

CHARTE

ÉTHIQUE & NUMÉRIQUE RH

#MakeHRgreatagain

1. OBJET & ORIGINE DE LA CHARTE

Le numérique pénètre progressivement tous les aspects de la vie privée et de la vie professionnelle. Il permet aux organisations de gagner en productivité, et également de disposer d'informations jusqu'alors difficilement disponibles. Les usages numériques évoluent plus rapidement que l'action du législateur, et certaines pratiques, en dehors de toute considération réglementaire, suscitent des interrogations quant à l'éthique qu'elles embarquent.

Un flou considérable demeure actuellement sur les sujets d'utilisation des données, en lien avec l'absence de bonnes pratiques en matière de numérique appliqué aux Ressources Humaines.

La présente Charte Ethique & Numérique RH a pour objet de poser un cadre de bonnes pratiques pour l'utilisation de solutions numériques dans le domaine des Ressources Humaines, afin que les droits, libertés et sensibilités de chacun.e soient respectés.

Lors de sa table ronde sur l'Intelligence Artificielle et les Ressources Humaines le 14 juin 2017, la CFE-CGC avait réalisé un questionnaire auprès de ses militants (1.263 répondants). Si beaucoup s'inquiétaient de la perte de contrôle humain (63%), 92% fixaient comme priorité l'établissement d'une charte éthique autour de l'usage des algorithmes dans le recrutement et la gestion RH.

Cette charte a été rédigée sous l'impulsion de la CFE-CGC, puis du Lab RH, en collaboration avec la CNIL, le Ministère du Travail, de l'Emploi, de la Formation Professionnelle et du Dialogue Social, et le Secrétariat au Numérique.

Cette charte s'appuie notamment sur le nouveau cadre juridique que constitue le Règlement de Gestion et de Protection des Données, qui s'appliquera dès le 25 mai 2018 aux responsables de traitement des données.

Incitée par le Règlement de Gestion de Protection des Données, cette Charte constitue pour ses adhérents un outil méthodologique de facilitation de mise en conformité avec leurs obligations.

Cette charte s'inscrit dans une politique générale de Responsabilité Sociale d'Entreprise, en impulsant des pratiques numériques vertueuses, respectueuses des parties prenantes. Elle ambitionne ainsi de créer les conditions favorables d'un développement économique basée sur la donnée.

2. DEFINITIONS

Algorithme : toute suite finie d'opérations logiques, combinant et transformant des données d'entrée en vue de fournir un ou plusieurs résultats. Un algorithme est constitué de critères et de pondérations, reliés entre eux par des opérations mathématiques. Un algorithme de qualité est censé reproduire les meilleures pratiques du processus qu'il gère, pour chacun des cas d'usage susceptibles d'être rencontrés.

Bonne pratique : tout ensemble de comportements qui font consensus et qui sont considérés comme indispensables par la plupart des professionnels pour la qualité d'un domaine donné. La gestion des bonnes pratiques dans un domaine implique une veille stratégique et une gestion approfondie des connaissances de ce domaine.

Donnée : toute information constitue potentiellement une donnée. Une information devient une donnée dès lors qu'elle est recueillie.

Donnée brute : toute donnée recueillie et n'ayant subi aucun traitement algorithmique.

Donnée sensible (Définition CNIL) : toute information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

Donnée transformée : toute donnée ayant subi un traitement algorithmique.

Donnée personnelle (Définition CNIL) : toute information identifiant directement ou indirectement une personne physique. Des exemples courants incluent : nom, identifiant, numéro de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...

IHM ou Interface Homme Machine : toute interface permettant une transmission d'informations entre un individu et un dispositif numérique de manière unilatérale ou interactive. Il existe des IHM d'entrée et de sortie, permettant respectivement l'acquisition et la restitution de données.

Des exemples courants d'IHM d'entrée incluent : souris, clavier, capteur, écran tactile, microphone, caméra...

Des exemples courants d'IHM de sortie incluent : écran, imprimante, haut-parleur...

Matching : toute opération visant à faire correspondre des objets, contenus ou individus en fonction d'un ensemble de critères pré-définis.

Matching Affinitaire : toute opération visant à suggérer une correspondance, à partir de données spécifiques aux deux objets, contenus ou individus à faire correspondre. Un matching affinitaire de qualité est basé sur une connaissance suffisante des critères et pondérations permettant la pertinence du matching.

Matching Prédicatif : toute opération visant à suggérer une correspondance future, à partir d'une large quantité de données issues du passé. Il s'agit d'une approche statistique basée sur une large quantité de données dépassant largement les objets, contenus ou individus à faire correspondre, et visant à prolonger dans le futur la validité de modèles statistiques mis en évidence grâce aux données du passé.

Responsabilité Sociale d'Entreprise (définition de la Commission Européenne) : La RSE est «La responsabilité des entreprises vis à vis des effets qu'elles exercent sur la société ». La Commission précise qu'afin de s'acquitter pleinement de leur responsabilité sociale, il convient que les entreprises aient engagé, en collaboration étroite avec leurs parties prenantes, un processus destiné à intégrer les préoccupations en matière sociale, environnementale, éthique, de droits de l'homme et de consommateurs dans leurs activités commerciales et leur stratégie de base.

Réseau Social d'Entreprise: Toute plateforme de communication interne à l'entreprise ou à un Groupe d'Entreprise. Le Réseau Social d'Entreprise vise à faciliter le travail collaboratif et à fluidifier les échanges entre salariés d'une même entreprise ou d'un même groupe. Cette plateforme peut s'ouvrir à l'ensemble des parties prenantes ayant un lien professionnel avec l'Entreprise (ou Groupe d'Entreprises), tels les prestataires, les clients, les distributeurs, etc...

Sous-Traitant: Toute entité (personne physique ou morale) juridiquement indépendante, qui sous la responsabilité d'une entreprise principale, s'engage envers cette dernière à réaliser un travail en sous-oeuvre.

Tiers-Fournisseur : Toute entité (personne physique ou morale) juridiquement indépendante, fournissant une prestation finie envers une entreprise principale, sans que cette dernière n'ait exercée sa responsabilité dans l'exécution du travail ayant conduit à la prestation.

Traitement de Données (Définition CNIL) : toute opération, ou ensemble d'opérations, portant sur des données, quel que soit le procédé utilisé. Des exemples de procédé de traitement de données incluent : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction. L'acquisition, la restitution et le stockage de données constituent donc une forme de traitement de données.

3. RAPPELS DES PRINCIPES DE LA CNIL

Cette charte vient en complément de la législation française en vigueur en matière de données, et des travaux menés par ailleurs par la CNIL.

Cette charte ne saurait en aucun cas se substituer à des obligations légales, ni des recommandations existantes de la CNIL.

Les travaux et publications de la CNIL en lien avec les Ressources Humaines peuvent être retrouvés sur les supports de la CNIL, notamment à l'adresse web suivante, disponible au moment de la publication de la présente charte :

<https://www.cnil.fr/fr/thematique/travail>.

4. RAPPELS DES PRINCIPES DU RGPD ou Règlement 2016/679 du 27 avril 2016

Le RGPD est le Règlement Général pour la Protection des Données. Il s'agit du règlement 2016/679 du Parlement européen et du Conseil européen du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

Le RGPD peut être consulté en français sur le site web de la CNIL à l'adresse web suivante, disponible au moment de la publication de la présente charte : <https://www.cnil.fr/fr/reglement-europeen-protection-donnees>.

Des informations complémentaires peuvent être consultées sur le site web dédié de l'Union Européenne, à l'adresse web suivante, disponible au moment de la publication de la présente charte : <http://www.eugdpr.org/>

La présente charte s'inscrit pleinement dans le respect du RGPD, et attire l'attention sur huit principes essentiels, définis dans le règlement européen :

La Transparence : l'employeur a l'obligation d'informer les salariés des motifs de traitement de ses données personnelles.

Le Recueil du Consentement : l'employeur doit recueillir le consentement des salariés dont les données sont traitées.

La limitation des finalités : l'employeur a l'obligation de traiter les données que dans le cadre d'une finalité précise et déterminée.

La minimisation des données : l'employeur s'engage à ce que seules les données qui sont nécessaires au regard de la finalité du traitement soient collectées et utilisées.

L'exactitude des données : l'employeur a l'obligation de s'assurer de l'exactitude des données et doit permettre aux salariés de corriger les inexactitudes.

La limitation de conservation : l'employeur a l'obligation de conserver les données uniquement sur une période en adéquation avec la finalité retenue.

La confidentialité et la sécurité : l'employeur doit s'assurer de la bonne protection des données, au regard de traitement inapproprié, de perte ou vol, et pouvoir démontrer la mise en place de mesure de sécurité approprié.

La Responsabilité : l'employeur doit être en capacité de démontrer le bon respect des principes ci-dessus.

5. CYCLE DE VIE DES DONNÉES

Toute donnée doit être recueillie pour commencer son cycle de vie. Certaines des données recueillies ont vocation à être traitées via un traitement algorithmique. Les données transformées, ainsi que les données brutes, peuvent être restituées à un utilisateur sous divers formats, via une IHM. La totalité de ces données peuvent être stockées dans des bases de données, selon une structuration pré-définie par les concepteurs de la base de données.

Chacune de ces étapes (acquisition, traitement, restitution, stockage et structuration), peut présenter des spécificités et enjeux, susceptibles de contrevenir aux dispositions légales en vigueur, et plus largement à des considérations éthiques. Afin d'agir au mieux, la présente charte propose d'identifier les bonnes pratiques pour chacune des étapes du cycle de vie des données.

6. BONNES PRATIQUES POUR L'ACQUISITION DES DONNÉES

L'acquisition des données est l'étape qui permet le recueil de données. Ce recueil peut être opéré manuellement ou automatiquement. Le mode manuel implique la saisie d'informations dans des

champs spécifiques sur une IHM, et donc une action volontaire de saisie de la donnée. Le mode automatique implique le recueil de données sans action volontaire de la part de l'individu concerné.

Dans les deux modes, manuel et automatique, il est impératif que les données recueillies concernant un individu soient recueillies en amont de l'usage fait de ces données sur **la base du volontariat et de façon éclairée** (déclaration ou acte positif explicite, informations claires et compréhensibles) permettant une liberté de choix, avec possibilité de réversibilité du consentement.

Le refus par un individu, de recueillir ses données personnelles, ne peut constituer pour l'individu en question un critère de discrimination.

Le recueil manuel de données personnelles par un tiers sans le consentement de l'individu concerné est à éviter, sauf à s'assurer que le tiers dispose des autorisations nécessaires. Cela inclut notamment :

- le remplissage de champs à but professionnel (recopie du profil LinkedIn d'un collaborateur en vue d'alimenter la CVthèque interne, saisie d'informations recueillies oralement...);
- le remplissage de champs à but commercial ou viral (recueil d'adresses mail, d'identifiants réseaux sociaux...).

Le recueil manuel de données personnelles par un tiers, doit s'effectuer de façon claire, lisible et concise. Il convient d'éclairer la personne afin qu'elle puisse effectuer son choix librement. A titre d'exemple, le recueil du consentement au travers d'une acceptation de Conditions Générales d'Utilisation volumineuse et illisible est à proscrire.

Le recueil automatique de données personnelles sans le consentement de l'individu concerné est à proscrire strictement. Cela inclut notamment :

- la récupération automatique de BioData sans l'accord formel de l'individu concerné (récupération des données du profil LinkedIn, récupération de données personnelles trouvées sur les moteurs de recherche...);
- l'interprétation de données personnelles à partir d'autres données sans l'accord formel de l'individu concerné (analyse automatique du comportement à partir du profil Facebook, à partir d'éléments de navigation ou de toute autre donnée...);
- la récupération massive et automatisée de données (crowling).
- la captation de toute information biométrique.

Principe d'extension des bonnes pratiques du recueil des données à toute la chaîne de valeur: Lorsque des travaux nécessitant le recueil de données, sont confiés à un Sous-traitant, l'entreprise s'assure que ce recueil s'effectue avec les mêmes garanties et dans les mêmes conditions que si elle exécutait elle-même ce recueil. Cette extension des bonnes pratiques s'applique aussi dans le cadre d'utilisation

d'outils fournis par des Tiers-Fournisseurs, tel le recours à des outils de Réseau Social d'Entreprise, ou des objets connectés de toute nature. L'entreprise ne peut proposer l'utilisation d'outils développés par un Tiers-Fournisseur, sans en garantir une application de règles d'acquisition des données identique à celle qu'elle s'impose à elle-même.

7. BONNES PRATIQUES POUR LE TRAITEMENT ALGORITHMIQUE DES DONNÉES

Principe de Loyauté du traitement algorithmique : Le traitement algorithmique des données doit s'effectuer de façon transparente, après information auprès des personnes concernées de l'utilisation de leurs données personnelles et de la finalité du traitement. Les personnes doivent également être informées des différents droits dont elles disposent ainsi que de leurs modalités d'exercice.

Principe de neutralité du traitement algorithmique : Le traitement algorithmique des données ne doit en aucun cas permettre d'aboutir à une donnée sensible.

Principe de simplicité et "d'explicabilité" du traitement algorithmique : les responsables des Ressources Humaines ne doivent pas appuyer leurs décisions sur le résultat d'algorithmes dont ils ne peuvent expliquer en détail la logique, les critères et les pondérations. Plus un algorithme est complexe, moins il sera évident de comprendre la logique des résultats qu'il proposera, et moins la décision qui en résultera relèvera d'une logique construite et responsable.

Principe de maîtrise du traitement algorithmique : la culture et les processus de toute organisation étant spécifiques, tout algorithme visant à remplacer un processus doit être co-construit, et au minimum validé par les responsables des Ressources Humaines qui en auront analysé les impacts dans le cadre d'une étude spécifique.

Dans le cas d'outils délivrés par un Tiers-Fournisseur, il conviendra de recenser tous ceux utilisant des traitements algorithmiques, d'en analyser les impacts afin de s'assurer de leur bon respect des bonnes pratiques. Cette analyse devra être effectuée régulièrement, pour garantir l'intégration des bonnes pratiques dans les montées de version des outils.

Afin de permettre un échange sur le sujet du traitement algorithmique avec les partenaires sociaux, l'entreprise intégrera cet item dans son Document Unique d'Evaluation des Risques Professionnels. .

Principe de précaution du traitement algorithmique : le matching prédictif ne doit pas être appliqué pour la gestion des Ressources Humaines appliquée à un individu en particulier. Ainsi, dans la mesure où le matching prédictif est basé sur des représentations statistiques, c'est sur le plan des populations qu'il doit être appliqué, afin de définir des tendances et informations de contexte pour un métier ou famille de métiers, un secteur d'activités, un groupe d'individus. Chaque individu doit être sujet à un matching qui ne réduit pas sa compatibilité à une moyenne statistique ou des personnes a priori similaires. En

effet, les modèles statistiques issus des données du passé ne présentent objectivement aucune validité pour le futur, en raison de quatre biais majeurs :

- les pratiques du passé ne sont pas exemplaires ;
- l'approche statistique a pour effet d'écraser les anomalies et valeurs insignifiantes, pourtant connues sous le nom de 'diversité' en matière de Ressources Humaines ;
- les conditions et le contexte du passé ne ressemblent aucunement aux conditions et au contexte du futur ;
- La prédictivité ne peut être mesurée que par la mise en situation et des attentes explicites.

Principe de sous-traitance du traitement algorithmique : Lorsqu'un traitement algorithmique est sous-traité, l'entreprise donneuse d'ordre doit s'assurer que le sous-traitant présente les mêmes garanties de protection et répond aux mêmes obligations qu'elle-même.

8. BONNES PRATIQUES POUR LA RESTITUTION DES DONNÉES

Les données brutes et transformées doivent pouvoir être restituées à un individu sans possibilité de mener à une action involontaire ou volontaire de discrimination, en lien avec le format de restitution des données.

L'individu doit être informé des droits dont il dispose lors de la restitution des traitements le concernant, en particulier son droit à ne pas faire l'objet d'une décision si le traitement est un traitement automatisé et produisant des effets juridiques.

L'entreprise s'assure que les droits décrits ci-dessus sont appliqués par les sous-traitantset/ou Tiers-Fournisseurs avec lesquels elle est en relation.

9. BONNES PRATIQUES POUR LA STRUCTURATION ET LE STOCKAGE DES DONNÉES

Les données brutes doivent être conservées sans aucune forme de traitement algorithmique, en tant que données brutes. Les données traitées doivent également être stockées.

Le responsable du traitement doit s'assurer de la sécurité et de la confidentialité des données conservées, y compris lorsqu'il a confié le traitement à un sous-traitant, ou lorsqu'il a mis en relation au moins un de ses salariés avec un Tiers-Fournisseur.

Dans tous les cas, la durée de stockage des données doit correspondre aux dispositions prévues par le RGPD.

10. SYMÉTRIE DES ATTENTIONS

Actions de Formation et sensibilisation

Pour permettre à cette charte de bonnes pratiques de se diffuser pleinement au sein de l'Entreprise, le responsable des traitements accompagnera sa mise en œuvre par des actions de formation auprès des acteurs intervenant dans une des étapes du cycle de vie de la donnée. Une sensibilisation de l'ensemble du personnel, expliquant le cycle de vie, ses enjeux et ses conséquences permettra de diffuser une « culture donnée » à toute l'entreprise

11. CONCLUSION

La présente charte présente un ensemble de définitions, principes et bonnes pratiques, afin de permettre une utilisation responsable des données personnelles dans le domaine des Ressources Humaines. L'ensemble des contenus décrits relèvent d'un bon sens commun, ainsi que d'une culture responsable du numérique, qu'il convient d'adopter et de diffuser largement.

Les Ressources Humaines ne pourront pleinement jouer leur rôle qu'en s'appropriant pleinement les enjeux liés aux données personnelles.

#MakeHRgreatagain