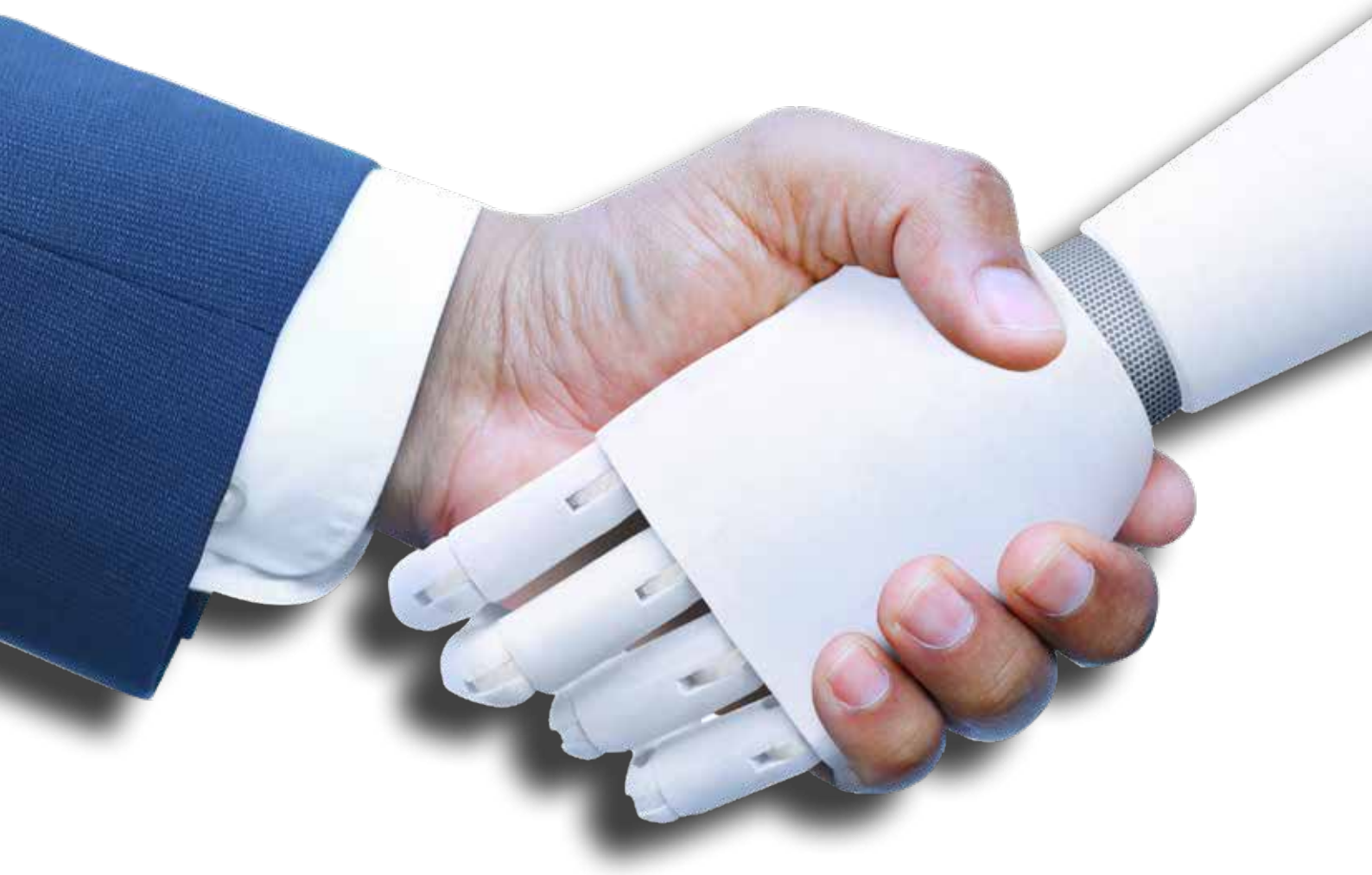
CHARTE ÉTHIQUE & NUMÉRIQUE RH

« *The price of greatness is responsibility** »

- Winston Churchill



*« *La responsabilité est le prix de la grandeur* »

#MAKEHRGREATAGAIN

« rendez leur grandeur aux ressources humaines »

PRÉAMBULE

L'utilisation de plus en plus importante des outils numériques au sein des ressources humaines est à voir comme une véritable opportunité pour les acteurs qui œuvrent dans ce domaine. En effet, aujourd'hui, grâce aux évolutions techniques et informatiques, les ressources humaines peuvent non seulement numériser[1] les tâches, mais surtout les digitaliser[2].

Ces progrès sont à envisager comme une liberté nouvelle offerte aux acteurs RH qui peuvent dès lors se concentrer sur le développement des compétences qui font d'eux des collaborateurs de qualité : créativité, esprit critique, communication et collaboration. Ces compétences font la force et la distinction de l'Homme face à la machine.

Cette Charte a pour but de faire prendre conscience aux acteurs RH que leur travail et leur rôle changent. Ils dessinent et dessineront, par leurs actions et leurs choix, le monde du travail de demain.

1 - Convertir un objet ou processus physique en objet ou processus numérique.
2 - Automatiser certaines tâches historiquement opérées par des humains afin de disposer de données utilisables pour des opérations qui n'étaient alors pas couvertes classiquement.

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.

S'il existe une doctrine élaborée par la CNIL sur certains points spécifiques traitant du Numérique dans les ressources humaines, tels les enregistrements, la géolocalisation ou encore la lecture des mails, plusieurs domaines, en particulier ceux utilisant les traitements algorithmiques, posent question. Du fait de l'absence de regroupement de bonnes pratiques sur l'ensemble du domaine des ressources humaines, un flou demeure actuellement sur les sujets d'utilisation des données.

La présente Charte éthique & 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. Elle entend couvrir le domaine des ressources humaines dans son ensemble, à savoir dès la phase de recrutement, avant même l'établissement d'un contrat de travail.

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 général sur la protection des données, définissant la protection des données comme un droit fondamental. Il s'applique depuis le 25 mai 2018 aux responsables de traitement des données, aux sous-traitants et à l'ensemble des acteurs.

Incitée par le RGPD et son article 88 offrant la possibilité de porter ce sujet au sein d'une convention collective, 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** (RSE), en impulsant des pratiques numériques vertueuses, respectueuses des parties prenantes. Elle ambitionne ainsi de créer les conditions favorables d'un développement économique basé sur la donnée.

Enfin, cette Charte, en tant que guide de bonnes pratiques, ambitionne d'être révisée de manière collaborative à intervalle régulier. Comme cela a été fait pour l'écriture de cette première version, la parole continuera de vous être donnée par le biais de dispositifs variés[3], car l'enrichissement que chacun peut apporter à cette Charte est notre manière de construire aujourd'hui et ensemble le monde dans lequel nous voulons vivre demain.

3 - Ateliers de co-construction, échanges sur plateformes numériques...

DÉFINITIONS

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.

Étude d'impact relative à la protection des données ou PIA (Privacy impact assessment) : mesure prévue par le Règlement général de la protection des données dès lors qu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. L'analyse d'impact repose sur :

- une évaluation juridique du traitement algorithmique (analyse de la nécessité et de la proportionnalité par rapport aux principes et droits fondamentaux) ;
- une évaluation technique du traitement algorithmique (analyse des risques concernant la sécurité des données).

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.

Collaborateur : tout individu qui intègre une organisation, peu importe le statut sous lequel il est désigné contractuellement (CDI, CDD, stagiaire, apprenti, intérimaire, bénévole, etc).

Délégué à la protection des données (DPD, ou DPO, pour Data protection officer) :

Personne physique ou morale chargée de mettre en œuvre la conformité au RGPD au sein de l'organisme qui l'a désigné, s'agissant de l'ensemble des traitements mis en œuvre par ledit organisme. A ce titre, et comme explicité dans la charte de déontologie[4] des délégués à la protection des données de l'AFCDP :

- il veille au respect du RGPD et de la Loi Informatique et Libertés ;
- il établit et maintient la documentation relative aux traitements de données à caractère personnel ;
- il fournit les recommandations et avertissements, demande des arbitrages ;
- il informe et sensibilise les personnels ;
- il informe et conseille son responsable de traitement/sous-traitant.

Il est le successeur du correspondant informatique et libertés.

Discrimination (définition du Code pénal) : toute distinction opérée entre les personnes physiques sur le fondement de leur origine, de leur sexe, de leur situation de famille, de leur grossesse, de leur apparence physique, leur situation économique, leur patronyme ou lieu de résidence, de leur état de santé, de leur perte d'autonomie, de leur handicap, de leurs caractéristiques génétiques, de leurs mœurs, de leur orientation sexuelle, de leur identité de genre, de leur âge, de leurs opinions politiques, de leurs activités syndicales, de leur capacité à s'exprimer dans une langue autre que le français, de leur appartenance ou de leur non-appartenance, vraie ou supposée, à une ethnie, une nation, une prétendue race ou une religion déterminée.

Nombre de ses informations peuvent être recueillies et traitées algorithmiquement. Le contexte de digitalisation ne doit pas faire oublier le maintien du respect de pratiques non-discriminantes.

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 estimatoire : toutes données recueillies dans le cadre des entretiens annuels. Ces données sont utilisées par les travailleurs des ressources humaines comme des documents de travail et ne font pas forcément l'objet d'une restitution.

Donnée de catégorie particulière ou donnée sensible (Définition RGPD) : toute information concernant l'origine raciale ou ethnique, les opinions politiques, les convictions philosophiques ou religieuses, l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Présentées comme interdites de traitement, ces données peuvent en fait l'être sous des conditions très strictes et décrites dans l'article 9.2 du RGPD, notamment une fois recueilli le consentement explicite des personnes.

Donnée transformée : toute donnée ayant subi un traitement algorithmique.

1 - accesible en ligne sur : https://www.afcdp.net/-Charte-de-Deontologie-du-DPO

Donnée à caractère personnelle (définition RGPD) : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

par ailleurs, dans la sphère professionnelle la donnée personnelle peut renvoyer aux données relatives aux parcours professionnels ou aux compétences d'une personne physique mais aussi, dans le cas de recours à des tests, aux données portant sur la personnalité d'une personne physique.

Donneur d'ordre : toute personne physique ou morale pour laquelle un projet est mis en œuvre et doit être réalisé. Il est généralement le commanditaire du projet. Le donneur d'ordre peut être interne ou externe à l'entreprise en charge de la réalisation du projet commandé :

- externe (ex : client) ;
- interne (ex : Comité d'entreprise ou Comité social et économique).

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...

Profilage (définition RGPD) : toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

Matching : Technique consistant à rapprocher des données de profilage avec des données extérieures en vue d'évaluer une compatibilité. L'objectif final est de faire correspondre des objets, contenus ou individus en fonction d'un ensemble de critères pré-définis.

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'entreprises. Le Réseau social d'entreprise vise à faciliter le travail collaboratif et à fluidifier les échanges entre collaborateurs 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.

Règlement européen ou RGPD : règlement européen 2016/679 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 (ci-après « RGPD »).

Responsable de traitement : personne physique ou morale, autorité publique, service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Sous-traitant : personne physique ou morale, autorité publique, service ou autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Il doit présenter les garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité, ce qui ne décharge pas le responsable du traitement de son obligation de veiller au bon respect de ces mesures.

Tiers-fournisseur : personne physique ou morale, autorité publique, service ou organisme, juridiquement indépendante et fournissant une prestation finie envers le responsable de traitement, sans que ce dernier n'ait exercé sa responsabilité dans l'exécution du travail ayant conduit à la prestation.

Traitement de données (définition RGPD) : 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, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

RAPPELS DES PRINCIPES « INFORMATIQUE ET LIBERTÉ »

Cette Charte vient en complément de la législation en vigueur actuellement en France en matière de données, à savoir le RGPD applicable à tous les états membres de l'Union européenne, complété au niveau national par la loi « informatique et liberté » du 6 janvier 1978 modifiée, et des doctrines de la CNIL personnalisées par secteur. 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

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 de l'AFCDP (Association française des correspondants à la protection des données à caractère personnel) qui met à disposition une version annotée et commentée du RGPD : https://www.afcdp.net/Reglement-annote-et-commente-avec

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 et la communication de l'information : l'employeur a l'obligation d'informer les collaborateurs sur l'utilisation qu'il fait de leurs données personnelles, mais aussi du pourquoi il le fait, pour qui et comment. A ce titre, il doit notamment informer les collaborateurs de la source des données personnelles lorsque celles-ci n'ont pas été recueillies directement ; les informer de la finalité de traitement de leurs données personnelles, ainsi que de la base juridique du traitement, et faire connaître le fondement du traitement si ce dernier répond à un intérêt légitime ; et de la durée de conservation des données personnelles. L'employeur doit mentionner l'existence d'une prise de décision automatisée avec l'importance et les conséquences prévues de ce traitement pour le collaborateur concerné. En cas de transfert des données personnelles hors UE, l'employeur doit en informer les collaborateurs. L'employeur doit faciliter l'exercice des droits des collaborateurs, et les informer des droits dont ils disposent (accès, rectification, effacement, portabilité, et possibilité d'introduire une réclamation auprès d'une autorité de contrôle) et leur communiquer les coordonnées du responsable de traitement et du délégué à la protection des données lorsque ce dernier a été désigné.

La licéité des traitements : De façon général, le RGPD prévoit qu'un traitement de données personnelles pour être licite, doit recueillir le consentement de la personne ou s'inscrire dans un des autres cas de licéité prévus par le règlement, à savoir répondre à un intérêt légitime, à une mission d'intérêt public, à une obligation légale, ou à une exécution de contrat passé avec le collaborateur, ou enfin à la sauvegarde des intérêts vitaux de la personne concernée.

De façon plus spécifique, la licéité d'un traitement des données sur le lieu de travail intègre, pour sa part, le caractère « non libre » du collaborateur ; lié par une relation de travail et donc un lien de subordination. Aussi, le groupement des « CNIL européennes », dit G29, considère que « le consentement est très peu susceptible de constituer une base juridique pour le traitement des données sur le lieu de travail, à moins que les employés ne puissent refuser le traitement sans conséquences défavorables ». Par conséquent, les principaux motifs de licéité de traitement sur le lieu de travail seront l'exécution d'un contrat ou l'intérêt légitime, voire les obligations légales.

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

A tire d'exemple : cas des collaborateurs clients de leur entreprise

Les données personnelles de collaborateurs recueillis dans le cadre de leur relation commerciale avec leur

entreprise ne peuvent être utilisées par l'entreprise qu'à cette fin et aux obligations réglementaires associées.

Exemple : un DRH de banque ne peut consulter les comptes bancaires d'un collaborateur ou d'un candidat potentiel, voire interroger le fichier Banque de France ou un opérateur de téléphone ne peut consulter les appels passés par ses collaborateurs.

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.

Par exemple, une utilisation abusive d'internet peut être détectée sans qu'il soit nécessaire d'analyser le contenu de sites web.

L'exactitude des données : l'employeur a l'obligation de s'assurer que les données soient mises à jour régulièrement, qu'elles soient enregistrées correctement, et qu'elles ne soient pas altérées après saisie dans ses systèmes. Il doit permettre aux collaborateurs 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 mesures de sécurité appropriées.

La responsabilité : l'employeur doit être en capacité de démontrer le bon respect des principes ci-dessus, et en particulier le bon respect de ses obligations d'information des collaborateurs.

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, idéalement 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 quelle que soit la nature de la donnée (personnelle, sensible, personnelle à caractère professionnelle, etc).

Tout **collaborateur** est susceptible de voir son employeur collecter de la donnée à son propos. De ce fait, les acteurs des ressources humaines doivent instaurer un climat de confiance vis-à-vis de ces pratiques, en s'appuyant notamment sur un arbitrage sain entre la logique des algorithmes, leurs expériences du métier et leur intelligence émotionnelle.

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 grâce à une **IHM**. Dans ce cas, la saisie est généralement effectuée de manière volontaire par l'individu concerné. Le mode automatique implique le recueil de données sans action volontaire de la part de l'individu concerné.

Dans le cas du recueil manuel comme dans celui du recueil automatique il est possible que la saisie soit effectuée par un tiers (Administration RH, manager,...). Il convient de dissocier le cas d'acquisition des données par recueil du consentement (recrutement, inscription à un réseau social d'entreprise optionnel), et le cas d'acquisition sans consentement pour répondre à un intérêt légitime par exemple.

Acquisition avec recueil du consentement

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 de profils issus de réseaux social/professionnel 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. Il serait préférable et bénéfique de proposer une version pictographique ou infographique afin de faciliter la lecture et la compréhension.

Dans le cadre d'un recrutement, 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 de données issues de profils créés sur des réseaux sociaux/professionnels, 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 sur les réseaux sociaux/professionnels, à partir d'éléments de navigation ou de toute autre donnée...) ;
- la récupération massive et automatisée de données (crawling et scaping) ;
- la captation de toute information biométrique ;

Acquisition sans recueil du consentement

L'acquisition de données personnelles peut se faire sans le recueil du consentement du collaborateur, notamment dans les cas où le traitement des données personnelles répond :

- à l'exécution d'un contrat (tel le contrat de travail avec le traitement de la paie qui est associée),
- à l'application d'une obligation légale (par exemple un employeur soumis à des traitements de lutte contre la fraude),
- à un intérêt légitime (par exemple l'analyse d'un registre d'entrée/sortie de collaborateurs ayant accès à une salle sécurisée après constatation d'un vol).

Quel que soit le motif, l'absence de recueil de consentement oblige l'employeur à fournir aux collaborateurs l'ensemble des informations prévues à l'article 14 du RGPD, et reprises en grande partie dans le principe de transparence et de communication de l'information de la présente Charte.

L'intérêt légitime ne peut être invoqué comme fondement juridique que si le traitement est strictement nécessaire à des fins légitimes et s'il est conforme aux principes de proportionnalité et de subsidiarité.

A titre d'exemple, le fait qu'un employeur soit propriétaire de moyens électroniques n'exclut pas le droit des collaborateurs à la confidentialité de leurs données de localisation. Le recueil des données de géolocalisation (caméras, serveurs, téléphone, voitures, bornes de passage...) doit se limiter au cas où il est strictement nécessaire à des fins légitimes. Les collectes de données

par le biais d'outils de l'entreprise devront être désactivées en dehors des heures de travail et pour les représentants du personnel, lors de leur activité syndicale (voiture de pool, mobile, ordinateur, borne de géolocalisation dans les locaux syndicaux, badgeuses…).

Dans le cas de traitement susceptible d'engendrer un risque élevé pour les droits et libertés des collaborateurs, l'employeur devra réaliser, avant le déploiement de l'outil, une étude d'impact relative à la protection des données. De façon pratique, la CNIL a dressé une liste de critères permettant d'appréhender le besoin d'étude d'impact. Ces critères regardent si le traitement utilise ou engendre une évaluation / scoring (y compris le profilage) ; une décision automatique avec effet légal ou similaire ; une surveillance systématique; une collecte de données sensibles ; une collecte de données personnelles à large échelle ; un croisement de données; des personnes vulnérables (patients, personnes âgées, enfants, etc) ; un usage innovant (utilisation d'une nouvelle technologie) ; l'exclusion du bénéfice d'un droit/ contrat. Un traitement répondant à au moins deux des critères énumérés doit nécessairement faire l'objet d'une étude d'impact relative à la protection des données.

Exemple : une entreprise qui met en place un contrôle de l'activité de ses salariés doit réaliser une étude d'impact relative à la protection des données car le traitement remplit le critère de la surveillance systématique et celui des données concernant des personnes vulnérables.

Lors de cette étude, il sera en particulier déterminé si toutes les données sont nécessaires, si ce traitement prévaut sur les droits généraux à la vie privée (dont jouissent également les collaborateurs sur le lieu de travail) et quelles mesures doivent être prises pour garantir que les atteintes au droit à la vie privée et au droit au secret des communications sont limitées au minimum nécessaire. L'analyse des risques sur la sécurité des données permettra de définir les mesures à mettre en œuvre pour garantir la protection des données.

Les principaux éléments sur l'analyse d'impact sont accessibles sur le site de la CNIL : https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

Lorsque l'employeur a recours à des traitements fondés sur l'intérêt légitime, il associe les partenaires sociaux de l'entreprise à l'élaboration et l'évaluation des mesures prises, et présente l'ensemble des éléments du dossier (y compris l'étude d'impact relative à la protection des données lorsque cette dernière a été effectuée) devant les instances représentatives du personnel en vue d'une consultation.

Lorsque le traitement de données personnelles répond à un intérêt légitime, le collaborateur ou le candidat doit être informé du fondement du traitement et de l'ensemble de ses droits.

A titre d'exemple, les professionnels RH sont amenés à recueillir des données personnelles dès la phase de recrutement. Il en va de la responsabilité des professionnels RH de s'assurer de leur droit à collecter ces données (il est interdit par exemple de collecter le numéro de Sécurité sociale) et de leur utilisation :

- accès autorisés uniquement aux tiers habilités ;
- traitement ne pouvant aboutir à une discrimination.

Les grands principes de l'acquisition de données

Principe de non détournement de finalité : L'acquisition des données personnelles ne peut s'effectuer que dans le cadre d'une finalité précise. Les données ne peuvent être réutilisées qu'après vérification par le responsable de traitement de la possibilité de le faire librement selon les règles établies à l'article 6.4 du RGPD.

Principe de responsabilité individuelle : les engagements et principes préconisés aux responsables RH ne doivent pas faire oublier aux individus qu'ils sont responsables des données qu'ils rendent publiques et accessibles à tous, notamment via les réseaux sociaux. Il est de leur devoir d'être vigilant quant au contenu des informations qu'ils renseignent.

Principe de responsabilité partagée : l'utilisation de données issues des réseaux sociaux doit être cadrée par des règles qui reposent à la fois sur la responsabilité personnelle des individus qui rendent publiques et accessibles un certain nombre de données et la responsabilité des entreprises.

Ces règles doivent être clairement communiquées et régulièrement rappelées afin d'éviter tout traitement arbitraire des données/ communications que les collaborateurs (ou candidats) pourraient mettre en ligne.

Exemple : Il est recommandé que les collaborateurs qui communiquent sur les réseaux sociaux le fassent à partir de comptes professionnels appartenant à l'entreprise, en ayant préalablement reçu l'autorisation de cette dernière.

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.

Enfin, le tiers fournisseur devrait être en mesure de bloquer certaines données qui, suivant la Loi ne doivent pas être utilisées.

Exemple : le taux de prélèvement à la source.

BONNES PRATIQUES POUR LE TRAITEMENT ALGORITHMIQUE DES DONNÉES

Principe de documentation : chaque traitement est consigné par le responsable de traitement dans le registre des activités de traitement, selon les modalités prévues par l'article 30 du RGPD, complété le cas échéant de l'étude d'impact relative à la protection des données si celle-ci été réalisée. Les informations communiquées aux collaborateurs sur les traitements les concernant, ainsi que les procédures mises en place leur permettant d'exercer leur droit viennent compléter la documentation.

Principe d'information : l'employeur a l'obligation d'informer le collaborateur lorsqu'il effectue des traitements sur ses données personnelles selon le principe de transparence et de communication de l'information du RGPD

Le site de la CNIL propose des exemples pratiques de mention d'information à adapter selon les cas de figure des traitements effectués :

https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation

De façon collective, il est primordial de porter à la connaissance des partenaires sociaux les éléments qui ressortent des différentes études et analyses (interne et externe à l'organisation) qui portent sur les algorithmes afin de permettre un échange éclairé sur le sujet du traitement algorithmique

Principe de limitation du traitement : selon le principe de limitation des finalités prévu par le RGPD, l'employeur ne peut utiliser un traitement qu'aux fins qu'il a déterminés dans la documentation.

Exemple : une entreprise assurant la maintenance d'ascenseurs qui a recours à un outil de géolocalisation de ses salariés en vue

d'optimiser l'organisation du travail ne peut s'en servir pour contrôler les déplacements de ses salariés.

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. Pour se faire il peut être envisagé de :

- mettre en ligne la charte sur l'ensemble des systèmes d'informations RH pour que le collaborateur puisse en prendre connaissance, la signer et l'archiver ;
- insérer les règles de traitement de données sur chaque page où les données seraient susceptibles d'être exploitées.

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 sécurité du traitement : le responsable de traitement, après avoir identifié les risques et les conséquences que le traitement peut engendrer sur la vie privée des collaborateurs, doit mettre en œuvre les moyens lui permettant d'en garantir la sécurité. Cette sécurisation peut recourir à la technique de chiffrement ou encore de « pseudonymisation » Au sens du RGPD, la pseudonymisation est un principe qui énonce que le traitement des données à caractère personnel doit être effectué de telle façon que celui-ci ne puisse plus être attribué à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

La CNIL rassemble dans un guide l'ensemble des mesures permettant de garantir la sécurité des données personnelles :

https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

L'Agence nationale de la sécurité des systèmes d'Information (l'ANSSI) met à disposition un kit de la sécurité des données (fiche, vidéo, guide, formation) : https://www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel/

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 comprennent pas la logique. Cette compréhension doit s'appuyer sur la connaissance :

- des données (échantillon) sur lesquelles repose l'algorithme ;
- des variables utilisées dans l'algorithme ;
- de la marge d'erreur du résultat de l'algorithme.

Par ailleurs, le traitement algorithmique doit respecter la notion d'égalité face à l'algorithme en bannissant toute forme de choix aléatoire, notamment dans le cas de profils ex-aequo.

Enfin 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 maitrise du traitement algorithmique : la culture et les processus de toute organisation étant spécifiques, tout algorithme visant à remplacer un processus peut être co-construit, et au minimum validé par les responsables des ressources humaines. En vertu du principe d'explicabilité, les outils internes à l'organisation ou délivrés par un tiers fournisseur devront être étudiés afin de bannir toute automatisation sans contrôle. Plus un algorithme impacte des décisions importantes plus il doit être maîtrisé et compris. La mesure de cette compréhension peut par exemple passer par un travail d'évaluation de l'impact algorithmique, mené conjointement par l'organisation et les fournisseurs de d'algorithme.

Rappelons que conformément à l'article 35 du RGPD dans le cas de traitement de données personnelles susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées le responsable de traitement qui pourra consulté le Délégué à la protection des données (ou DPO) a l'obligation de mener une étude d'impact relative à la protection des données.

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. L'entreprise donneuse d'ordre en tant que responsable de traitement a l'obligation de veiller au bon respect des mesures mises en œuvre par le sous-traitant.

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. Dès lors, il est essentiel de considérer l'intégralité du panel afin de construire un algorithme qui permet une restitution accessible à tous (malvoyant par exemple).

L'individu doit pouvoir, à tout moment et facilement, consulter et récupérer les données personnelles et agrégées collectées par son employeur dès lors que ces dernières sont restituables. En effet toutes les données ne le sont pas. C'est notamment le cas des données estimatoires qui ont font l'objet d'une utilisation managériale confidentielle.

En cas de rupture de contrat, le collaborateur doit de nouveau être informé de la durée de conservation de ses données personnelles et de son droit à l'effacement, dans les conditions prévues à l'article 17 du RGPD.

En cas de rupture de contrat, le collaborateur doit être informé de la durée de conservation de ses données personnelles et de son droit à l'effacement, dans les conditions prévues à l'article 17 du RGPD.

L'entreprise s'assure que les droits décrits ci-dessus sont appliqués par les **sous-traitants** et/ou **tiers-fournisseurs** avec lesquels elle est en relation.

Dans le cas de contrat de tiers-fournisseurs faisant l'objet d'accord avec les partenaires sociaux, les éléments ayant trait aux différentes étapes du cycle de vie de la donnée sont portés en annexe des accords.

Exemple : accord de vote électronique dans le cadre d'un protocole électoral.

Exemple : accord sur les garanties de santé, prévoyance et retraite.

BONNES PRATIQUES POUR LA STRUCTURATION ET LA DURÉE DE CONSERVATION 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 conservées.

Le responsable du traitement doit s'assurer de la sécurité et de la confidentialité des données conservées, notamment en encadrant l'administration de la gestion des accès aux données, grâce à des profils utilisateurs intégrant une mise à jour des droits.

Ces principes de sécurité et de confidentialité s'appliquent y compris lorsque le traitement des données a été confié à un **sous-traitant**, ou lorsqu'il a mis en relation au moins un de ses collaborateurs avec un **tiers-fournisseur**.

Dans tous les cas, la durée de conservation des données doit correspondre aux dispositions prévues par le RGPD. A noter que certains documents ont une durée de conservation spécifique (fiches de paie, documents des Prud'hommes, etc).

MOYENS DONNÉS AU DELEGUÉ À LA PROTECTION DES DONNÉES

Afin de permettre au délégué à la protection des données de remplir pleinement sa mission, le responsable de traitement met à sa disposition les moyens matériels et organisationnels nécessaires afin de lui garantir l'effectivité de ses missions. Il s'assure qu'il dispose également des ressources nécessaires à ses missions notamment :

- en l'associant d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données ;
- en lui donnant accès aux données ;
- en lui permettant de se former.

INFORMATIONS ET COMMUNICATION

INFORMATION INDIVIDUELLE DES COLLABORATEURS

Les collaborateurs doivent pouvoir identifier les personnes en charge :

- de la récolte des données ;
- de leur traitement ;
- de leur suppression.

Dans le cadre de l'obligation d'information, le collaborateur sera notamment informé des droits dont il dispose, y compris celui de saisir l'autorité de contrôle.

Le collaborateur pourra consulter à tout moment ses données, soit au travers d'outils numériques simples et/ou en ayant des interlocuteurs disponibles et identifiables.

ACTIONS DE FORMATION ET SENSIBILISATION

Pour permettre à cette Charte de bonnes pratiques de se diffuser pleinement au sein de l'entreprise, le délégué à la protection des données pourra, s'il existe, accompagner 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, intégrant également une sensibilisation aux enjeux de sécurité des données.

INFORMATION DES PARTIES PRENANTES

Afin d'associer les différentes parties prenantes de l'entreprise à la politique mise en œuvre de protection des données, une présentation du rapport annuel du DPD est effectué en Conseil d'administration, ainsi qu'en Comité social d'entreprise pour un partage avec les élus du personnel.

Les élus sont les représentants des collaborateurs. À ce titre, ils doivent pouvoir s'assurer de la bonne utilisation et de la sécurisation des données, du bon respect des traitements. Pour ce faire, il convient de prévoir la présentation du registre des traitements de façon annuelle en CSE et les éventuelles études d'impact. Ils devront avoir une visibilité sur les règles utilisées dans les algorithmes et ce qu'il résulte de leur traitement, par le biais d'audit, si nécessaire, lors d'une commission du suivi des traitements des données, par exemple.

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

« rendez leur grandeur aux ressources humaines »

RÉDACTEURS
CFE-CGC :
Raphaëlle BERTHOLON
Fanny MEDINA

Le Lab RH :
Jérémy LAMRI
Boris SIRBEY

RELECTEURS
& CONTRIBUTEURS PRINCIPAUX
Michel BARABEL
Laurence DEVILLERS
Géraldine GALINDO
François GEUZE
David GUILLOCHEAU
André PERRET
Jean PRALONG
Bruno RASLE
Frédéric THORA

RELECTEURS
& CONTRIBUTEURS SECONDAIRES
Caroline ADAM
Thierry ARPIN-PONT
Simon BARON
Jean-Christophe BEAU
Stéphanie BELLANGER
David BERNARD
Sophie BINOT
Nicolas BLANC
Filipe BORGES
Christine BOSSERT
Victor BOUI
Anne BOURGNE
Christophe CHERON
Eric D'AMBRA
Martin DAVY
Jean-François GARNIER
Cedric GERARD
Louis GIBAULT
Philippe GORCE
Jessica GRAZIANI
Carole LAUBRY
André LEGAULT
Andrea LEGOURD
Olivier MARCE
Christine MAUCOURT
Céline MEYRIGNAC
Loïc MICHEL
Aurélie PIAT
Bruno PRADAL
Cédric ROBIN
Yann RUSE
Selim SAADI
Alexis TEPLITCHI
Cristel Brice ZOHOUN

MAISON DE LA CFE-CGC
59 RUE DU ROCHER
75008 PARIS
WWW.CFECGC.ORG

LAB RH
58 BIS RUE DE LA CHAUSSÉE D'ANTIN
75009 PARIS
WWW.LAB-RH.COM