LesJeudis

RGPD

Enjeux et obligations pour les DRH : les bonnes pratiques pour réussir sa mise en conformité

DROITS DES SALARIÉS | OBLIGATIONS DES DRH | CONFIDENTIALITÉ DES DONNÉES

LES ORIGINES DU RGPD

N'oubliez pas les enjeux

Validé en avril 2016, le Règlement Général sur la Protection des Données (RGPD) est exécutoire depuis le 25 mai 2018. Il renforce la protection de la vie privée de tous les citoyens européens.

Trop d'abus et plus de transparence ! Ces deux termes résument les enjeux du RGPD. L'évolution rapide des technologies de récupération et d'analyse de la data ainsi que la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel.

Ce **règlement de 99 articles** a été imaginé et rédigé de façon à **limiter les informations personnelles recueillies à l'insu des individus**, ou sans réelle justification, par toutes les entreprises (et en particulier les spécialistes de la donnée ou data broker) et les **GAFA**.

Depuis le 25 mai 2018, les mêmes obligations sont donc imposées aux entreprises établies hors de l'Union européenne, dès lors qu'elles proposent des produits ou services aux résidents européens.

S'il s'agit d'un règlement européen, il n'exclut pas que le droit des États membres précise les circonstances **des situations particulières de traitement** (Article 88 pour des ajustements de la protection des données dans la relation de travail). Chaque État peut en effet préciser les conditions dans lesquelles le traitement de données à caractère personnel est licite.

Mais les entreprises américaines sont-elles incitées à respecter cette obligation ?

Au printemps 2018, les États-Unis ont adopté le **Cloud Act**. Le « Clarifying Lawful Overseas Use of Data Act » permet aux autorités américaines d'accéder aux données étrangères. Toute société de droit américain (et donc les fournisseurs cloud) doit leur fournir les informations demandées dans un mandat.

Cela signifie aussi que cette demande ne peut se faire « seulement dans le cadre d'enquêtes judiciaires ». Le but est de simplifier et d'accélérer cette procédure en s'adressant directement aux éditeurs plutôt que de passer par le biais d'une demande d'entraide judiciaire internationale (mutual legal assistance treaties **MLAT**).

En clair, toute société de droit américain doit communiquer les données demandées, sans considération du lieu où elles sont localisées (et même si ce datacenter est en Europe…).

DONNÉES À CARACTÈRE PERSONNEL

Sachez identifier une personne

Il s'agit de « toute information se rapportant à une personne physique identifiée ou identifiable ». Une personne peut notamment être identifiée :

Directement :

- Nom
- Prénom
- Date de naissance

Indirectement :

- Numéro de téléphone
- Donnée biométrique
- Identité physique
- Identité physiologique
- Identité génétique
- Identité psychique
- Voix
- Image

4 %

L’article 83.6 du RGPD précise que la sanction peut atteindre « jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu ».

DROITS DES SALARIÉS, OBLIGATIONS DES DRH

Prenez vos précautions

La protection des données et les obligations des entreprises sont détaillées dans une centaine d'articles. Ce règlement européen renforce certains principes déjà existants et en ajoute de nouveaux.

Le DRH, manipulant énormément de la data, **doit revoir ses modes de gestion, de sécurisation et de conservation des données personnelles**. Le texte européen indique notamment que « les données à caractère personnel devraient être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées ».

Cette obligation s'applique aux données de tous les citoyens européens que traite une entreprise mais également à ses propres données RH.

SANCTIONS PÉNALES

5 ans

Outre des sanctions administratives (Article 83), les États membres peuvent également mettre en place des sanctions supplémentaires en cas de violation du RGPD, en particulier pour compléter ce texte. On les retrouve en France à la section « Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques » (articles 226-16 à 226-24) du Code pénal. Il y a une sanction pénale en cas de **détournement de la finalité des données personnelles** lors d'un traitement de données (Article 226-21 du Code pénal). Les sanctions pénales peuvent aller jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amende (Article 226-16 du Code pénal).

LES PRINCIPES DU RGPD

Devenez incollable

Consentement

Consentement explicite de la personne concernée à obtenir avant toute utilisation de données à caractère personnel

↑ PRINCIPE RENFORCÉ

Plus de transparence

Plus de transparence et de licéité dans le traitement des données

↑ PRINCIPE RENFORCÉ

Protection à la conception des données

Mise en place de mesures appropriées à la conception des données et dans leur traitement

↑ PRINCIPE RENFORCÉ

Accès et portabilité

Possibilité de **récupérer les données** communiquées et les **transmettre à une autre plateforme**

+ NOUVEAU PRINCIPE

Rectification et effacement

Possibilité de **demander l'effacement** de ses données personnelles

= PRINCIPE MAINTENU

Sous-traitants

Obligation de **garantir le respect des dispositions par l'ensemble de ses sous-traitants**

+ NOUVEAU PRINCIPE

LA MISE EN CONFORMITÉ D'UNE ENTREPRISE

Adoptez les bonnes méthodes

Contrats de travail, charte informatique, registre des traitements RH, gestion des archives papier… Le RGPD s'appliquant aussi bien aux fichiers numériques qu'aux documents papier (dès lors qu'ils font l'objet de fichiers), il est indispensable d'assurer la conformité de tous vos traitements de données personnelles relatives à vos salariés.

Cette démarche concerne notamment les informations relatives à la **gestion de carrière** au sein de votre organisation.

Toute personne concernée doit avoir le **droit de connaître les finalités du traitement des données à caractère personnel**, l'identité des destinataires, la durée, la logique qui sous-tend leur éventuel traitement automatisé et les conséquences que ce **traitement** pourrait avoir, au moins en cas de profilage.

BON À SAVOIR

L'employeur ne peut demander à ses salariés que les informations utiles pour accomplir ses missions. C'est le **principe de minimisation des données**. De son côté, l'employé peut exercer ses droits sur ses données personnelles en vous demandant d'y répondre dans le délai d'un mois.

Il y a bien sûr des **exceptions**. C'est le cas notamment lorsque « le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail » (Article 9-2-b).

Autre exception, lorsque le « traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux… » (Article 9-2-h).

Le registre du traitement

En listant tous vos traitements de données, vous disposerez d'une vision d'ensemble. Identifiez les activités principales de votre entreprise qui nécessitent la collecte et le traitement de données. Concernant les RH, il y a notamment le recrutement, l'évolution de carrière, la formation…

« NOUS SOMMES TOUS CONCERNÉS PAR LE RGPD »

« La protection des données personnelles était déjà l'une de nos préoccupations au sein du Groupe Néo-Soft puisque nous sommes certifiés ISO 27001. Avec l'entrée en vigueur du RGPD, nous avons dû revoir nos différents processus RH et recrutement. Nous nous sommes d'abord demandés si nous devions collecter telle ou telle information et quelles étaient les finalités. Cette étape a été très positive car elle nous a permis de faire un état de nos traitements et recueils. Nos salariés se sont intéressés à cette problématique en nous posant des questions sur les lieux de stockage et d'archivage par exemple. Des candidats nous ont aussi demandé de supprimer des informations les concernant.
Nous avons nommé en interne un DPO avec une équipe projet dédiée. Ils ont rapidement pris en main la sensibilisation et la formation des équipes, en priorisant la direction et les managers afin de susciter l'adhésion.
Ensuite, nous avons créé des modules de formation e-learning avec un tronc commun pour tous les salariés. Le pôle RH et nos consultants techniques ont bénéficié d'une session plus spécialisée.
Concernant nos sous-traitants, tous n'étaient pas au même stade que nous et ils ont dû se mettre en conformité. Nous avons été exigeants mais c'était déjà le cas dans le cadre de l'ISO 27001. Il est encore trop tôt pour savoir si notre conformité est un avantage concurrentiel mais les clients y sont très sensibles. Dans les appels d'offres, il y a déjà des critères sur le RGPD. Nous sommes capables de les accompagner, en particulier grâce à COGITAL et LYMEO, nos deux filiales spécialisées en sécurité et RGPD. »

NS
NEO|SOFT

Wafa Abda
Directrice des Ressources Humaines & Communication

LA CORESPONSABILITÉ ENTREPRISE / SOUS-TRAITANTS

Soyez vigilant

Le RGPD consacre une logique de responsabilisation de tous les acteurs impliqués dans le traitement des données personnelles. Les prestataires, qu'ils soient ou non européens, doivent être en conformité dès lors qu'ils traitent de données personnelles de citoyens européens.

Tous les métiers font appel, sans parfois s'en rendre compte, à des prestataires et des partenaires. Pour les RH, il s'agit principalement de **l'utilisation d'un logiciel en mode SaaS** (en ligne) et de **l'hébergement des données « sociales »** dans le cloud (qui peut être un datacenter en dehors de l'Europe)…

Vous êtes-vous posé ces questions ?

Tous mes prestataires et partenaires sont-ils fiables ?

Ont-ils eux aussi entamé leur mise en conformité avec ce règlement ?

Leurs contrats intègrent-ils des clauses spécifiques ?

Sont-ils capables de restaurer mes données très rapidement en cas de piratage ou de sinistre ?

Quel est le format des données restaurées ?

Certes, toutes ces problématiques ne concernent pas directement la conformité avec le RGPD. Mais elles peuvent avoir un impact sur la confidentialité et **l'intégrité de vos données** et donc sur la **pérennité de votre activité**.

Autant de questions que vous devez vous poser (en étant soutenu et accompagné par votre direction générale). D'ailleurs, le texte européen vous incite à prendre toutes les précautions nécessaires :

Vous ne devez faire appel qu'à « des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée », précise l'Article 28-1 du RGPD.

CONTRE LA MONTRE

72 heures chrono

En cas de fuite de données à caractère personnel engendrant un risque pour les droits et libertés, l'entreprise doit avertir - lorsque c'est possible - la CNIL 72 heures au plus tard après en avoir pris connaissance (Article 33).

LA CORESPONSABILITÉ ENTREPRISE / SOUS TRAITANTS

Prenez vos responsabilités (suite)

Au fur et à mesure qu'une entreprise s'attaque à sa mise en conformité, elle découvre souvent des prestataires auxquels elle n'avait pas pensé immédiatement. Et pourtant, ces sous-traitants accèdent (et traitent) peut-être de données personnelles.

Il est donc indispensable de les étudier précisément. **Avec l'aide de votre DPO, vous pouvez demander des précisions aux sous-traitants** quant au traitement des données personnelles que vous leur confiez.

Cette démarche n'est pas à prendre à la légère, car le chef d'entreprise reste « responsable des traitements et de la sécurité appliqués aux données personnelles y compris lorsqu'elles sont stockées sur des terminaux dont il n'a pas la maîtrise physique ou juridique », a rappelé la CNIL.

D'où la nécessité de revoir précisément ces documents, car ces contrats (ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre) lient « le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement », précise l'Article 28-3.

BON À SAVOIR

Le RGPD précise qu'un sous-traitant ne peut être recruté par un sous-traitant qu'après avoir obtenu l'autorisation écrite de son client. Ce « sous-traitant de rang 2 » devra respecter « les mêmes obligations en matière de protection de données que celles fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant conformément au paragraphe 3, sont imposées à cet autre sous-traitant par contrat ou au moyen d'un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre » (Article 28-4).

LA SÉCURITÉ ET LA CONFIDENTIALITÉ DES DONNÉES

Réduisez les risques

Indirectement, ce règlement impose un changement de culture au sein des entreprises. La sécurité informatique et la confidentialité ne doivent plus être négligées.

Le RGPD impose que les données soient traitées de façon à garantir une sécurité appropriée et à éviter leur divulgation au moyen de mesures techniques ou organisationnelles appropriées (règlt UE 2016/679 du 27 avril 2016, art. 5).

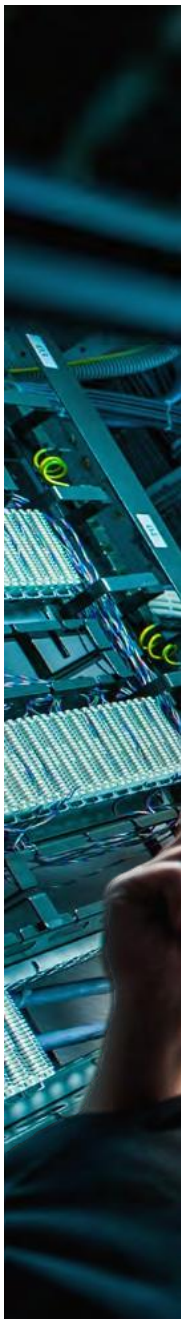
Une analyse de sécurité du système d'information est recommandée afin de repérer d'éventuelles failles de sécurité. Elles peuvent être dues à des vulnérabilités logicielles, des processus inappropriés ou de mauvaises habitudes (un mot de passe partagé entre le DRH et son assistant(e) par exemple). Cette analyse de sécurité sera aussi l'occasion de faire l'inventaire exhaustif des prestataires intervenant dans le traitement de vos données personnelles.

Chiffrement des données

Afin de garantir la sécurité, vous pouvez déployer du chiffrement (Article 34-3-a). Plus connue sous le terme de « cryptage », cette méthode consiste à **protéger vos fichiers en les rendant illisibles** par toute personne n'ayant pas la clé dite de déchiffrement. Sans le bon mot de passe, le contenu reste inaccessible.

BON À SAVOIR

La pseudonymisation des données à caractère personnel peut réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de protection des données. Mais l'introduction explicite de la pseudonymisation dans le RGPD ne signifie pas que les entreprises et leurs sous-traitants ne doivent pas déployer d'autres solutions de sécurité…



SÉCURITÉ

5 règles de base à appliquer*

1. Utilisez un mot de passe « fort » (ex. : 57JhpRD!) et différent pour chacun de vos comptes
2. Contrôlez et limitez les accès aux fichiers sensibles
3. Effectuez des mises à jour régulières de vos logiciels et postes de travail
4. Chiffrez les dossiers sensibles, surtout s'ils sont hébergés dans le cloud
5. Sauvegardez régulièrement vos données sur différents supports

** Ces règles ne dispensent aucunement d'établir une politique globale de sécurité à tous les niveaux.*

LE RÔLE DU DPO

Soyez bien accompagné

Le DPO est le garant de la conformité à la législation sur la protection des données personnelles au sein de l'entreprise. Il a une mission d'information, de conseil et de contrôle du respect de la législation relative à la protection des données personnelles.

Le Data Protection Officer (DPO) ou DPD (Délégué à la protection des données) peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

Autant rechercher un mouton à cinq pattes, car il doit :

- Disposer de compétences techniques ;
- Disposer de moyens suffisants ;
- Avoir la capacité d'agir en toute indépendance.

Certes, sa désignation est obligatoire (selon l'Article 37) que lorsque :

- Le traitement est effectué par une autorité ou un organisme public ;
- Les activités de base du responsable ou du sous-traitant consistent en des traitements qui exigent un suivi régulier et systématique ;
- Les activités de base du responsable ou du sous-traitant consistent en des traitements à grande échelle.

Mais dans la réalité, **de nombreuses entreprises font appel à un DPO externalisé**, car elles n'ont pas les compétences en interne, ni le temps, ni les moyens à y consacrer. Revers de la médaille, de nombreuses entreprises se sont engouffrées sur ce marché pour proposer ce type de prestations alors qu'elles n'ont pas les compétences ni la volonté d'assurer un accompagnement à long terme de leurs clients. Encore une fois, la mise en conformité du RGPD ne peut se faire en quelques semaines et avec des logiciels.

C'est une mission qui exige de la méthodologie, des compétences et une rigueur. Il est donc préférable de faire appel à des prestataires qui ont des DPO certifiés. Certes, cette certification n'est pas obligatoire pour exercer les fonctions de délégué à la protection des données. «Il s'agit d'un mécanisme volontaire permettant aux personnes physiques de justifier qu'elles répondent aux exigences de compétences et de savoir-faire du DPO prévues par le règlement. »,insiste la CNIL.
Mais elle a le mérite de démontrer les compétences du DPO.

BON À SAVOIR

La CNIL ne délivre pas elle-même de certification DPO (référentiel CNIL1827457X). Méfiance donc si vous recevez des emails prétendant que leurs DPO sont certifiés par la CNIL.

LES CONSEILS D'UN DPO

Suivez le guide

Questions à Laurence Filiol, DPO certifié Bureau Veritas*

Quelles données personnelles l'entreprise a-t-elle le droit de collecter et traiter dans le cadre d'un recrutement ? Quel en est le principe ?

Le principe est simple : la finalité du traitement des candidatures étant d'évaluer la capacité du candidat à occuper l'emploi à pourvoir, les données collectées et traitées devront avoir un lien direct et nécessaire avec l'emploi proposé. C'est un principe que l'on retrouve dans les règles de la CNIL et dans le Code du travail (loi El Khomri, art. L.1221-6 section 2) lorsqu'il s'agit de recrutement de collaborateurs. Le personnel chargé du recrutement ne pourra collecter que les données qui sont pertinentes par rapport à cette finalité. Ainsi, la collecte relative au numéro de sécurité sociale du candidat, sa domiciliation bancaire, son état de santé, les informations concernant son entourage familial (nom, prénom, nationalité, profession et employeur du conjoint), sa nationalité d'origine ne sont **pas pertinentes dans la mesure où ces données personnelles ne permettent pas d'apprécier la capacité du candidat à occuper un poste.**

Peut-on traiter toutes les données ?

La CNIL ne permet pas de traiter des données à caractère personnel qui, directement ou indirectement, feraient apparaître l'appartenance syndicale, les origines raciales ou ethniques, la religion du candidat, par exemple, et cela, combien même le candidat consentirait par écrit au traitement de ces informations dans la mesure où il n'existe pas de lien direct et nécessaire avec l'emploi à pourvoir. Aussi **de telles informations ne peuvent-elles être collectées que, dans certains cas, lorsqu'elles sont dûment justifiées par la spécificité du poste à pourvoir.**

Quelles sont les bonnes pratiques ?

Si on garde en tête ce principe, le bon usage des méthodes et techniques d'aide au recrutement ou d'évaluation du candidat, devient plus simple. Si, par exemple, dans une entreprise, il est d'usage que les entretiens d'embauche donnent lieu à des comptes-rendus contenant des « zones de commentaires », les informations collectées sur le candidat dans cet espace se limiteront à l'évaluation de ses compétences et de ses aptitudes professionnelles à occuper le poste proposé. **Les appréciations ne comporteront que des éléments pertinents et non excessifs par rapport à la finalité du traitement, excluant de ce fait, tout commentaire inapproprié, subjectif et insultant.** Cette bonne pratique est d'autant plus recommandée que le candidat a le droit d'accéder à son dossier à tout moment.

De même, dans le cas où l'évaluation du candidat fait appel à des tests de personnalité par exemple, ces derniers ont comme finalité unique d'apprécier la capacité du candidat à occuper l'emploi proposé. Là encore, les informations demandées doivent présenter un lien direct et nécessaire avec l'emploi proposé. La loi El Khomri réglemente l'usage de ces outils pour le recrutement (art. L.1221-6 section 2). Elle précise notamment que le test doit toujours être précédé du consentement du candidat et qu'une information préalable sur l'objectif et le type de test utilisé doit être délivrée à l'intéressé. **La loi stipule également que les résultats des tests doivent rester confidentiels.**

Quels sont les droits des candidats ?

La CNIL rappelle que le candidat a également le droit d'« obtenir sur demande et dans un délai raisonnable toutes les informations le concernant y compris les résultats d'analyses et des tests ou évaluations professionnelles éventuellement pratiqués ». Il peut aussi demander la suppression de son test, une fois réalisé. Si le candidat ne demande pas la destruction de son dossier, les données seront automatiquement détruites 2 ans après le dernier contact. **Seul l'accord formel du candidat permet une conservation plus longue.**

Enfin, en matière de collecte de données personnelles, l'entreprise est autorisée à recueillir les références du candidat auprès de son environnement professionnel (supérieurs hiérarchiques, collègues, maîtres de stages) dès lors qu'il en a été préalablement informé.

** Les propos n'engagent que Laurence Filiol.*

LES CONSEILS D'UN DPO

Suivez le guide (suite)

Quelles précautions l'entreprise doit-elle être prendre si elle propose un espace recrutement sur son site internet ?

Lorsque le site internet de l'entreprise prévoit un espace de recrutement permettant à l'internaute de répondre à une offre d'emploi et donc de déposer un CV et/ou une lettre de motivation, votre site doit prévoir un moyen de recueillir (et de tracer), préalablement à l'envoi des documents, l'accord du candidat au traitement de sa candidature. Cette demande de consentement doit clairement expliciter la finalité du traitement et le consentement doit se matérialiser par un acte positif (une case à cocher). Une mention d'information facilement accessible sera proposée au candidat.

Comment proposer une information qui respecte le règlement européen ?

Cette information, pour être conforme RGPD, contiendra au moins les éléments suivants :

- **l'identité et les coordonnées du responsable du traitement** et le cas échéant de son délégué à la protection des données ;
- **la finalité du traitement** (par exemple, « traitement des données personnelles du candidat en vue d'évaluer sa capacité à occuper l'emploi à pourvoir ») ;
- **la base juridique du traitement** (le cas échéant, le consentement) ;
- **les destinataires des données** (sont uniquement concernées les personnes intervenant dans le processus de sélection) ;
- l'existence ou l'intention de réaliser un **transfert de données personnelles hors UE** si elle existe ; **les droits des personnes** (droit de retrait du consentement, d'accès, rectification, effacement, limitation, opposition, portabilité et droit d'introduire une réclamation auprès de la CNIL) et **les modalités d'exercice de ces droits** ;
- **la durée de conservation des données personnelles**. Cette durée doit être proportionnelle à la finalité du traitement qui, en l'occurrence, est le temps de la sélection des candidats au poste proposé (voir l'encadré « Bon à savoir ») ;
- **des informations sur le caractère réglementaire ou contractuel de la fourniture de données à caractère personnel** ainsi que sur les conséquences éventuelles de la non-fourniture de ces données;
- **l'existence éventuelle de dispositifs automatiques de décision** (y compris le profilage) et dans ce cas, des informations utiles sur la logique sous-jacente, l'importance et les conséquences prévues pour le candidat. Cela concerne certaines entreprises qui se servent d'algorithmes dans leur processus de recrutement.

En principe, **il est interdit de prendre une décision au sujet d'une personne, si elle est entièrement informatisée** et si elle produit des effets juridiques à son égard ou a un impact significatif sur elle. Cependant, le traitement visant à faciliter le recrutement, notamment grâce à un algorithme de sélection fait partie des traitements soumis[1] à une étude d'impact (AIPD[2]) préalablement à leur mise en oeuvre.

À cet ensemble d'éléments, l'entreprise pourra également inclure des informations relatives aux mesures techniques et organisationnelles prises par l'entreprise pour assurer la sécurité des données du candidat.

Attention, dans le cas où des données personnelles ne sont pas collectées directement auprès du candidat (par exemple, dans le cas où l'entreprise utilise des outils de sourcing en recrutement), **la mention d'information doit également identifier la source des données** et, le cas échéant, si les données sont issues de sources accessibles au public.

Par ailleurs, si votre entreprise externalise la fonction de recrutement des collaborateurs, sachez que **votre prestataire et votre entité sont conjointement responsables du traitement des données personnelles du candidat**. Dans ce cas, vous devez vous assurer de la conformité RGPD de votre prestataire et fixer les obligations de chacune des parties en matière de protection des données personnelles au moyen d'un acte juridique.

1. Délibération 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

2. AIPD : Analyse d'Impact relative à la Protection des Données

BON À SAVOIR

À l'issue de la sélection et dans le cas où le candidat n'est pas retenu, deux solutions peuvent être envisagées :

- l'entreprise prévient le candidat que sa candidature n'a pas été retenue et supprime immédiatement son dossier ;
- l'entreprise, dans l'email lui signifiant qu'il n'a pas été retenu, lui demande son consentement pour conserver son dossier plus longtemps considérant que le profil de la personne répond aux exigences d'un autre poste à pourvoir. Quoi qu'il en soit, les données du candidat ne pourront être conservées au-delà de 2 ans à compter de son dernier contact.

CONCLUSION

Positivez

La mise en conformité avec le RGPD est un processus à long terme. Il implique une démarche globale et méthodique.
Tous les métiers sont concernés. Mais la direction générale l'est encore plus, car c'est elle qui doit instaurer une nouvelle gouvernance de la donnée. Ce texte appelle à un profond changement de culture au sein des organisations.

Loin d'être un règlement de plus, le RGPD doit être considéré comme le fondement de la confiance entre acteurs économiques et citoyens. Il représente également un vecteur d'accélération de la maturité numérique des entreprises.

Le principe de « responsabilité » (« d'accountability ») oblige les entreprises à mettre en œuvre des mécanismes et des procédures internes (notion d'audit) permettant la protection des données à caractère personnel. L'employeur doit donc assurer **la traçabilité des données** et se constituer des preuves démontrant qu'il respecte ses dispositions.

De manière plus globale, les entreprises doivent renforcer la protection de leurs données confidentielles et personnelles.

ET MAINTENANT ?

Nos 5 conseils

1 Ne vous précipitez pas : la mise en conformité est un long processus
2 Faites une cartographie précise de vos traitements de données à caractère personnel
3 Soyez soutenu et accompagné par votre direction générale
4 Sensibilisez vos collaborateurs aux enjeux du RGPD et à la sécurité des données
5 Faites-vous accompagner par un DPO et des experts en sécurité informatique

À PROPOS DE LESJEUDIS

Groupe LesJeudis accompagne le recrutement de ses clients depuis 25 ans avec des solutions sur mesure à chaque étape : accès à des candidats, publication d'offres, gestion des candidatures et promotion de la marque employeur.

En plaçant l'innovation et le service client au cœur de sa stratégie, il propose des services RH optimisés pour répondre aux besoins de plus de 1000 entreprises, de l'ESN aux Grands Groupes. Si vous cherchez un partenaire pour le sourcing, l'analyse des candidatures et la stratégie de marque employeur, LesJeudis est l'interlocuteur idéal.

Découvrir nos solutions