LA LETTRE
NEWS DE LA FORMATION PROFESSIONNELLE

MAI 2019

TRANSFORMATION DIGITALE DES RH

Tuto n°2

Service RH : quelles mesures prendre pour devenir conforme au RGPD ?

Le Réglement Général pour la Protection des Données a fête ses 1 an le 25 mai dernier. De nombreuses entreprises n'ont pas encore pris toutes les mesures nécessaires pour se mettre en conformité. Le service RH étant très impacté par le RGPD, nous vous résumons dans ce tutoriel les mesures à prendre pour vous mettre en conformité.

Difficile de faire un bilan 1 an après l'entrée en vigueur du RGPD. Aujourd'hui, nous savons toutefois que des sanctions ont été prononcées dans douze pays européens. Les montants des amendes vont de 9700 euros (Autriche) à 400 000 euros (Portugal). Rappelons que l'amende de non-conformité peut s'élever jusqu'à 4% du chiffre d'affaire de l'entreprise.

L'European Data Protection Board (EDPB) qui chapeaute les autorités européennes a révélé que ces dernières avaient étudié 280 000 dossiers depuis l'arrivée du RGPD, dont 144 376 issus de plaintes. A l'occasion de l'anniversaire du RGPD, la CNIL (Commission Nationale de l'Informatique et des Libertés) s'est récemment exprimée sur le sujet : *"l'année 2019 marque l'achèvement de la transition vers le RGPD. Il est essentiel que, désormais, les organismes appliquent complètement le nouveau texte".* Les entreprises sont prévenues, la CNIL va progressivement faire preuve de moins de souplesse.

Les services RH sont fortement impactés par le RGPD, car ils collectent, traitent et archivent un volume conséquent de données personnelles. Le chantier pour se mettre en conformité est certes conséquent, mais il peut apporter de nombreux bénéfices à l'entreprise : bases de données propres, confiance des salariés et des candidats... Quelles mesures prendre pour y arriver ? Suivez le guide.

I. NOMMER UN DPO

Le Data Protection Officer ou Délégué à la Protection des Données (DPP) est le chef d'orchestre de la conformité au RGPD au sein de l'entreprise.

Il a notamment pour missions :
- Informer et conseiller le responsable du traitement, les sous-traitants et les employés
- Contrôler le respect du règlement et du droit national en matière de protection des données
- Conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données
- Coopérer avec l'autorité de contrôle (qui correspond à la CNIL en France)

Le DPO peut être nommé en interne. Dans ce cas, il doit être le plus indépendant possible afin de pouvoir remplir l'intégralité de ses missions sans barrières. Vous pouvez également faire appel à un cabinet d'audit ou d'avocats pour remplir ses fonctions.

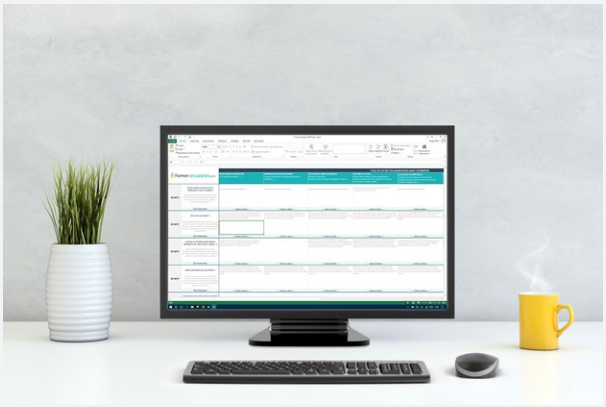
II. CRÉER ET ENTRETENIR UN REGISTRE DES TRAITEMENTS DES DONNÉES RH

Un registre de traitement des données, quésaco ? C'est un document, au format word par exemple, dans lequel vous allez répertorier toutes vos activités liées à de la manipulation de données.

Pour chacune de ces activités (ici, la candidature), vous allez devoir détailler :
- Les objectifs poursuivis par le traitement de données
ex : coordonnées afin de contacter le candidat, expériences professionnelles et parcours scolaire afin de savoir si le candidat correspond bien au poste
- Les catégories de personnes concernées
ex : les candidats
- Les catégories de données collectées
ex : identité, vie personnelle, vie professionnelle
- Si des données sensibles sont traitées ou pas
ex : non, pas de recueil de données liées à l'origine ethnique, la conviction religieuse...
- La durée de conservation des données
ex : 2 ans maximum de conservation du CV d'un candidat
- Les catégories de destinataires des données
e.g. Recruteurs, logiciel de recrutement
- Si des données sont transmises hors de l'UE, et si oui, vers quel pays
ex : non
- Les mesures de sécurité prévues pour préserver la confidentialité des données
e.g. contrôles d'accès, antivirus, chiffrement des données, vérification de la conformité RGPD de mon logiciel de recrutement

La CNIL met à disposition des entreprises un modèle de registre de traitements des données. Nous vous conseillons de le remplir en étant accompagné par votre DPO, pour être sûr de bien faire.

Outil RH RGPD



Nous avons imaginé un tableur excel regroupant **toutes les activités du service RH** (recrutement, administration du personnel, gestion de la paie...). Ce tableau vous aidera à avoir une **vue d'ensemble de vos différents traitements de données**. Après avoir rempli ce tableau, il vous sera alors plus facile de rédiger la partie RH du registre de traitement des données.

Télécharger l'outil RGPD

III. METTRE EN PLACE LES ACTIONS DE MISE EN CONFORMITÉ

>> Faire le grand ménage

Si vous avez en votre possession des données physiques ou informatiques qui ne vous servent plus à rien (le fin fond de votre armoire ?), c'est le moment de vous en débarrasser ! La règle est la suivante : si les données vous ont permis d'atteindre votre objectif, il est nécessaire de les supprimer. En reprenant l'exemple de la candidature, vous pouvez supprimer tous les CV de candidats que vous avez finalement recrutés. Pour les CV non retenus, la loi dit que vous ne pouvez les conserver que 2 ans.

>> Limiter la durée de conservation des données personnelles

Le RGPD limite la durée légale de conservation des données personnelles. Par exemple, le CV d'un candidat non retenu peut être conservé jusque 2 ans après le dernier contact avec lui. Les bulletins de paie peuvent être conservés 5 ans maximum.

En général, les SIRH et Logiciels de gestion de la paie gèrent automatiquement les effacements des données, ou permettent tout du moins de les paramétrer.

Pour en savoir plus sur la durée de conservation des données, c'est par ici.

>> Minimiser les données personnelles collectées

Le RGPD a instauré le principe de minimisation des données. L'employeur est ainsi tenu de recueillir uniquement les données nécessaires, adéquates et pertinentes à la finalité du traitement. Sauf dérogations particulières, la collecte de données sensibles est prohibée.

>> Assurer la sécurité et la confidentialité des données

L'entreprise est garante de la sécurité et de la confidentialité des données de ses candidats, collaborateurs et ex-collaborateurs. Il faut donc vérifier que tous les outils RH utilisés permettent un traitement sécurisé de

la données. Ces outils doivent également permettre de modifier et supprimer les données à tout moment.

Assurez-vous également que les données soient hébergées sur des serveurs respectant les standards de sécurité. En cas de fuite/perte de données, la CNIL doit être informée dans les 72 heures suivant sa découverte sous peine de recevoir une amende. Pour information, 2044 entreprises françaises ont effectué cette démarche depuis l'instauration du RGPD. Afin d'anticiper un tel cas, la CNIL recommande aux entreprises de **rédiger un modèle d'email dont la légalité a été validée et qui puisse être envoyé à tout moment**.

Pour chaque traitement de données, le RGPD oblige l'entreprise à restreindre l'accès aux données. Les intervenants internes et externes doivent être renseignés dans le registre de traitement des données cité plus haut.

Quant aux collaborateurs, il est nécessaire de les sensibiliser aux cyber-risques. Vous pouvez par exemple créer un référentiel de sécurité et le diffuser au sein de votre entreprise.

Enfin, si vous sentez qu'un traitement de données peut engendrer un risque élevé pour les droits et libertés de vos collaborateurs, la CNIC impose de réaliser une **Analyse d'Impact relative à la Protection des Données (AIPD)**. Récemment, elle a même rendu l'AIPD obligatoire pour les services RH. Nous vous conseillons de vous rapprocher de votre DPO pour la mettre en place.

>> Informer et obtenir le consentement de vos collaborateurs / candidats

RGPD est synonyme de transparence. Il est nécessaire d'informer clairement vos collaborateurs : quelles sont les données personnelles utilisées ? Dans quel but ? Combien de temps seront-elles conservées ? Toutes ces informations peuvent être indiquées dans vos supports : contrats de travail, site de recrutement... Le RGPD prescrit un consentement "spécifique, clair, équivoque". Dans le cas d'un candidat par exemple, on pourrait imaginer une case à cocher au moment de la candidature indiquant : "j'accepte que mon CV soit conservé 2 ans dans le but d'un recrutement futur".

Le RGPD a créé de nouveaux droits aux salariés, tels que le droit à l'oubli et droit à la portabilité des données. Ils doivent également être informés de ces droits et en cas d'exercice de leur droit, l'entreprise devra leur répondre dans un délai d'un mois.

>> Mettre à jour vos politiques de confidentialité

Depuis l'entrée en vigueur du RGPD, votre politique de confidentialité doit informer les collaborateurs de l'usage prévu de leurs données personnelles, détailler une base légale pour la gestion des données RH et expliciter les mesures qui assureront la sécurité des données.

La mise en conformité au RGPD demande donc un effort conséquent de la part du service RH, mais un effort qui sera largement récompensé sur le long terme. Plutôt que de la redouter, il est préférable d'y voir l'opportunité de réorganiser vos processus afin de les fluidifier, renforcer votre marque employeur... Un dernier conseil : ne faites pas cavalier seul. Pour être réussie, la mise en conformité RGPD doit être l'affaire de tous au sein de l'entreprise !

CHIFFRES-CLÉ : LE RGPD, 1 AN APRÈS

281 088 dossiers traités par les autorités en Europe dont :
144 376 plaintes (11 900 en France)
89 271 notifications de fuites de données (2044 en France)

63% de dossiers clôturés
37% de dossiers en cours de traitement

50 millions € : la condamnation record de Google pour ses manquements au RGPD

9700 € : sanction financière la plus faible en Europe
400 000 € : sanction financière la plus haute en Europe

67% des citoyens Européens ont entendu parler du RGPD
36% des citoyens Européens ont bien compris les enjeux du RGPD

Source : EDPB, numerama

L'actu RH du mois de mai

L'actualité de la formation professionnelle en ce mois de mai a surtout été marquée par le **printemps de la formation**, mis en place par Unow.

5 webinars ont eu lieu sur 5 thèmes : les dernières tendances du digital learning, le récapitulatif de la réforme, l'évaluation de l'efficacité des formations, le CPF, et la valorisation des formations en interne pour engager les apprenants.

Les replays ainsi que de **nombreuses ressources** liées à cet événement sont disponibles **ICI**

Les événements à venir en juin

4 juin
Paris
Congrès learning, talent & development

6 juin
Monaco
Top DRH

20 et 21 juin
Paris
Digital learning day