DONNÉES PERSONNELLES (RGPD)

L'impact pour les RH

Livre blanc élaboré en coopération avec CAPTIVEA FCP

Sommaire

Introduction

Le Règlement général sur la protection des données 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) est destiné à harmoniser et normaliser les différentes lois sur la protection des données personnelles existantes dans les pays de l'Union européenne.

Le 25 mai 2018, le RGPD entrera en vigueur dans le droit français. S'agissant d'un règlement et non d'une directive, il sera d'application immédiate et ne nécessitera aucune loi de transposition.

Ainsi, chaque pays de l'Union européenne appliquera le même texte. Il convient toutefois de rappeler que la législation nationale des États membres pourra venir compléter certaines dispositions du RGPD.

Ce règlement poursuit essentiellement trois objectifs :

– renforcer les droits des personnes ;

– responsabiliser les professionnels ;

– augmenter la coopération entre les autorités protectrices de données personnelles sur le territoire de l'Union européenne (en France, la CNIL).

1 LE CONTEXTE DU RGPD

L'évolution des technologies a profondément modifié le contexte de collecte et de partage des données personnelles.

En outre, les divergences d'application dans les États membres posent de sérieux obstacles aux entreprises exerçant leurs activités au niveau européen.

C'est la raison pour laquelle les États membres ont fait le choix d'un règlement communautaire.

Dès son entrée en vigueur, toutes les obligations déclaratives à l'égard de la CNIL disparaîtront.

Désormais, les responsables de traitement de données personnelles devront, dès la conception du traitement puis à tout moment de son existence, mettre en œuvre les mesures techniques et organisationnelles nécessaires pour s'assurer de la conformité des traitements qu'ils initient et pouvoir le démontrer en cas de contrôle par l'autorité administrative compétente.

En particulier, la sécurité des données devra être assurée en continu et prendre en compte les évolutions technologiques.

Et pour vous, RH ?

Cette nouvelle façon d'appréhender la gestion des données personnelles devra être mise en œuvre par les employeurs en ce qui concerne, entre autres, les données de leurs salariés, dans le respect des principes véhiculés par le RGPD.

En effet, en ressources humaines un grand nombre de données personnelles sont collectées, traitées, stockées et analysées de façon récurrente.

Ce nouveau règlement doit vous amener à vous interroger sur l'utilisation que vous faites de ces données.

Cependant, si vous devez être conforme au RGPD, l'ensemble de vos salariés seront impliqués et auront aussi des droits et des obligations.

2 COMMENT SE METTRE EN CONFORMITÉ

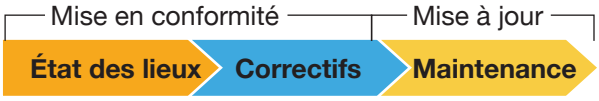
Vous devez dès à présent vous mettre en conformité.

Nous allons détailler ici quelles sont les étapes pour y parvenir au sein de votre service des ressources humaines.

Les grandes étapes

Il est important de comprendre que cette mise en conformité s'inscrit dans le temps. Une fois que vous l'aurez réalisé, il faudra continuer ces bonnes pratiques dans le temps.

Voici donc les grandes étapes :



État des lieux

• Préparation

Au sein de l'entreprise, plusieurs interlocuteurs ont ou vont être désignés, puis formés, pour permettre cette mise en conformité :

– un responsable de traitement : il s'agira, dans la majorité des cas, de la personne morale incarnée par son représentant légal. Il pourra être accompagné de responsable(s) adjoint(s) ;

– un délégué à la protection des données : véritable garant de la conformité, la désignation d'un DPO est obligatoire dans certaines entreprises.

• Audit

Il faut identifier et cartographier l'ensemble des traitements et les analyser selon les axes suivants :

1/ Identifier les données à caractère personnel

Une donnée à caractère personnel est une information qui permet d'identifier une personne de manière directe (nom, prénom, image, etc.) ou indirecte (le numéro de Sécurité sociale, un identifiant de connexion informatique, etc.).

2/ Définir la licéité des traitements

Les différentes formes de licéité des traitements, c'est-à-dire de leur base légale, vous sont expliquées dans la partie 4 de ce livre blanc.

3/ Définir la durée de conservation de ces données

Vous ne pouvez pas conserver ces données de manière illimitée ni même « au cas où », mais vous devez décider de cette durée et faire le nécessaire au-delà.

4/ Définir le responsable de traitement

Le responsable de traitement de l'entreprise doit être clairement identifié.

5/ Analyser la relation avec les sous-traitants

Le sous-traitant effectue des traitements pour le compte du responsable de traitement et doit à ce titre être lui aussi en conformité avec le RGPD.

Votre SIRH ou votre logiciel de paie peuvent être des sous-traitants.

6/ Auditer la sécurité

Il s'agit d'examiner dans votre service les niveaux de sécurité accordés aux données personnelles pour voir si des améliorations sont nécessaires et, si oui, lesquelles ?

7/ Vérifier la possibilité pour les personnes d'exercer leurs différents droits

Plan d'action – Correctifs

Une fois l'audit réalisé, élaborez un plan d'action qui va vous permettre non seulement de définir comment corriger les non-conformités actuelles, mais aussi de mettre en place des actions pour rester conforme dans le temps. Le plan d'action servira également à définir le budget associé à ces actions et le planning de correction.

Notez-le

Vous devez documenter l'ensemble des éléments qui prouve votre mise en conformité, notamment en tenant à jour le registre des traitements (reportez-vous à la partie 3 de ce livre blanc).

Maintenance

Une fois que tous vos processus sont en conformité avec les nouvelles exigences du RGPD, vous devez continuer en ce sens, c'est-à-dire actualiser le registre de traitement et ne collecter que les données nécessaires.

Rappelez-vous que toutes les déclarations préalables à la CNIL disparaissent mais que vous devrez pouvoir prouver à tout moment que vous êtes en conformité.

3 LE REGISTRE DES TRAITEMENTS

Le registre des traitements est un document que toute entreprise doit mettre en place pour effectuer sa mise en conformité.

Les traitements concernés dans le cadre des RH sont notamment :

– la paie ;
– le recrutement (de la candidature à l'embauche) ;
– la tenue du registre du personnel ;
– les congés et les absences ;
– les notes de frais ;
– la BDES ;
– les entretiens individuels ;
– les activités syndicales.

Pour chaque traitement, il faut identifier et consigner les informations suivantes :

– **le nom du traitement** tel que paie, recrutement, etc. ;
– **sa date de création** ;
– **les finalités et les sous-finalités par exemple** :
  • établir la paie,
  • pouvoir recontacter un candidat,
  • remboursement des notes de frais ;
– **la description du traitement ;**
– **les interlocuteurs** :
  • responsable de traitement,
  • représentant du responsable de traitement,
  • délégué à la protection des données,
  • sous-traitant.
– **les mesures de sécurité techniques** telles que les données cryptées ou l'accès par mot de passe ;
– **les mesures de sécurité organisationnelles**, par exemple bureaux fermés à clé ou les placards sécurisés ;
– **les données à caractère personnel courantes**. En ressources humaines différentes données peuvent être collectées :
  • état civil, identité, données d'identification,
  • état de santé (handicap, maladie, etc.),
  • revenus, situation financière, situation fiscale,
  • données bancaires,
  • image,
  • adresse IP,
  • parcours professionnel, etc.

– **la licéité du traitement** : reportez-vous à la partie 4 de ce livre blanc ;

– **la nécessité d'une étude d'impact**. Une étude d'impact peut-être nécessaire si le traitement présente un risque élevé pour les droits et les libertés des personnes concernées :
  • évaluation ou profilage,
  • surveillance systématique,
  • données sensibles (origine raciale ou ethnique, opinions politiques, données génétiques, données biométriques, convictions religieuses, etc.),
  • traitement à grande échelle ;

  Cette étude d'impact peut être menée, par exemple, grâce à l'outil mis à disposition par la CNIL.

– **les destinataires des traitements** (salariés, sous-traitant, IRP, etc.).

Pour chaque traitement, il faut identifier le niveau de sécurité requis en fonction de la criticité des données et du volume.

Nous pouvons identifier 3 niveaux de sécurité :

– **niveau minimum :** appliquer les pratiques de sécurité basiques.
  Exemple : accès par le biais d'une authentification ;

– **niveau moyen :** appliquer les pratiques de sécurité basiques avec quelques axes de sécurité supplémentaires.
  Exemples : accès sécurisé HTTPS, complexité du mot de passe. Accès avec des profils en fonction de chaque personne ;

– **niveau élevé :** il s'agit du niveau moyen avec des solutions techniques supplémentaires.
  Exemples : accès par le biais d'un VPN, cryptage des données.

4 LES DROITS DES PERSONNES CONCERNÉES

Le règlement s'attache à protéger les droits des personnes en réaffirmant certains principes et en renforçant les droits des personnes dont les données sont collectées.

Vous concernant, les principales personnes concernées seront les salariés de votre entreprise.

Mais attention, vous pouvez collecter des données personnelles concernant d'autres personnes que vos salariés : un consultant extérieur, comme un avocat ou un conseiller, un candidat pour un emploi, un prestataire externe, etc.

Licéité du traitement

Pour être licite, un traitement doit reposer sur une des bases légales proposées par le règlement. En outre, le responsable de traitement devra toujours être en mesure d'indiquer à la personne qui en ferait la demande le fondement légal du traitement, indiqué dans le registre, dont ses données personnelles font l'objet.

Plusieurs bases légales sont notamment susceptibles de fonder un traitement en matière de ressources humaines :

L'exécution d'un contrat : le traitement est nécessaire dans le cadre de l'exécution d'un contrat ou dans l'intention d'en conclure un.
Exemple : le traitement des données des salariés pour procéder à leur paie.

L'obligation légale : le traitement est effectué conformément à une obligation légale à laquelle le responsable de traitement est soumis.
Exemple : le traitement des données relatives aux salariés pour pouvoir les communiquer à la Sécurité sociale et/ou à l'administration fiscale.

Le consentement : c'est un élément phare du règlement. Le consentement doit porter sur une ou plusieurs finalités spécifiques, ce qui exclut un consentement exprimé de manière générale. Il doit impérativement être donné de manière indépendante à d'autres questions.

Il peut s'agir par exemple du consentement des salariés pour l'utilisation de leurs photographies pour le site Internet de la société.

Le consentement doit pouvoir être retiré aussi facilement qu'il a été donné.

Consentement valide

Pour être valide le consentement doit provenir d'une déclaration expresse ou d'un comportement démontrant le consentement sans ambiguïté.
Exemple : – votre salarié peut vous adresser un courrier ou un mail ;
– si vous transmettez la demande par le biais de l'intranet de l'entreprise, le consentement peut être donné en cochant une case.

A contrario, le silence du salarié ou la case précochée ne vaut pas consentement.

Dès les entretiens d'embauche, en passant par la vie du salarié dans l'entreprise jusqu'à son départ, il faut définir les processus de gestion des droits à la personne pour être prêt en cas de demande particulière d'un de vos salariés ou d'une personne qui a candidaté.

Désormais, toute personne engagée dans la collecte de données devra être en mesure d'indiquer clairement sa finalité, telle que décrite dans le registre de traitement.

Le renforcement des droits des salariés

Le RGPD introduit de nouveaux droits et élargit ceux déjà existants :

– **droit à l'information :** le responsable de traitement est tenu de fournir notamment l'identité et les coordonnées du responsable du traitement et, le cas échéant, les coordonnées du délégué à la protection des données, de même que les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;

– **droit d'accès :** droit pour la personne dont les données sont collectées de savoir si elles font l'objet d'un traitement et, dans l'affirmative, les finalités du traitement, les destinataires, la durée de conservation des données, ainsi que, notamment, l'existence du droit de rectification ou d'effacement ;

– **droit à rectification :** droit d'obtenir dans les meilleurs délais la rectification de données inexactes ou incomplètes ;

– **droit à l'oubli :** droit pour une personne de demander l'effacement de ses données personnelles auprès du responsable de traitement, sous certaines conditions ;

– **droit à la limitation du traitement :** dans certains cas, la personne concernée peut exiger que le responsable de traitement puisse conserver ses données sans pouvoir s'en servir ;

– **droit à portabilité :** droit pour une personne d'obtenir voire de réutiliser ses données personnelles :
  • droit de récupérer les données personnelles la concernant pour les conserver,
  • droit de les transférer à un autre organisme.

  Toutefois, il faut que trois conditions soient réunies :
  • les données personnelles doivent avoir été fournies par la personne elle-même...,
  • … sur la base du consentement ou de l'exécution d'un contrat. Ainsi, les données personnelles traitées par l'employeur sur une autre base ne bénéficieront pas de la portabilité,
  • la portabilité ne doit pas porter atteinte aux droits et libertés de tiers.

Ces droits devront impérativement être pris en compte par les responsables de traitement. Ces derniers doivent répondre à la personne concernée dans les meilleurs délais et au plus tard dans le délai d'un mois à compter de la réception de la demande.

Notez-le

Le salarié peut exercer ces droits sous réserve que l'exécution du contrat ne soit pas remise en question. Le responsable de traitement est en droit de s'opposer à certaines demandes jugées abusives ou trop répétées..

Votre salarié a lui aussi des devoirs. Toute personne qui serait amenée à gérer des données personnelles en dehors du cadre défini engage sa propre responsabilité. Une sensibilisation dans l'entreprise peut s'avérer utile. Votre salarié a également des obligations vis-à-vis des données personnelles des clients, fournisseurs et employés de l'entreprise.

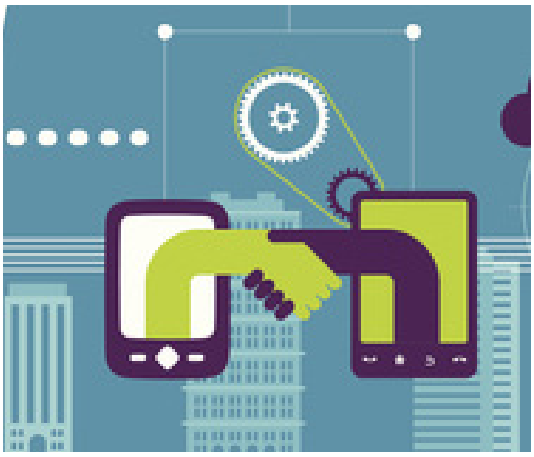
Il convient de rappeler que les sanctions pouvant être prononcées par la CNIL peuvent être très lourdes : de 10 à 20 M€, ou, dans le cas d'une entreprise, de 2 à 4 % de son chiffre d'affaires annuel mondial.

Conclusion

Le RGPD est un sujet majeur de l'année 2018 sur lequel il est important d'être en règle. L'objectif défendu par la RGPD est noble même si sa mise en place peut paraître fastidieuse.

La mise en conformité facilitera votre travail au quotidien en limitant la collecte aux données qui vous sont réellement utiles. Cela vous permet de minimiser le risque de perte de données ou de modification grâce à un accès limité.

Le RGPD est aussi un atout pour l'image que les salariés peuvent avoir du service RH. Il est un gage de sécurité et renforce la confiance que chacun ressent quant à la sécurité de ses données.



À propos des auteurs

Sébastien RISS

Sébastien RISS est dirigeant de la société Captivea. De formation ingénieur, il s'est passionné dès le début pour le RGPD et a donné plusieurs conférences en France sur le sujet. Captivea a tout naturellement ajouté des prestations d'accompagnement à la mise en conformité.

Captivea a été fondée il y a 10 ans avec l'objectif de positionner l'informatique au service de l'entreprise.

C'est une équipe de 25 personnes qui intervient sur 2 domaines d'activité :

– le premier domaine concerne l'intégration de logiciels de gestion d'entreprise. Solutions CRM (Force force de vente, marketing automation, service client), marketing automation, ERP (gestion globale de l'entreprise au sens large du terme), et de solutions sur mesure ;

– le second domaine d'activité concerne les services IT, autour de l'hébergement cloud, du travail collaboratif et de la **conformité RGPD**.

Par ses compétences dans ces deux domaines, Captivea permet à ses clients d'améliorer leur organisation et leur rentabilité.

Captivea a accompagné plus de 200 entreprises de type PME et des grands comptes, comme La Banque Postale, les Éditions Tissot ou Mobalpa.

https://www.captivea.com

https://www.conformite-rgpd.com

Florence COTTIN-PERREAU

Florence COTTIN-PERREAU a fondé le cabinet FCP AVOCAT il y a un peu plus de vingt ans.

Spécialisée en propriété intellectuelle (brevets, marques, dessins et modèles et droit d'auteur), elle accompagne les PME/PMI dans la protection et la gestion de leur patrimoine intellectuel, par le prisme des autres domaines du droit : droit commercial, droit du travail, etc., grâce à une solide expérience en droit de l'entreprise.

Elle est l'auteur de nombreux articles sur le RGPD et a participé à plusieurs colloques destinés à préparer la mise en conformité des entreprises.

https://www.fcp-avocats.com