Référentiel

RELATIF AUX TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL

MIS EN ŒUVRE PAR DES ORGANISMES PRIVES OU PUBLICS

AUX FINS DE GESTION DU PERSONNEL

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1 A qui s'adresse ce référentiel ?

Ce référentiel encadre la mise en œuvre des traitements courants de « gestion du personnel » par les employeurs de droit public ou privé, quelle que soit leur forme juridique.

Les termes « personnes employées », « personnels » « effectifs », « moyens humains » ou « ressources humaines », employés dans ce référentiel, sont considérés comme synonymes et désignent l'ensemble des collaborateurs permanents ou temporaires de l'employeur, quel que soit leur statut, type ou durée de contrat, et niveau de rémunération. Sont notamment couverts par les dispositions du présent référentiel les salariés, les agents de la fonction publique, les stagiaires, les vacataires, *etc.*, faisant partie des effectifs de l'organisme employeur.

2. Portée du référentiel

Les traitements visant à permettre la gestion du personnel, qu'ils soient mis en œuvre à partir d'outils internes ou externalisés auprès d'un prestataire de service, conduisent à collecter des données relatives à des personnes physiques (employés, salariés, stagiaires, *etc.*). A ce titre, ils sont soumis aux dispositions du règlement général sur la protection des données (RGPD), à la loi du 6 janvier 1978 modifiée (dite loi « Informatiques et Libertés » ou LIL) ainsi qu'aux dispositions spécifiques relatives aux relations de travail.

Les organismes concernés, en tant que responsables de traitement, doivent mettre en œuvre toutes les mesures techniques et organisationnelles appropriées afin de garantir un haut niveau de protection des données personnelles dès la conception des traitements et tout au long de la vie de ceux-ci. Ils doivent, en outre, être en mesure de démontrer cette conformité à tout instant. Les traitements mis en œuvre doivent être inscrits dans le registre prévu à l'article 30 du RGPD (voir les modèles de registre sur le site cnil.fr).

L'application de ce référentiel permet d'assurer la conformité des traitements de gestion courante des ressources humaines (RH) au regard des principes relatifs à la protection des données. Ces traitements sont à distinguer des traitements de gestion RH impliquant le recours à des outils innovants tels que la psychométrie ou encore les traitements algorithmiques à des fins notamment de profilage, qui ne sont pas couverts par le présent référentiel.

Le référentiel ne porte également pas sur les traitements relatifs au contrôle individuel de l'activité des salariés ainsi que sur les traitements dits « de Big Data », qui font l'objet de travaux actuellement menés au sein de la Commission nationale de l'informatique et des libertés (CNIL) et feront l'objet d'une communication distincte.

Les employeurs s'écartant de ces principes au regard des conditions particulières tenant à leur situation doivent être en mesure de justifier l'existence d'un tel besoin et prendre toutes les mesures appropriées de manière à garantir la conformité de leurs traitements à la réglementation en matière de la protection des données à caractère personnel.

Ce référentiel constitue également une aide à la réalisation d'une analyse d'impact relative à la protection des données (AIPD) dans les cas où celle-ci est nécessaire. Les organismes pourront ainsi définir les mesures permettant d'assurer la proportionnalité et la nécessité de leur traitements (points 3 à 7), de garantir les droits des personnes (points 8 et 9) et la maîtrise de leurs risques (point 10). À cette fin, l'organisme pourra se référer aux lignes directrices de la CNIL sur les analyses d'impact relatives à la protection des données (AIPD).

3. Objectif(s) poursuivi(s) par le traitement (finalités)

Un traitement de gestion du personnel peut être mis en œuvre pour les finalités suivantes :

a) **recrutement sans recours à des outils innovants** ;

b) **gestion administrative des personnels** ;

c) **gestion des rémunérations et accomplissement des formalités administratives y afférentes** ;

d) **mise à disposition du personnel d'outils informatiques** ;

e) **organisation du travail** ;

f) **suivi des carrières et de la mobilité** ;

g) **formation ;**

h) **gestion des aides sociales.**

Les informations recueillies pour l'une de ces finalités ne peuvent pas être réutilisées pour poursuivre un autre objectif qui serait incompatible avec la finalité initiale. Tout nouvel usage des données doit en effet respecter les principes de protection des données personnelles. Les traitements mis en œuvre ne doivent pas donner lieu à des interconnexions ou échanges autres que ceux nécessaires à l'accomplissement des finalités ci-dessus énoncées

4. Bases légales du traitement

Chaque finalité du traitement doit reposer sur l'une des « bases légales » fixées par la réglementation. Les différents fondements autorisant un organisme à traiter des données personnelles, applicables aux traitements de gestion du personnel, sont listés ci-dessous.

a) **le consentement libre, spécifique, éclairé et univoque de la personne concernée ;**

Il convient de noter que dans le cadre de la très large majorité des traitements mis en œuvre dans la sphère travail, le consentement du salarié ne peut servir de base légale aux traitements mis en œuvre : il n'est en effet pas considéré comme librement donné en raison du « *déséquilibre manifeste* » entre les parties (voir considérant 43 du RGPD) résultant du lien de subordination existant entre le salarié et l'employeur.

Le consentement, pour être valable, requiert une action positive et spécifique de la personne concernée (par exemple : une case à cocher dédiée, non pré-cochée). A cet égard, l'acceptation de conditions générales d'utilisation ne peut suffire : l'accord doit être libre, non influencé ou contraint (il ne peut conditionner la souscription à un service ou l'achat d'un bien, la création d'un compte en ligne pour accéder à un service, *etc.*), ni ne doit entrainer de conséquences négatives pour la personne en cas de refus.

b) **l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à sa demande** ;

c) **le respect d'une obligation légale incombant à l'organisme,** imposant la mise en œuvre d'un traitement entrant dans le cadre de la gestion du personnel ;

d) **l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement** ;

e) **la réalisation de l'intérêt légitime poursuivi par l'organisme ou par le destinataire des données, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.**

La base légale doit être portée à la connaissance des personnes dont les données sont traitées puisqu'elle permet, notamment, de déterminer les droits qu'elles peuvent exercer.

5. Données personnelles concernées

Dans un souci de minimisation des données personnelles traitées, l'organisme doit veiller à ne collecter et n'utiliser que les données pertinentes et nécessaires au regard de ses propres besoins de gestion du personnel. Il peut s'agir des données relatives :

a) **à l'identification de l'employé** ;

b) **à l'évaluation des compétences du candidat au moment du recrutement ;**

c) **au suivi de carrière et de la formation de l'employé** ;

d) **à l'établissement de la fiche de paie et aux obligations légales connexes** (notamment, dans le cadre du prélèvement à la source, le taux d'imposition) ;

e) **à la validation des acquis de l'expérience** ;

f) **à la gestion des déclarations d'accident du travail et de maladie professionnelle, à la gestion des arrêts de travail et autres cas d'absences autorisées et au suivi des visites médicales de l'employé** ;

g) **aux sujétions particulières ouvrant droit à congés spéciaux ou à un crédit d'heures de délégation** ;

h) **aux outils et matériel mis à la disposition de l'employé dans le cadre de ses missions professionnelles** ;

i) **à la gestion des activités sociales et culturelles mises en œuvre par l'employeur** ;

j) **aux élections professionnelles et réunions des instances représentatives du personnel**.

Certaines données, en raison de leur caractère particulièrement sensible, bénéficient d'une protection particulière et ne peuvent être traitées que dans des cas spécifiques.

Il s'agit notamment de :

- données sensibles, c'est-à-dire celles dont le traitement est par principe interdit sauf à pouvoir se prévaloir d'une des exceptions limitativement énumérées. Il s'agit des données qui révèlent l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne, des données génétiques, des données biométriques utilisées 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 (article 9.1 RGPD) ;
- le numéro de sécurité sociale (NIR) ;
- les données relatives aux infractions, condamnations pénales et mesures de sûreté connexes concernant des personnes physiques.

Ces données ne peuvent être collectées et traitées que dans des conditions strictement définies par les textes.

Exemple : lorsqu'un salarié est victime d'un accident du travail, il doit en informer l'employeur qui est tenu de le déclarer à l'organisme d'assurance maladie compétent.

Dans la déclaration d'accident du travail, l'employeur doit notamment indiquer la nature et le siège des lésions de la victime. Or, ces données sont relatives à l'état de santé de l'employeur et constituent de ce fait des données sensibles, dont le traitement est soumis au respect des dispositions de l'article 9 du RGPD. En l'espèce, l'employeur est autorisé à collecter ces données sensibles en application de l'article 9-2-b).

Un tableau, ci-après, cite les données pouvant être collectées et traitées selon les finalités du traitement.

Après s'être assuré de la nécessité et de la pertinence des données personnelles qu'il traite, l'organisme doit par ailleurs s'assurer, tout au long de la durée de vie du traitement, de la qualité de ces données qui doivent être exactes et mises à jour.

6. Destinataires des informations

Les données personnelles doivent uniquement être rendues accessibles aux personnes habilitées à en connaitre au regard de leurs attributions.

Les habilitations d'accès doivent être documentées par les organismes, et les accès aux différents traitements doivent faire l'objet de mesures de traçabilité. **Voir point 9 relatif à la sécurité.**
Le responsable de traitement qui souhaite avoir recours à un sous-traitant doit veiller à ne faire appel qu'à des organismes présentant des garanties suffisantes. Un contrat définissant les caractéristiques du traitement ainsi que les différentes obligations des parties en matière de protection des données doit être établi entre elles (article 28 du RGPD). Un guide du sous-traitant, édité par la CNIL, précise ces obligations et les clauses à intégrer dans les contrats.

6.1. Les personnes accédant aux données pour le compte de l'employeur

Seules les personnes habilitées au titre de leurs missions ou de leurs fonctions, doivent pouvoir accéder aux données à caractère personnel traitées, et ce, dans la stricte limite de leurs attributions respectives et de l'accomplissement de ces missions et fonctions. Il peut s'agir, par exemple :

- des personnes habilitées chargées de la gestion du personnel ou de la gestion de la paie ;
- des personnes habilitées chargées d'assurer la sécurité des personnes et des biens, pour les besoins du contrôle d'accès aux locaux et aux outils de travail ;
- des supérieurs hiérarchiques des employés concernés, à l'exclusion des données relatives à l'action sociale directement mise en œuvre par l'employeur.

6.2. Les destinataires des données

Le RGPD définit les destinataires comme « *tout organisme qui reçoit la communication des données* ». Dans le domaine RH, peuvent notamment être destinataires des données :

- les instances représentatives du personnel, s'agissant des coordonnées professionnelles des employés après accord formalisé avec l'employeur et recueil de l'accord exprès des intéressés, et des données strictement nécessaires à la défense des intérêts des employés ;

- des organismes gérant les différents systèmes d'assurances sociales, d'assurances chômage, de retraite et de prévoyance, les caisses de congés payés, les organismes publics et administrations légalement habilités à les recevoir ;
- des personnes des services chargés du contrôle financier dans l'entreprise et des organismes financiers intervenant dans la gestion des comptes de l'entreprise et du salarié ;
- des organismes habilités à recevoir des informations statistiques relatives à la paie.

Pour assurer la continuité de la protection des données à caractère personnel, les transferts de ces dernières en dehors de l'Union européenne sont soumis à des règles particulières. Ainsi, conformément aux dispositions des articles 44 et suivants du RGPD, toute transmission de données hors de l'UE doit:

- soit être fondée sur une décision d'adéquation ;
- soit être encadrée par des règles internes d'entreprise, des clauses types de protection des données, un code de conduite ou un mécanisme de certification approuvé par la CNIL ;
- soit être encadrée par des clauses contractuelles *ad hoc* préalablement autorisées par la CNIL ;
- soit répondre à l'une des dérogations prévues à l'article 49 du RGPD.

Pour en savoir plus, consulter la rubrique qui s'intitule « Transférer des données hors de l'UE » sur le site de la CNIL.

7. Durées de conservation

Une durée de conservation précise des données doit être fixée en fonction de chaque finalité : ces données ne peuvent être conservées pour une durée indéfinie.

Les données nécessaires au recrutement sont conservées pendant deux ans à compter du dernier contact avec le candidat non retenu.

Les données nécessaires à la gestion du personnel sont conservées, par principe, pendant la durée de la relation de travail, sauf disposition légale ou réglementaire contraire.

Elles peuvent également être conservées après l'exécution du contrat, en archivage intermédiaire, si le responsable du traitement en a l'obligation légale (par exemple, pour répondre à des obligations comptables, sociales ou fiscales) ou s'il souhaite se constituer une preuve en cas de contentieux et dans la limite du délai de prescription/forclusion applicable.

Exemple : les données nécessaires à l'établissement de la déclaration sociale nominative (DSN) d'un employé doivent pouvoir être conservées pendant toute la durée de travail, dans la mesure où l'employeur est obligé de procéder à une telle déclaration chaque mois. Une fois le contrat terminé, l'employeur peut conserver ces éléments à des fins probatoires pour pouvoir justifier de ses diligences en cas de contrôle de l'URSSAF ou de contentieux éventuels. Cette durée devra correspondre à celle de la prescription en la matière.

Pour en savoir plus, vous pouvez vous référer aux guides de la CNIL :
- « Sécurité : Archiver de manière sécurisée » ;
- « Limiter la conservation des données ».

Les données utilisées à des fins statistiques ne sont plus qualifiées de données à caractère personnel dès lors qu'elles auront ont été dûment anonymisées (Voir les lignes directrices du CEPD sur l'anonymisation).

8. Information des personnes

Un traitement de données personnelles doit être mis en œuvre en toute transparence vis-à-vis des personnes concernées.

Dans le cadre des traitements RH, au regard des dispositions de la législation sociale, une information individuelle et collective doit être délivrée préalablement à la mise en œuvre d'un traitement de données personnelles.

Ainsi, dès le stade de la collecte des données personnelles, les personnes concernées doivent être informées des modalités de traitement de leurs données ainsi que de la manière d'exercer leurs droits conformément aux dispositions des articles 12, 13 et 14 du RGPD.

Voir les modèles de mention d'information.

Les instances représentatives du personnel doivent par ailleurs être informées et consultées dans le cadre prévu par le code du travail.

9. Droits des personnes

Les personnes concernées disposent des droits suivants, qu'ils exercent dans les conditions prévues par le RGPD (voir la rubrique qui s'intitule « respecter les droits des personnes » sur le site de la CNIL) :

- droit de **s'opposer au traitemen**t de leurs données, sous réserve qu'il soit prévu en application des dispositions de l'article 21 du RGPD.
  Aussi, en ce qui concerne les traitements RH :
  - Il n'y aura pas de droit d'opposition lorsque le traitement répond à une obligation légale, est nécessaire à l'exécution d'un contrat ou plus rarement est fondé sur le consentement du salarié.
  - En revanche, le droit d'opposition pourra être exercé pour des motifs légitimes lorsque le traitement est mis en œuvre sur la base de l'intérêt légitime du responsable de traitement, ou pour l'exécution d'une mission d'intérêt public ou d'une mission relevant de l'exercice de l'autorité publique.

- droit **d'accès, de rectification et, dans des conditions particulières, d'effacement** (renvoyer au site) des données qui les concernent ;

- droit à la **limitation** du traitement (par exemple, lorsque la personne conteste l'exactitude de ses données, celle-ci peut demander à l'organisme le gel temporaire du traitement de ses données, le temps que celui-ci procède aux vérifications nécessaires) ;

- droit à la **portabilité** : l'organisme doit permettre à toute personne de recevoir, dans un format structuré et couramment utilisé, l'ensemble des données traitées par des moyens automatisés. La personne concernée peut demander à ce que ses données soient directement transmises par l'organisme initial à un autre organisme.
  Ne sont concernées, que les données fournies par la personne sur la base de son consentement ou d'un contrat. Il est donc recommandé de préciser aux personnes les traitements concernés par ce droit à la portabilité.

Par exemple : un salarié pourra le cas échéant demander à récupérer les données qu'il a fournies dans le cadre de l'embauche (données d'identification, données relatives à la protection sociale, à sa formation professionnelle, *etc.*), voire à demander la transmission directe de ces informations à son futur employeur.

10. Sécurité

L'organisme doit prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des données à caractère personnel et, notamment au moment de leur collecte, durant leur transmission et leur conservation, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

En particulier, dans le contexte spécifique du présent référentiel, **soit l'organisme adopte les mesures suivantes, soit il justifie de leur équivalence ou du fait de ne pas avoir besoin ou pouvoir y recourir** :

Catégories	Mesures
Sensibiliser les utilisateurs	Informer et sensibiliser les personnes manipulant les données
	Rédiger une charte informatique et lui donner une force contraignante
Authentifier les utilisateurs	Définir un identifiant (login) unique à chaque utilisateur
	Adopter une politique de mot de passe utilisateur conforme aux recommandations de la CNIL
	Obliger l'utilisateur à changer son mot de passe après réinitialisation
	Limiter le nombre de tentatives d'accès à un compte
Gérer les habilitations	Définir des profils d'habilitation
	Supprimer les permissions d'accès obsolètes
	Réaliser une revue annuelle des habilitations
Tracer les accès et gérer les incidents	Prévoir un système de journalisation
	Informer les utilisateurs de la mise en place du système de journalisation
	Protéger les équipements de journalisation et les informations journalisées
	Prévoir les procédures pour les notifications de violation de données à caractère personnel
Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session
	Utiliser des antivirus régulièrement mis à jour
	Installer un « pare-feu » (firewall) logiciel
	Recueillir l'accord de l'utilisateur avant toute intervention sur son poste
Sécuriser l'informatique mobile	Prévoir des moyens de chiffrement des équipements mobiles
	Faire des sauvegardes ou des synchronisations régulières des données
	Exiger un secret pour le déverrouillage des smartphones
Protéger le réseau informatique interne	Limiter les flux réseau au strict nécessaire
	Sécuriser les accès distants des appareils informatiques nomades par VPN
	Mettre en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
	Installer sans délai les mises à jour critiques

Catégories	Mesures
	Assurer une disponibilité des données
Sécuriser les sites web	Utiliser le protocole TLS et vérifiez sa mise en œuvre
	Vérifier qu'aucun mot de passe ou identifiant ne passe dans les url
	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	Mettre un bandeau de consentement pour les cookies non nécessaires au service
Sauvegarder et prévoir la continuité d'activité	Effectuer des sauvegardes régulières
	Stocker les supports de sauvegarde dans un endroit sûr
	Prévoir des moyens de sécurité pour le convoyage des sauvegardes
	Prévoir et tester régulièrement la continuité d'activité
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées
	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans une main courante
	Encadrer par un responsable de l'organisme les interventions par des tiers
	Effacer les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	Prévoir une clause spécifique dans les contrats des sous-traitants
	Prévoir les conditions de restitution et de destruction des données
	S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)
Sécuriser les échanges avec d'autres organismes	Chiffrer les données avant leur envoi
	S'assurer qu'il s'agit du bon destinataire
	Transmettre le secret lors d'un envoi distinct et via un canal différent
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées
	Installer des alarmes anti-intrusion et les vérifier périodiquement
Encadrer les développements informatiques	Proposer des paramètres respectueux de la vie privée aux utilisateurs finaux
	Éviter les zones de commentaires ou les encadrer strictement
	Tester sur des données fictives ou anonymisées
Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues
	Conserver les secrets et les clés cryptographiques de manière sécurisée

Pour ce faire, le responsable de traitement pourra utilement se référer au Guide de la sécurité des données personnelles.

11. Analyse d'impact sur la protection des données (AIPD)

En application des dispositions de l'article 35 du RGPD, **le responsable de traitement pourrait avoir à réaliser une analyse d'impact** dès lors que son traitement de gestion RH présenterait un risque élevé pour les droits et les libertés des personnes.

Pour l'appréciation de ces risques, il conviendra de se référer aux critères établis par le Comité européen de la protection des données (CEPD) dans les lignes directrices concernant l'analyse d'impact relative à la protection

des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé », ainsi qu'à la liste adoptée par la CNIL, des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

Pour réaliser une étude d'impact, le responsable de traitement pourra se reporter :

- aux principes contenus dans ce référentiel ;
- aux outils méthodologiques proposés par la CNIL sur son site web.

Si l'organisme en a désigné, le délégué à la protection des données (DPO) devra être consulté.

Conformément à l'article 36 du RGPD, le responsable de traitement doit consulter la CNIL préalablement à la mise en œuvre du traitement si l'analyse d'impact indique qu'il ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable.

Tableau 1. Illustration pratique des finalités et des bases légales

Ce tableau mentionnant les objectifs et les finalités poursuivis par les traitements RH ainsi que les bases légales envisageables, a vocation à être complété par les bases légales applicables, à la suite des travaux du groupe de travail portant sur l'identification des bases légales.

Activités de traitement	Finalités	Bases légales envisageables (à discuter)
Recrutement	Gestion du recrutement	- Exécution du contrat (mesures précontractuelles) - Intérêt légitime
	Constitution d'une CV-thèque	- Consentement - Intérêt légitime
Gestion administrative du personnel	Gestion du dossier professionnel des employés, tenu conformément aux dispositions législatives et réglementaires, ainsi qu'aux dispositions statutaires, conventionnelles ou contractuelles qui régissent les intéressés.	- Exécution du contrat - Intérêt légitime.
	Réalisation d'états statistiques ou de listes d'employés pour répondre à des besoins de gestion administrative.	- Intérêt légitime
	Gestion des annuaires internes et des organigrammes.	- Intérêt légitime
	Gestion des dotations individuelles en fournitures, équipements, véhicules et cartes de paiement.	- Exécution du contrat
	Gestion des élections professionnelles.	- Obligation légale

	Gestion des réunions des instances représentatives du personnel.	- Intérêt légitime - Obligation légale
Gestion des rémunérations et accomplissement des formalités administratives y afférentes	Etablissement des rémunérations, mise à disposition des bulletins de salaire, déclaration sociale nominative.	- Obligation légale - Exécution du contrat
Mise à disposition des personnels d'outils informatiques	Suivi et maintenance du parc informatique.	- Intérêt légitime
	Gestion des annuaires informatiques permettant de définir les autorisations d'accès aux applications et aux réseaux.	- Intérêt légitime
	Mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux.	- Intérêt légitime
	Gestion de la messagerie électronique professionnelle.	- Intérêt légitime
	Réseaux privés virtuels internes à l'organisme permettant la diffusion ou la collecte de données de gestion administrative des personnels (intranet).	-- Exécution du contrat (mesures précontractuelles) - Intérêt légitime
Organisation du travail	Gestion des agendas professionnels.	- Exécution du contrat
	Gestion des tâches des personnels.	- Exécution du contrat (mesures précontractuelles) - Intérêt légitime
Suivi des carrières et de la mobilité	Evaluation professionnelle des personnels, dans le respect des dispositions législatives, réglementaires ou conventionnelles qui la régissent.	- Intérêt légitime - Exécution d'un contrat
	Gestion des compétences professionnelles internes.	- Intérêt légitime
	Validation des acquis de l'expérience professionnelle.	- Obligation légale
	Simulation de carrière.	- Intérêt légitime
	Gestion de la mobilité professionnelle.	- Exécution du contrat (mesures précontractuelles) - Intérêt légitime
Formation	Suivi des demandes de formation et des périodes de formation effectuées.	- Exécution du contrat (mesures précontractuelles) - Intérêt légitime
	Organisation des sessions de formation.	- Exécution du contrat (mesures précontractuelles) - Intérêt légitime
	Evaluation des connaissances et des formations.	- Exécution du contrat

		(mesures précontractuelles) - Intérêt légitime
Gestion des aides sociales	Gestion de l'action sociale et culturelle directement mise en œuvre par l'employeur, à l'exclusion des activités de médecine du travail, de service social ou de soutien psychologique.	- Intérêt légitime

Tableau 2. Exemple de données pouvant être collectées et traitées selon les finalités du traitement

Catégories de données	Exemples de données
Identification de l'employé	**Données relatives à l'identité** : nom, prénom, photographie (facultatif), sexe, date et lieu de naissance, nationalité, coordonnées professionnelles, coordonnées personnelles (facultatif), références du passeport (uniquement pour les personnels amenés à se déplacer à l'étranger), situation familiale, situation matrimoniale, enfants à charge, type de permis de conduire détenu par l'employé.
	Données relatives à la situation professionnelle : lieu de travail, numéro d'identification interne, date d'entrée dans l'entreprise, ancienneté, emploi occupé et coefficient hiérarchique, section comptable, nature du contrat de travail, taux d'invalidité, reconnaissance de la qualité de travailleur handicapé (RQTH), autres catégories de bénéficiaires de la loi n° 87-517 du 10 juillet 1987 (invalide pensionné, mutilé de guerre, assimilé mutilé de guerre).
	Données relatives au titre valant autorisation de travail : type, numéro d'ordre et copie du titre pour les employés étrangers en application de l'article R. 620-3 du code du travail.
	Coordonnées des personnes à prévenir en cas d'urgence.
	Distinctions honorifiques.
Suivi de la carrière et de la formation de l'employé	**Gestion de la carrière de l'employé** : date et conditions d'embauche ou de recrutement, date, objet et motif des modifications apportées à la situation professionnelle de l'employé, simulation de carrière, desiderata de l'employé en termes d'emploi, sanctions disciplinaires à l'exclusion de celles consécutives à des faits amnistiés.
	Evaluation professionnelle de l'employé : dates des entretiens d'évaluation, identité de l'évaluateur, compétences professionnelles de l'employé, objectifs assignés, résultats obtenus, appréciation des aptitudes professionnelles sur la base de critères objectifs et présentant un lien direct et nécessaire avec l'emploi occupé, observations et souhaits formulés par l'employé, prévisions d'évolution de carrière.
	Formation : diplômes, certificats et attestations, langues étrangères pratiquées, suivi des demandes de formation professionnelle et des périodes de formation effectuées, organisation des sessions de formation, évaluation des connaissances et des formations.
	Suivi administratif des visites médicales des employés : dates des visites, aptitude au poste de travail (apte ou inapte, propositions

	d'adaptation du poste de travail ou d'affectation à un autre poste de travail formulées par le médecin du travail).
Etablissement des fiches de paie et obligations légales connexes	Numéro de sécurité sociale dans les conditions fixées par le décret n° 91-1404 du 27 décembre 1991 ou par l'article L. 444-5 du code du travail, numéros attribués par les organismes d'assurances sociales, de retraite et de prévoyance, situation familiale, situation matrimoniale, enfants à charge, régime et base de calcul de la rémunération, éléments déterminant l'attribution d'un complément de rémunération, congés et absences donnant lieu à retenues déductibles ou indemnisables ainsi que toute retenue légalement opérée par l'employeur, frais professionnels, taux de prélèvement à la source, données transmises via la Déclaration sociale nominative.
Validation des acquis de l'expérience	Date de la demande de validation, diplôme, titre ou certificat de qualification concerné, expériences professionnelles soumises à validation, validation (oui/non), date de la décision.
Gestion des déclarations d'accident du travail et de maladie, autres absences	Coordonnées du médecin du travail, date de l'accident ou de la première constatation médicale de la maladie, date du dernier jour de travail, date de reprise, motif de l'arrêt (accident du travail ou maladie professionnelle), travail non repris à ce jour et autres éléments nécessaires auxdites déclarations.
Sujétions particulières ouvrant droit à congés spéciaux ou à un crédit d'heures de délégation	Données relatives à l'exercice d'un mandat électif ou représentatif syndical, la participation à la réserve opérationnelle ou aux missions de sapeur-pompier volontaire.
Outils et matériel mis à la disposition de l'employé dans le cadre de ses missions professionnelles	**Annuaires internes et organigrammes** : nom, prénom, photographie (facultatif), fonction, coordonnées professionnelles, le cas échéant, formation et réalisations professionnelles.
	Agendas professionnels : dates, lieux et heures des rendez-vous professionnels, objet, personnes présentes.
	Tâches des personnels : identification des personnels concernés, répartition des tâches.
	Gestion des dotations individuelles en fournitures, équipements, véhicules et cartes de paiement : gestion des demandes, nature de la dotation, dates de dotation, de maintenance et de retrait, affectations budgétaires.
	Annuaires informatiques permettant de définir les autorisations d'accès aux applications et aux réseaux.
	Données de connexion enregistrées pour assurer la sécurité et le bon fonctionnement des applications et des réseaux informatiques, à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés.
	Messagerie électronique : carnet d'adresses, comptes individuels, à l'exclusion de toute donnée relative au contrôle individuel des communications électroniques émises ou reçues par les employés.
	Réseaux privés virtuels de diffusion ou de collecte de données de gestion administrative des personnels (intranet) : formulaires administratifs internes, organigrammes, espaces de discussion, espaces d'information.
Activités sociales	Identité de l'employé et de ses ayants droit ou ouvrants droit, revenus,

et mises en œuvre par l'employeur	avantages et prestations demandés et servis.
Elections professionnelles et réunions des instances	**Elections professionnelles** : établissement de la liste électorale (identité des électeurs, âge, ancienneté, collège), gestion des candidatures (identité, nature du mandat sollicité, éléments permettant de vérifier le respect des conditions d'éligibilité, le cas échéant appartenance syndicale déclarée par les candidats) et publication des résultats (identité des candidats, mandats concernés, nombre et pourcentage de suffrages obtenus, identité des personnels élus et, le cas échéant, appartenance syndicale des élus).
	Gestion des réunions des instances représentatives du personnel : convocations, documents préparatoires, procès-verbaux.