'aux données à caractère personnel qui sont traitées par un organisme dans le cadre d'une activité professionnelle. La définition d'une donnée à caractère personnel est volontairement très large de sorte que presque toute donnée est incluse dans la définition.

En effet, les données à caractère personnel correspondent à toutes les informations se rapportant à une personne physique identifiée ou identifiable directement (par exemple, nom et prénom) ou indirectement (par exemple, numéro de sécurité sociale, adresse e-mail, enregistrement des conversations) (article 4 RGPD). Par conséquent, toutes les données qui permettent de remonter à une personne physique, même indirectement, sont des données à caractère personnel.

À l'inverse, sont exclues de cette définition toutes les données se rapportant à une personne morale : entreprise, organisme privé ou public, État etc.

Quelles données personnelles un cabinet de recrutement peut-il collecter ?

Tous les cabinets de recrutement sont naturellement amenés à collecter des catégories assez génériques de données personnelles.

Par exemple :

- Concernant le candidat : CV, lettre de motivation, lettres de recommandation, coordonnées bancaires, contrat de travail, numéro de sécurité sociale, diplômes, adresse e-mail, adresse postale, parcours professionnels et expériences personnelles, etc.

- Concernant vos clients : même dans une relation B2B, il y a de la donnée à caractère personnel dans la mesure où derrière une entreprise se cache toujours une personne physique. Dans ce cas, la donnée personnelle sera relative à l'e-mail professionnel et à l'identité de la personne physique représentant l'entreprise.

- Concernant vos propres employés : le RGPD s'applique à l'ensemble des données personnelles que vous pourriez collecter pour les besoins de votre activité professionnelle. À ce titre, les données que vous collectez sur vos employés bénéficient d'une protection égale à celle que vous collectez pour vos clients.

Ou sont rangées ces données personnelles ?

Les données personnelles se baladent absolument partout. Alors, pour faire le point, posez-vous les questions suivantes :

- Quels outils stockent et traitent des données personnelles ? Aujourd'hui, tout se trouve dans les CRM, des bases de données internes, les éditeurs de mailing, les boites mail, etc. Notez de façon exhaustive tous les outils digitaux (et non digitaux) que vous utilisez.

- Quels types de données trouve-t-on dans ces outils ? Il y a les données qui se voient comme "le nez au milieu de la figure". Ce sont celles qui identifient directement une personne : le nom, le prénom. Puis, nous avons les données plus “subtiles” et indirectes comme un numéro de téléphone, un numéro client, une date de naissance, etc.

Leto

LIMITEZ LES DONNÉES COLLECTÉES À CE QUI EST NÉCESSAIRE

Qu’est-ce qu’une donnée nécéssaire ?

Limiter la collecte des données à ce qui est nécessaire est également appelé "la minimisation des données personnelles". Il s'agit d'un principe fondamental du RGPD (article 5 RGPD).

Le principe de minimisation des données exige que l'organisme ne collecte que les informations indispensables à son activité. Autrement dit, plus vous limitez la collecte de données, plus vous vous rapprochez de la conformité.

En pratique, ce principe incite les entreprises à se demander si les données qu'elles collectent sont réellement nécessaires à leur activité. Si ce n'est pas le cas, ces données doivent être supprimées, anonymisées ou leur collecte doit être limitée à ce qui est essentiel.

Cette nécessité doit être appréciée en rapport avec la finalité de la collecte.

La finalité d'un traitement correspond à l'objectif ou encore la raison pour laquelle l'organisme collecte ou utilise une donnée personnelle. La finalité a pour objet de restreindre l'utilisation des informations à l'objectif prédéterminé. Si les données sont utilisées à des fins différentes de celles prévues, des sanctions peuvent être encourues.

Il convient d'être particulièrement vigilant en ce qui concerne la nécessité de collecter des données sensibles. En effet, il existe une catégorie particulière de données que vous n'avez pas le droit de collecter, sauf exception (article 9 RGPD).

Il s'agit des informations suivantes :

- Informations relatives à l'origine raciale ou ethnique,
- Informations relatives aux opinions politiques,
- Informations relatives aux convictions religieuses ou philosophiques,
- Informations relatives à l'appartenance syndicale,
- Informations relatives à la vie sexuelle ou à l'orientation sexuelle,
- Données génétiques,
- Données biométriques (permettant l'identification d'une personne unique),
- Données de santé,
- Informations relatives aux condamnations pénales bénéficiant d'une protection similaire prévue à l'article 10 RGPD.

Vous ne pouvez pas collecter ces informations sauf dans les cas suivants :

1. La personne concernée a librement donné son consentement,
2. Le traitement est nécessaire à l'exécution d'un contrat (par exemple avec votre client),
3. Les données sont rendues publiques par la personne concernée.

Quelques exemples

Lors d'un entretien avec un candidat, vous êtes limité dans les informations que vous pouvez collecter et donc dans les questions que vous pouvez poser. La finalité de cet entretien est de pouvoir examiner le profil d'un candidat et répondre aux besoins de votre client.

- Ainsi, demander à un candidat des éléments sur ses origines ethniques n'est pas nécessaire pour répondre à cet objectif.

- Pour donner un autre exemple, demander au candidat des informations sur son état de santé n'est possible que si le poste pour lequel il envisage de candidater exige une condition de santé particulière.

- Enfin, le numéro de sécurité sociale qui correspond à une donnée de santé (et donc une donnée sensible) n'est pas nécessaire pour l'activité d'un cabinet de recrutement. Seul l'organisme recruteur final est en droit de solliciter cette information.

METTEZ EN PLACE DES DURÉES DE CONSERVATION ET MESURES DE SÉCURITÉ

Comment fixer une durée de conservation ?

L'une des façons de protéger les données personnelles est de ne les conserver que le temps nécessaire et pas au-delà, pour deux raisons :

- Les données conservées longtemps ne sont plus à jour. Les entreprises ont l'obligation de conserver des données exactes sur les personnes concernées.
- Les personnes ont le droit à l'effacement automatique de leurs données.

Concrètement, pour un cabinet de recrutement, cela signifie qu'il ne peut pas conserver indéfiniment des données personnelles. Une durée de conservation doit être fixée avant leur collecte.

Pour savoir comment déterminer une durée de conservation, il convient de noter que l'entreprise peut soit renseigner un délai (6 mois, 3 ans, etc.) soit en référence à un événement (par exemple jusqu'à la fin du contrat de travail) ou en référence à une durée (3 ans à compter la collecte).

Pour aider les entreprises, la CNIL a rédigé plusieurs référentiels qui recommandent des durées de conservation en fonction du contexte.

En ce qui concerne le recrutement d'un candidat, la CNIL recommande de fixer une durée de conservation de 2 ans à compter du dernier contact avec le candidat.

Est-il possible de s'éloigner des recommandations de la CNIL ? En principe, les référentiels de la CNIL n'ont pas de force contraignante, il ne s'agit que de recommandations. Ainsi, pour s'en éloigner, il convient de pouvoir justifier précisément les raisons et de prévoir des garanties.

Leto

Les cabinets de recrutement peuvent conserver les données des candidats au-delà de cette période dans les conditions suivantes :

- Informer préalablement les personnes concernées de la durée de conservation, de la nature du traitement de leurs données personnelles et surtout de la manière dont elles peuvent exercer leurs droits, notamment solliciter la suppression de leurs données personnelles (CV, lettre de motivation, etc.).

- Ne pas fixer une durée de conservation abusive au regard de l'obligation de conserver des données personnelles à jour. En effet, en matière de recrutement, le profil des candidats est amené à évoluer dans le temps si bien qu'une durée de conservation doit être cohérente avec cet objectif.

- Enfin, il vous est toujours possible de solliciter le consentement des personnes concernées pour dépasser la durée de conservation de deux ans. Au surplus, ces personnes ont toujours la possibilité de revenir sur leur consentement et solliciter un effacement de leurs dossiers avant l'expiration de ce délai.

Comment assurer la sécurité des données personnelles ?

La protection des données personnelles conduit naturellement à prévoir des mesures de sécurité adéquates. En effet, les entreprises sont tenues d'assurer la confidentialité des données personnelles et de prévenir tout risque de violation de données personnelles (altération, divulgation, fuite, vol ou destruction de données personnelles intentionnelles ou accidentelles).

Ces mesures de sécurité peuvent être organisationnelles, techniques ou physiques, conformément à l'article 32 du RGPD. L'important est qu'elles soient suffisantes pour réduire tout risque de violation de données.

L'important est de garder à l'esprit que les mesures de sécurité doivent être adéquates pour prévenir les risques de violation de données (fuite, vol, incident qui viendrait altérer, détruire les données ou permettre un accès non autorisé).

Leto

Quelques exemples de mesures de sécurité

- Stocker les supports de sauvegarde dans un endroit sûr
- Réaliser une revue annuelle des habilitations
- Informer et sensibiliser les personnes manipulant les données personnelles
- Rédiger une charte informatique et un accord de confidentialité signés par vos employés.
- Installer un pare-feu (firewall) logiciel
- Utiliser des antivirus régulièrement mis à jour
- Effacer les données de tout matériel avant sa mise au rebut
- Adopter une politique de mot de passe utilisateur conforme aux recommandations de la CNIL.
- Faire des sauvegardes ou des synchronisations régulières des données

INFORMEZ LES CANDIDATS DE LEURS DROITS ET LES METTRE EN OEUVRE

Cette étape est la plus importante car elle est directement vérifiable par les autorités, vos clients et les personnes concernées. C'est aussi une élément fondamental du régime de protection des données : faire preuve de transparence et permettre aux personnes de reprendre le contrôle de leurs données personnelles.

De quoi s'agit-il ?

Votre entreprise a l'obligation de respecter des principes de transparence et de loyauté à l'égard des candidats qui vous confient leurs données. La première étape est de les informer, par écrit de préférence, lors de la collecte des données personnelles, sur le traitement qui va en être fait, la durée de conservation ainsi que l'ensemble des droits dont ils disposent parmi lesquels :

- droit d'accéder facilement à leurs données ;
- droit de s'opposer au traitement lorsqu'il existe une raison relevant d'une situation particulière ;
- droit à la portabilité des données (copie des données) ;
- droit à l'effacement des données ;

L’ensemble des droits “classiques” énumérés par le RGPD peuvent être exercés par le candidat, à vous de trouver une organisation optimale pour faire droit à la demande et d’autre part de connaître la réglementation pour savoir si des objections peuvent lui être opposées (intérêt légitime de l’entreprise, obligation légale, etc.).

En effet, votre organisme a le droit de refuser une telle demande lorsque les conditions le justifie. Par exemple, si votre employé demande une suppression de l’ensemble de ses données personnelles alors qu’il est en poste, vous avez naturellement le droit de décliner sa demande en vertu du contrat de travail qui le lie à votre structure.

À l’inverse, un candidat qui n’a pas été retenu pour le poste auquel il postulait a le droit de solliciter la suppression de l’ensemble des informations que vous détenez sur cette personne. Dans un tel cas, vous avez un délai d’un mois pour procéder à cette demande et confirmer répondre à la personne concernée.

Comment mettre en oeuvre ces obligations ?

1 - Rédiger une politique de confidentialité

Afin d'être entièrement transparent sur la manière dont vous traitez les données personnelles des candidats et leurs droits, vous pouvez rédiger une politique de confidentialité. Ce document est devenu un incontournable ! Plus largement, il permet d'informer vos utilisateurs, clients et partenaires de la manière dont vous traitez leurs données personnelles et comment vous assurez leur protection.

Il sera précisé notamment :

- les raisons pour lesquelles les données sont collectées ;
- le détail des traitements ;
- les modalités pour exercer les droits ;
- la liste des sous-traitants, etc.

Vous souhaitez vous informer sur la note ou vous en inspirez ? Politique de confidentialité.

2 - Implémentez votre processus d'exercice de droits de confidentialité

Pour vous, cela demande la mise en place de modalités pratiques (formulaire en ligne, coordonnées dédiées), d'un parcours interne efficace au sein de votre entité pour le traitement des demandes et d'un process de réponse auprès des personnes concernées qui soient compréhensibles, accessibles, formulées en des termes clairs et simples.

Rendez-vous sur notre simulateur : combien coûte un exercice de droit ?

Pour vous aider, chez Leto, notre solution met à disposition un portail dédié à vos utilisateurs sur lequel ils peuvent formuler leurs demandes d'exercice de droit. Elles arrivent ensuite directement sur la plateforme et vous permet d'identifier les données à supprimer et de générer un email de confirmation aux personnes.

CONSTRUISEZ VOTRE REGISTRE DE TRAITEMENTS

Le registre des activités de traitement est un document obligatoire recensant l'ensemble des traitements de données personnelles.

Un traitement est toute opération sur une donnée à caractère personnel : collecte, enregistrement, utilisation, transmission, destruction etc. Un traitement est tout ce qui peut possiblement être fait sur une donnée personnelle. Concrètement un traitement c'est une utilisation d'un fichier contenant un groupe de données personnelles.

Il convient de renseigner, dans ce registre et pour traitement, plusieurs éléments :

- Pourquoi collectez- vous ces données ? Chaque donnée que vous récoltez doit avoir une utilité précise, une raison (aussi appelé "finalité"). Cette finalité doit vous guider : si par mégarde vous n'utilisez pas les données en cohérence avec cet objectif, alors il serait temps de l'éliminer de votre base de données ;

- Combien de temps gardez-vous ces données ? Leur durée de conservation doit être cohérente et justifiée au regard de l'objectif de leur traitement. Ne vous inquiétez pas, la CNIL a créé un référentiel afin de vous aider à y voir plus clair :
- Qui y a accès ? Identifiez les destinataires auxquels les données seront communiquées, y compris les sous-traitants. Attention ! Elles doivent être accessibles aux seules personnes compétentes.
- Quelles sont les mesures de sécurité mises en place pour assurer la protection de ces données.
- Coordonnées des personnes associées aux traitements.

Votre registre de traitement doit permettre d'identifier les différents responsables en matière de protection de données personnelles. Il s'agit des personnes suivantes :

- Responsable de traitement : Le responsable de traitement est la personne qui détermine la finalité et les moyens du traitement de la donnée personnelle. Il s'agit de la personne morale (votre entreprise) incarnée par son représentant légal.
- Sous-traitants : Le sous-traitant est la personne ou l'organisme (souvent un prestataire de service) qui traite des données à caractère personnel pour le compte et sur les instructions du responsable de traitement. Par exemple votre éditeur de logiciel, votre comptable etc.
- Le délégué à la protection des données ou DPO si vous avez désigné une telle personne dans votre entreprise.

Exemple de traitement à propos de la mise à disposition des recruteurs des profils des candidats

- Catégorie de données collectées : nom, prénom, adresse e-mail, numéro de téléphone, CV, lettre de motivation et toute autre information pertinente.
- Finalité : mise à disposition des profils et proposer d'offres d'emploi.
- Accès : responsable de traitement (service concerné au sein du cabinet de recrutement) recruteurs, plateforme d'hébergement de ces données.
- Durée de conservation : 2 ans à compter du dernier contact avec le candidat. Après ce délai, les données seront supprimées ou anonymisées à des fins statistiques.
- Mesure de sécurité : toutes mesures techniques et organisationnelles adéquates.
- Base légale : dans ce cas précis, deux sont possibles :
- Consentement : Le candidat a donné son consentement pour le traitement de ses données personnelles à des fins spécifiques (par exemple, postuler à un emploi, recevoir des alertes d'emploi).
- Intérêt légitime : le cabinet de recrutement est légitime à traiter ces données pour proposer ses services aux recruteurs et placer les candidats aux postes appropriés.

5. CHOISISSEZ UN OUTIL RGPD POUR VOUS ÉPAULER

Manager l'ensemble de ces données de façon manuelle est très chronophage au regard de la quantité des données collectées.

Nous vous invitons à auditer plusieurs outils et d'en choisir un en fonction de son coût, de son expérience utilisateur et de son SAV.

Sinon, il y a Leto, qui permet à tout non-juriste de pouvoir administrer automatiquement l'ensemble des données !

FAITES CONFIANCE À LETO

Comment mettre en œuvre le RGPD dans une entreprise de manière efficace ? Comment transformer cette contrainte réglementaire en opportunité de développement de son activité ?

C’est en partant de ces enjeux rencontrés dans leurs expériences entrepreneuriales que Benjamin et Édouard ont créé Leto.

Leto est une solution Saas dont l’ambition est d’automatiser la mise en conformité au RGPD et d’en faire une réalité opérationnelle au quotidien dans l’entreprise.

POWDER

“L’équipe Leto nous a accompagné à chaque étape, nous permettant de gagner un temps précieux et de rassurer nos clients et partenaires quant à notre engagement en matière de protection des données personnelles de nos utilisateurs."
Kevin Cathaly, CTO de Powder

QOMON

“Nous sommes très satisfaits de la solution. Elle nous permet de répondre rapidement aux questions de nos prestataires sur le RGPD mais aussi les "privacy laws" en général qui voient le jour partout dans le monde. Les vrais plus avec Leto : la connexion automatique et le fait de pouvoir engager les équipes en interne autour de la protection des données personnelles de nos utilisateurs ”.
Florent Barre, CEO chez Qomon

Retrouvez tous nos témoignages Clients

LETO VOUS PERMET DE

Gagner du temps au quotidien

Leto réalise et maintient automatiquement l'inventaire des types de données personnelles traitées par l'organisation et toute la documentation de conformité.

Raccourcir votre cycle de vente

Leto aide vos équipes (commerciale, compliance, etc.) à répondre aux audits et questionnaires conformité de vos prospects

Réduire votre risque réputationnel

Leto aide vos équipes (commerciale, compliance, etc.) à répondre aux audits et questionnaires conformité de vos prospects

Améliorer la maturité des équipes

Leto sensibilise l'ensemble vos collaborateurs à la protection des données personnelles grâce une technologie unique de microlearning ultra-personnalisé.

LETO.LEGAL

ENVIE D'EN SAVOIR DAVANTAGE ?

N'HÉSITEZ PAS À NOUS CONTACTER.

NOTRE E-MAIL :
contact@leto.legal

NOTRE SITE WEB :
leto.legal

NOTRE NEWSLETTER :
leto.legal/newsletter-rgpd

NOTRE CHAINE YOUTUBE :
youtube.com/@letolegal

NOS LIVRES BLANCS :
leto.legal/livre-blanc/rgpd