ALEGRIA

travailler dans la bonne humeur

GUIDE RGPD A DESTINATION DES DRH

LIVRE BLANC ALEGRIA

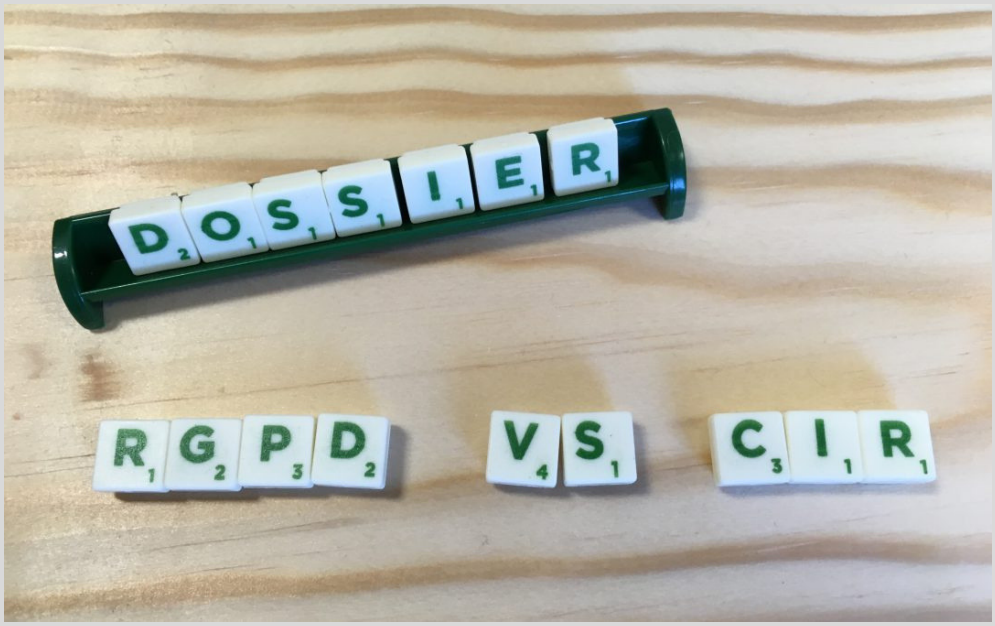
http://alegria.in/
https://www.linkedin.com/in/externalisation-grh-alegria/

« Une personne concernée devrait avoir le droit d'accéder aux données à caractère personnel qui ont été collectées à son sujet et d'exercer ce droit facilement et à des intervalles raisonnables, afin de prendre connaissance du traitement et d'en vérifier la licéité. »

Christine DRH de l'établissement "La Chocolaterie de Charly" se demande comment elle va pouvoir récolter toutes les données de ses salariés tout en respectant les consignes du RGPD sur lesquelles elle ne dispose que de très peu d'information à ce jour.

Si vous êtes comme Christine, alors ce livre blanc est fait pour vous !

SOMMAIRE



Qu'est-ce que le RGPD ?

De quoi s'agit-il ?

Le Règlement Général sur la Protection des données « RGPD » est le nouveau cadre juridique de l'Union Européenne qui gouverne la collecte et le traitement des données à caractère personnel des utilisateurs. Le RGPD est entré en vigueur le 25 mai 2018 et a pour objectifs de :

- Renforcer la protection des données pour les individus
- Sécuriser les données de manière collective

Qui est concerné ?

Toute organisation établie sur le territoire de l'Union Européenne devra se conformer au Règlement RGPD, même si le traitement des données s'effectue depuis l'étranger.
De même que toute organisation établie en dehors de l'Union Européenne, traitant des données personnelles de personnes situées sur le territoire de l'Union.

Qu'est-ce que le RGPD ?

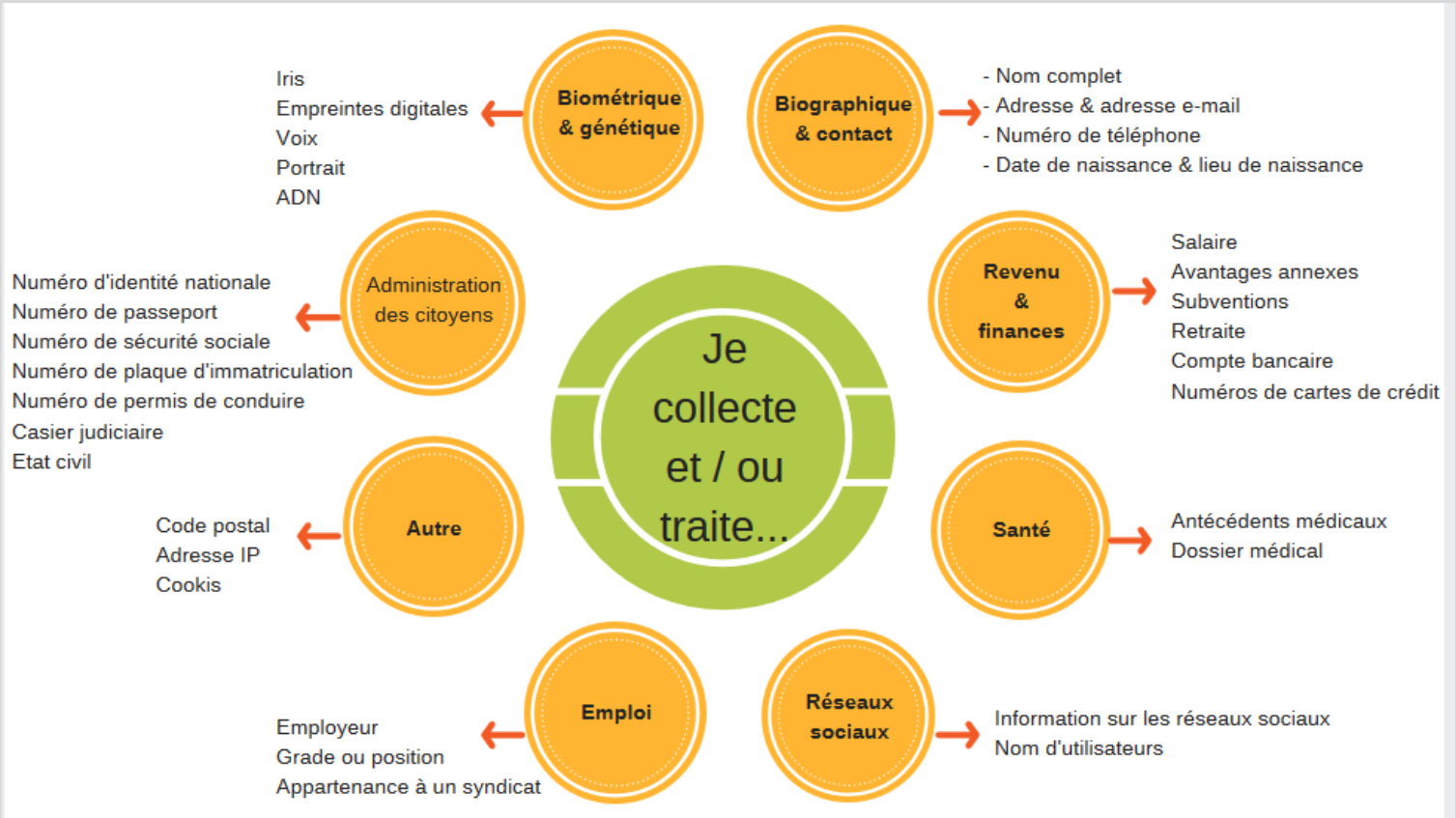
De quoi parle-t-on ?

Données à caractère personnel

"Toute information se rapportant à une personne physique identifiée ou identifiable.
Une définition basée sur le concept d'identification des personnes physiques"
Exemple : Coordonnées postales, téléphoniques, mail etc.

Traitement de données

"Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel"
Exemple : Stockage, organisation, extraction, modification, communication, rapprochement ou interconnexion



Droits et devoirs des salariés

Droit à l'information

Pour être loyale et licite, la collecte de données personnelles doit s'accompagner d'une information claire et précise auprès des personnes concernées sur la façon dont celle-ci va être réalisée

Une possibilité de recours en cas de non-respect de ces droits, auprès de la Commission nationale de l'informatique et des libertés (Cnil) de chaque pays d'Europe

Le droit à la limitation

Le recueil de vos données doit répondre à un motif légitime consigné dans un registre spécifique de l'entreprise

Le droit à l'oubli

Vos données personnelles ne pourront être conservées au-delà de la durée qui aura été indiquée lors de la collecte. Passé ce délai les données devront etre supprimées

Le droit à la suppression

Les salariés doivent pouvoir demander une copie de leurs données personnelles. En cas d'erreur, en particulier en cas de préjudice potentiel, l'entreprise doit rectifier dans les plus brefs délais les informations détenues. Il doit être également possible de demander la suppression des données en retirant son consentement à leur usage

Devoirs

Vos salariés s'engageront à respecter ces règles par différents biais qu'il vous faudra déterminer : mention dans le contrat de travail, signature d'une Charte informatique, signature d'une politique de confidentialité, etc.

5 actions RH pour être prêts!

A savoir : L'employeur ne peut révéler les coordonnées personnelles d'un employé que si la loi ou une décision de justice le prévoit

1. Mettre en place un registre des traitements

La toute première étape est de nommer un délégué à la protection des données, en interne, ou en externe.
Ensuite, l'élaboration (et la tenue) du registre des traitements mis en oeuvre dans l'entreprise est une des clés de voûte du RGPD !
Vous devez être en capacité d'identifier avec précision les types de données à caractère personnel dont dispose votre organisation, notamment le service RH, et savoir où celles-ci sont stockées et transférées.
L'élaboration du registre consiste à indiquer pour chaque traitement de données personnelles:

- La finalité du traitement (exemples: gestion des clients, paye, etc.)
- Les catégories de personnes concernées (exemples: salariés, clients, etc.)
- La nature des données traitées (exemples: noms, prénoms, données de santé, etc.)
- Les catégories de destinataires amenées à utiliser les données (DRH, service informatique, prestataires, etc.)
- Les transferts en dehors de l'UE
- Les durées de conservation
- Les mesures de sécurité techniques et organisationnelles mises en place pour la proctection de ces données.

5 actions RH pour être prêts!

2. Informer, informer et informer !

Information CSE

Prevenez les membres de votre CSE concernant cette nouvelle réglementation et ce qu'elle implique ! Ils disposent certainement de données personnelles sur les salariés, notamment via le registre unique du personnel, et doivent être vigilants à respecter les principes cités en amont ! (photos du personnel prises lors d'évènements, informations sur les enfants du personnel, etc.).

5 actions RH pour être prêts!

2. Informer, informer et informer ! (suite)

Information aux managers

Les managers doivent également se sentir concernés par le règlement européen, en tant que salariés mais aussi en tant que responsables d'équipes ! Les supérieurs hiérarchiques peuvent accéder aux informations nécessaires à l'exercice de leur fonction (exemple : données d'évaluations, rémunération, etc.) mais il est important qu'ils montrent l'exemple en protégeant les données de leurs collaborateurs.

Cette communication peut être l'occasion de remettre à plat les processus internes afin de renforcer la sécurité !

Conserver sur son disque dur le CV d'un candidat ou le compte rendu par exemple sont des pratiques à bannir.
En cas de doute quant à la protection des données, ils peuvent se référer au délégué à la protection des données désigné ou au service RH

5 actions RH pour être prêts!

3. Sensibiliser, sensibiliser et sensibiliser !

Information générale aux salariés

Informez vos collaborateurs dès que vous leur demandez des informations (exemple mise à jour des données administratives, demande de formation, formulaire d'entretien d'évaluation, etc.) en insérant une note explicative sur la façon dont vous allez les stocker.

Sensibilisez-les sur leurs droits & sur les règles internes de gestion des données personnelles, mais aussi sur les règles élémentaires de sécurité.

A savoir: L'entreprise dispose désormais de 1 mois (2 mois en cas de demandes complexes) pour répondre aux sollicitations des salariés en matière de données personnelles.

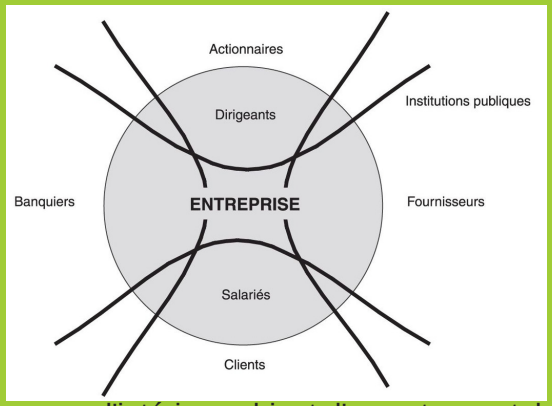
Quels outils pour sensibiliser vos salariés au RGPD ?

Notes de communications internes , rédaction et diffusion d'un « Guide pratique », mise en place de formations managers ou de réunions d'information

Documents officiels tels que le contrat de travail (non obligatoire bien que recommandé), le règlement intérieur ou la charte informatique.

5 actions RH pour être prêts!

4. Vérifier que vos prestataires travaillent en respectant les principes du RGPD



agences d'intérim, cabinet d'expert-comptable, conseil juridique, externalisation RH, etc.

Il est mportant d'être certain que les prestataires avec lesquels vous travaillez vont, eux aussi, protéger les données de vos collaborateurs et sont en mesure de les modifier ou de les supprimer dans les temps ! Pensez aux clauses à mettre en place dans vos contrats commerciaux !

5. Faire du nettoyage !

Pensez à supprimer les archives papiers et informatiques qui sont hors délais et qui n'ont plus de raison d'être.

Il peut être judicieux de se pencher régulièrement sur les informations à supprimer, en mettant en place des alertes par exemple.

ALEGRIA
travailler dans la bonne humeur

Mémo: clauses RGPD

Les bons réflexes RGPD!

A adopter !

• Demander l'avis d'un expert local de la protection de la vie privée en amont du démarrage d'un projet/produit pour s'assurer que les mesures nécessaires sont prises afin d'intégrer la vie privée dès la conception

• Ne pas laisser de données personnelles non sécurisées : par exemple sur l'imprimante, sur notre bureau ou via votre mail personnel

• S'assurer du respect du Droit à l'image lors du recueil et de la diffusion de photos/vidéos de collaborateurs ou de personnes extérieures

• Etre prudent avec le partage de données personnelles avec d'autres : les limiter et se demander s'il est nécessaire de les conserver.

Exemple de questions à se poser : quel est l'utilité de cette donnée ? Ai-je besoin de la conserver ? Combien de temps ? A quel endroit afin d'éviter au maximum le risque de brèche ? (Préférez le réseau sécurisé plutôt que le bureau de votre ordinateur).

Les bons réflexes RGPD!

Communication par mail

• Les données personnelles ne doivent pas être envoyées par e-mail, chat ou par message texte. Ceci s'applique lorsque vos salariés envoient des données personnelles à propos d'une personne différente de la personne avec laquelle ils sont en train d'interagir.

• Si une personne envoie un courriel contenant des données sensibles, il convient de noter que cela ne constitue pas un consentement du traitement de ces données. Il ne faut donc pas répondre à l'e-mail sans supprimer les données sensibles et par la suite l'e-mail d'origine lui-même.

Rappel : Gestion de la messagerie par l'employeur

L'employeur peut contrôler et limiter l'utilisation d'internet (via des dispositifs de filtrage de sites, détection de virus, etc.) et de la messagerie (outils de mesure de la fréquence des envois et/ou de la taille des messages, filtres « anti-spam », etc.)

Le contrôle doit avoir pour objectif :

* D'assurer la sécurité des réseaux
* De limiter les risques d'abus d'une utilisation trop personnelle

Par défaut, les courriels ont un caractère professionnel. L'employeur peut les lire, y compris en dehors de la présence de l'employé.

Pour qu'ils soient protégés et considérés confidentiels, les messages personnels doivent être identifiés comme tels, par exemple :

* en précisant dans leur objet « Personnel » ou « Privé »,
* en les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

Dans ce cas, la responsabilité de la sécurité des données revient au salarié.

Les bons réflexes RGPD!

Consultations obligatoires

Les instances représentatives du personnel doivent être informées ou consultées avant la mise en oeuvre d'un dispositif de contrôle de l'activité.

Chaque employé doit être notamment informé :

- des finalités poursuivies,
- de la base légale du dispositif (obligation issue du code du travail, ou intérêt légitime de l'employeur),
- des destinataires des données,
- de la durée de conservation des données
- de son droit d'opposition pour motif légitime,
- de ses droits d'accès et de rectification,
- de la possibilité d'introduire une réclamation auprès de la CNIL.

Le Délégué à la Protection des Données (DPO) doit être associé à la mise en oeuvre de ce dispositif.

L'employeur doit inscrire ce dispositif de contrôle dans son registre des activités de traitement de données.

Durées légales de conservation des données

- Données paie : 5 ans
- Images sur caméra : l'employeur doit définir une durée de conservation
- Données relatives aux accès du lieu de travail : suppression après 3 mois
- Les données utilisées pour le suivi du temps de travail, y compris les données relatives aux motifs des absences, doivent être conservées pendant 5 ans
- CV lors de recrutement : 2 ans
- Logs de connexion : ne pas les conserver plus de 6 mois

Focus: recrutement

Vous l'aurez compris, il est indispensable
d'informer les candidats sur ce que vous allez
faire avec les données qu'ils vous ont transmises,
et pendant combien de temps !

Exemple :

« Madame, Monsieur,
Nous accusons réception de votre candidature et nous vous remercions de l'intérêt que vous portez à l'entreprise. Votre dossier sera traité dans les plus brefs délais.
Sans nouvelles de notre part dans un délai de trois semaines à la réception de ce mail, veuillez considérer que nous ne sommes pas en mesure de donner une suite favorable à votre candidature.
Sauf avis contraire de votre part, l'ensemble de vos données et des éléments que vous nous avez transmis sera conservé dans notre base de données pendant une durée maximale de (...) afin de vous faire part d'éventuelles opportunités susceptibles de correspondre à votre profil.
Ces données seront uniquement conservées à des fins de recrutement et ne seront accessibles qu'aux personnes chargées du recrutement.
Conformément à la réglementation en vigueur en matière de protection des données personnelles, vous disposez d'un droit d'accès aux informations vous concernant, ainsi que d'un droit de rectification, d'opposition, de limitation du traitement et de suppression que vous pouvez exercer par mail en vous adressant à l'adresse suivante : (...) »

Focus: recrutement (suite)

• Veillez à stocker vos CV dans un endroit sécurisé : dans un dossier sur votre réseau protégé, dans un système d'information RH mais éviter votre bureau d'ordinateur !

• Mettez-vous des alertes afin de penser à supprimer les CV de votre CVthèque au bout de deux ans ou avant si les candidats n'ont pas accepté qu'ils soient conservés !

• Assurez-vous que les managers avec lesquels vous travaillez sur les recrutements ne conservent pas les CV au-delà des 2 ans et dans des endroits sécurisés !

Les managers qui interviennent dans le processus de recrutement peuvent accéder aux informations d'un candidat.

Attention, les données collectées doivent être seulement celles indispensables pour évaluer la candidature.

En plus des administrations informées de l'embauche (pôle emploi, organismes de retraite, de prévoyance, de santé, etc.), seules les personnes chargées de la gestion du personnel doivent avoir accès aux informations des employés.

ALEGRIA
travailler dans la bonne humeur

Pour en savoir plus :
www.alegria.in
04.57.39.16.66