Commission nationale de l'informatique et des libertés

Délibération n° 2019-160 du 21 novembre 2019 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel

NOR : *CNIL2009233X*

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du parlement européen et du Conseil 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 ;

Vu le code du travail ;

Vu le code civil, notamment son article 9 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu les lois n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat, n° 84-53 du 26 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale, et n° 86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière ;

Vu le décret n° 2011-675 du 15 juin 2011 relatif au dossier individuel des agents publics et à sa gestion sur support électronique ;

Vu le décret n° 2019-536 du 29 mai 2019 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu l'arrêté du 21 décembre 2012 relatif à la composition du dossier individuel des agents publics géré sur support électronique,

Après avoir entendu M. Alexandre LINDEN, commissaire, en son rapport et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations ;

Adopte le référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel, qui sera publié au *Journal officiel* de la République française.

La présidente,
M.-L. Denis

RÉFÉRENTIEL

RÉFÉRENTIEL RELATIF AUX TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL MIS EN ŒUVRE AUX FINS DE GESTION DU PERSONNEL

Adopté le 21 novembre 2019

1. A qui s'adresse ce référentiel ?

Ce référentiel s'adresse aux **organismes privés ou publics, quelle que soit leur forme juridique, et encadre la mise en œuvre de leurs traitements courants de « gestion du personnel ».**

Pour les besoins du présent référentiel, les termes : « personnes employées », « personnels » « effectifs », « moyens humains » ou « ressources humaines », sont considérés comme synonymes et désignent l'ensemble des collaborateurs permanents ou temporaires de l'employeur, quels que soient leur statut, leur type ou durée de contrat, leur 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.

Les organismes mettant en place des traitements de gestion du personnel doivent s'assurer de sa conformité :

- aux dispositions du règlement général sur la protection des données (RGPD) ainsi qu'à celles de la loi du 6 janvier 1978 modifiée (LIL) ;
- à l'ensemble des autres règles applicables telles que la législation du travail, les textes régissant la fonction publique, les conventions collectives, etc.

2. **Portée du référentiel**

Ce référentiel a pour objectif de fournir aux organismes publics et privés mettant en œuvre des traitements de gestion courante des ressources humaines (RH), un outil d'aide à la mise en conformité à la réglementation relative à la protection des données à caractère personnel.

Il couvre les traitements mis en place couramment par les organismes-employeurs dans le cadre de la gestion de leur personnel.

Il n'a dès lors pas vocation à s'appliquer aux traitements mis en œuvre notamment par les organisations syndicales, les instances représentatives du personnel, ou encore les services de médecine de travail.

En raison de leur sensibilité, ce référentiel n'a pas vocation à encadrer :

– les traitements de gestion RH impliquant le recours à des outils innovants tels que la psychométrie (i.e. les techniques de quantifications des aspects de personnalité), les traitements algorithmiques à des fins notamment de profilage, ou encore les traitements dits de « *Big Data* », qui seront traités à part ;
– les traitements ayant pour objet ou pour effet le contrôle individuel de l'activité des salariés.

Le respect de ce référentiel permet aux organismes de s'assurer de la conformité des traitements de données mis en œuvre dans ce cadre aux principes relatifs à la protection des données.

Les organismes qui s'écarteraient du référentiel au regard des conditions particulières tenant à leur situation doivent être en mesure de justifier l'existence d'un tel besoin, puis prendre toutes les mesures appropriées à même de garantir la conformité des traitements à la réglementation en matière de protection des données à caractère personnel.

Le référentiel n'a pas pour objet d'interpréter les règles de droit autres que celles relatives à la protection des données à caractère personnel. Il appartient aux acteurs concernés de s'assurer qu'ils respectent les autres réglementations qui peuvent par ailleurs trouver à s'appliquer.

Ce référentiel constitue également une aide à la réalisation d'une analyse d'impact relative à la protection des données (AIPD), dans le cas où celle-ci est nécessaire.

Pour réaliser une étude d'impact, le responsable de traitement pourra également se reporter aux outils méthodologiques proposés par la CNIL sur son site web. Les organismes seront ainsi à même de définir les mesures permettant d'assurer la proportionnalité et la nécessité de leurs traitements (points 3 à 7), de garantir les droits des personnes (points 8 et 9) et la maîtrise de leurs risques (point 10). A cette fin, l'organisme s'appuiera sur les lignes directrices de la CNIL sur les AIPD. Si l'organisme en a désigné un, le délégué à la protection des données (DPD/DPO) devra être consulté.

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

Le traitement mis en œuvre doit répondre à un objectif précis et être justifié au regard des missions et des activités de l'organisme.

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

a) Recrutement ;
b) Gestion administrative des personnels ;
c) Gestion des rémunérations et accomplissement des formalités administratives afférentes ;
d) Mise à disposition du personnel d'outils professionnels ;
e) Organisation du travail ;
f) Suivi des carrières et de la mobilité ;
g) Formation ;
h) Tenue des registres obligatoires, rapports avec les instances représentatives du personnel ;
i) Communication interne ;
j) Gestion des aides sociales ;
k) Réalisation des audits, gestion du contentieux et du précontentieux.

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. **Base(s) légale(s) du traitement**

Lorsqu'un traitement poursuit plusieurs finalités, le responsable du traitement doit déterminer la base légale la plus appropriée pour chacune d'elles (art. 6.1 du RGPD).

Il appartient au responsable de traitement de déterminer ces bases légales avant toute opération de traitement, après avoir mené une réflexion, qu'il pourra documenter, au regard de sa situation spécifique et du contexte.

Ayant un impact sur l'exercice de certains droits, ces bases légales font partie des informations devant être portées à la connaissance des personnes concernées.

Afin d'aider les organismes dans cette analyse, le présent référentiel présente les différentes bases légales applicables, puis propose, à titre indicatif, un choix de base légale pour chaque finalité dans un tableau.

Aussi, les bases légales les plus fréquemment mobilisables dans le contexte de gestion des ressources humaines, sont :

– **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 (par ex. les obligations liées à la déclaration sociale nominative (DSN) ou encore à la tenue d'un registre unique du personnel) ;
– **l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à sa demande.**

A noter : un contrat conclu entre l'employeur et un tiers (par ex. un client ou un prestataire) ne peut pas en tant que tel constituer la base légale d'un traitement de données d'une personne qui n'y est pas elle-même partie.

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

Dans certains cas exceptionnels, les bases légales suivantes peuvent également être invoquées dans le contexte RH :

– **le consentement libre, spécifique, éclairé et univoque de la personne concernée.**

A noter : les employés ne sont que très rarement en mesure de donner, de refuser ou de révoquer librement leur consentement, étant donné la dépendance qui découle de la relation employeur/employé. Ils ne peuvent donner leur libre consentement que dans le cas où l'acceptation ou le rejet d'une proposition n'entraine aucune conséquence sur leur situation.

Exemples : les traitements effectués dans le cadre des opérations de recrutement ne peuvent pas être fondés sur le consentement des candidats, dès lors qu'un refus de leur part pourrait affecter leurs chances d'obtenir un emploi (ou certains types d'emplois).

A l'inverse, l'enregistrement d'un clip promotionnel dans un espace de travail faisant apparaitre des employés identifiables, peut être fondée sur leur consentement dès lors que les personnes concernées bénéficient d'un choix d'apparaitre ou non dans ces enregistrements, et à condition que le choix réalisé n'ait aucun impact à leur égard (notamment à l'égard des conditions de travail, de rémunération, d'avancement, etc.).

Pour une étude d'ensemble des différentes bases légales, voir l'avis de l'ex-G29, devenu Comité Européen de la Protection de Données (CEPD) nº 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE.

Le tableau reproduit ci-dessous vise à apporter aux responsables de traitement des éléments concrets relatifs à l'identification de bases légales susceptibles d'être utilisées dans les cas les plus courants.

Bien entendu, ces éléments doivent être adoptés à la situation spécifique de chaque organisme concerné. Ainsi, par exemple, selon que l'organisme en question relève du secteur privé ou public, certains traitements répondant pourtant à la même finalité (par exemple, ceux liés au recrutement du personnel) peuvent être fondés sur des bases légales différentes (intérêt légitime dans le secteur privé, exécution d'une mission d'intérêt public dans le secteur public).

Pour plus de conseils sur la méthode à suivre, vous pouvez également reporter à l'article « La licéité du traitement : l'essentiel sur les bases légales prévues par le RGPD », publié sur le site de la CNIL.

Activités de traitement	Finalités	Bases légales envisageables (sous réserve de choix différents justifiés par un contexte spécifique)
Recrutement	Traitement des candidatures (CV et lettre de motivation) et gestion des entretiens	- Mesures précontractuelles
	Constitution d'une CV-thèque	- 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
	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.	- Intérêt légitime
	Gestion des élections professionnelles.	- Obligation légale
	Organisation des réunions des instances représentatives du personnel.	- Obligation légale

Activités de traitement	Finalités	Bases légales envisageables (sous réserve de choix différents justifiés par un contexte spécifique)
Gestion des rémunérations et accomplissement des formalités administratives	Etablissement des rémunérations, mise à disposition des bulletins de salaire	- Exécution du contrat
	Déclaration sociale nominative.	- Obligation légale
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).	- Intérêt légitime
Organisation du travail	Gestion des agendas et projets professionnels.	- 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
	Gestion des compétences professionnelles internes.	- Intérêt légitime
	Gestion prévisionnelle de l'emploi et des compétences (GPEC)	- Intérêt légitime
	Gestion de la mobilité professionnelle.	- Exécution du contrat
Formation	Gestion des demandes de formation et des périodes de formation effectuées.	- Exécution du contrat
	Organisation des sessions de formation et évaluation des connaissances et des formations.	- 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

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 strictement nécessaires au regard de ses propres besoins de gestion du personnel. Il peut s'agir de données relatives :

a) A l'identification de l'employé ;

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

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

d) A 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) A la validation des acquis de l'expérience ;

f) A 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 ou situations particulières ouvrant droit à congés spéciaux ou à un crédit d'heures de délégation ;

h) Aux outils et matériels professionnels mis à la disposition de l'employé dans le cadre de ses missions (*i.e.* cartes de paiement, dotation en matériel informatique, etc.) ;

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

j) Aux élections professionnelles et réunions des instances représentatives du personnel ;

k) A la lutte contre la discrimination, à l'obligation d'emploi résultant des articles L. 5212-2 et suivants du code du travail, etc.

De manière générale, l'employeur ne doit collecter que les données dont il a réellement besoin, et ne doit le faire qu'à partir du moment où ce besoin se concrétise.

Exemple 1 : lors de la conclusion d'un contrat de travail, l'employeur a l'obligation d'accomplir certaines formalités déclaratives qui requièrent le traitement du numéro de sécurité sociale (NIR) des salariés. Si cette utilisation est alors justifiée, elle ne saurait être demandée à un candidat avant la validation définitive de sa candidature.
Exemple 2 : les informations pouvant être demandées à un candidat à l'embauche, doivent présenter un lien direct avec l'appréciation de ses qualités et compétences professionnelles, et ne doivent donc pas porter sur la composition de sa famille, sur des informations relatives à ses proches, etc. En revanche, lorsqu'un salarié en poste demande à bénéficier d'un congé spécifique pour le décès ou l'accompagnement de grave maladie d'un proche, l'employeur peut exiger la production de documents établissant la réalité des situations invoquées.

Attention : Les données, dont le traitement est justifié pour une finalité déterminée, ne peuvent être réutilisées à d'autres fins que si cette utilisation est elle-même légalement justifiée.

Par ailleurs, certaines catégories de données appellent une vigilance renforcée en raison de leur caractère particulièrement sensible. Bénéficiant d'une protection particulière, elles ne peuvent être collectées et traitées que dans des conditions strictement définies par les textes.

Il s'agit notamment :

– **du numéro de sécurité sociale ;**
– **des données relatives aux infractions, condamnations pénales et mesures de sûreté connexes.**

Exemple : à la suite d'un accident du travail concernant l'un de ses salariés, l'employeur remplit une déclaration d'accident du travail dans laquelle il doit indiquer la nature et le siège des lésions de la victime. Or, ces données sont relatives à l'état de santé de l'employé et constituent de ce fait des données sensibles. Leur traitement est donc en principe interdit en vertu de l'article 9.1 du RGPD.
Toutefois, l'employeur bénéficie d'une exception pour les traiter sur le fondement de l'article 9-2-b) du RGPD (« *le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale* [...]).

Dans certains cas très limités :

– **des données sensibles** (article 9 du RGPD, articles 6 et 44 de la LIL), c'est-à-dire celles qui révèlent l'origine ethnique ou prétendument raciale, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne, les données génétiques, les données biométriques, les données concernant la santé ou celles concernant la vie sexuelle ou l'orientation sexuelle d'une personne.

Un tableau reproduit ci-dessous recense des 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 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° 2019-341 du 19 avril 2019 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

Catégories de données	Exemples de données
	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 et mises en œuvre par l'employeur	Identité de l'employé et de ses ayants droit ou ouvrants droit, revenus, avantages et prestations demandés et servis.
Relations avec les instances représentatives de personnel	Convocations, documents préparatoires, comptes rendus, procès-verbaux divers.

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 données**

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 (cf. point 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 cadre de ce référentiel, peuvent **notamment** être destinataires des données :

– les instances représentatives du personnel, pour les données strictement nécessaires à leurs missions dans les conditions fixées par les textes applicables ;
– les 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 ;
– les entités chargées de l'audit et du contrôle financier de l'organisme employeur ;
– les différents prestataires auxquels l'organisme employeur est susceptible de sous-traiter la gestion de certaines activités (restauration collective, vote électronique, archivage des documents, tenue des comptes d'épargne, etc.) ;
– les entités en charge de l'action culturelle et sociale telles que les comités sociaux et économiques (CSE), à condition que le bénéficiaire en ait fait la demande.

Pour assurer la continuité de la protection des données à caractère personnel, leur transfert en dehors de l'Union européenne est 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 :

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

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

7. **Durées de conservation**

Conformément à l'article 5-1-*e* du RGPD, les données à caractère personnel ne doivent être conservées sous une forme permettant l'identification des personnes que le temps strictement nécessaire à la réalisation des finalités poursuivies. C'est donc au regard de la finalité que la durée de conservation sera déterminée.

La durée de conservation de données ou, lorsqu'il est impossible de la fixer, les critères utilisés pour déterminer cette durée, font partie des informations qui doivent être communiquées aux personnes concernées.

Dans ces conditions, il incombe au responsable du traitement de déterminer cette durée en amont de la réalisation du traitement.

Par exemple, de nombreuses données nécessaires à la gestion de la relation contractuelle (contrat de travail) doivent être conservées pendant la durée de la relation de travail, sauf disposition légale ou réglementaire contraire.

Cela ne fait toutefois pas obstacle à leur conservation sous forme d'archives intermédiaires distinctes de la base active, avec accès restreint, dans la mesure où il existerait des dispositions législatives ou réglementaires spécifiques (par exemple, pour répondre à des obligations comptables, sociales ou fiscales, ou encore si ces données présenteraient un intérêt en cas de contentieux, justifiant de les conserver le temps des règles de prescription/forclusion applicables.

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).

Le tableau suivant contient des illustrations pratiques des durées de conservation pouvant, selon le contexte, être retenues par les organismes concernés :

Activités de traitement	Détails du traitement	Base active	Archivage intermédiaire	Textes de référence
Gestion de la paie	Bulletin de salaire	1 mois	5 ans	L. 3243-4 du code du travail
			50 ans en version dématérialisée	D. 3243-8 du code du travail
	Eléments nécessaires au calcul de l'assiette	1 mois	6 ans	L. 243-16 du code sécurité sociale
	Saisie des données calculées (DSN)	Le temps nécessaire à l'accomplissement de la déclaration	6 ans	L. 243-16 du code sécurité sociale
	Ordre de virement pour paiement	Le temps nécessaire à l'émission du bulletin de paie	10 ans à compter de la clôture de l'exercice comptable	L. 123-22 du code du commerce

Activités de traitement	Détails du traitement	Base active	Archivage intermédiaire	Textes de référence
Registre unique du personnel		La durée pendant laquelle le salarié fait partie des effectifs	5 ans à compter du départ du salarié de l'organisme	R. 1221-26 du code du travail
Gestion des mandats des représentants du personnel	Nature du mandat et syndicat d'appartenance	6 mois après la fin du mandat	6 ans (prescription pénale pour délit)	L. 2411-5 du code du travail
Gestion des mandats des représentants du personnel	Les données relatives aux sujétions particulières ouvrant droit à congés spéciaux ou à crédit d'heures de délégation (ex : exercice d'un mandat électif ou représentatif syndical)	Le temps de la période de sujétion de l'employé concerné	6 ans (prescription pénale pour délit)	L. 2142-1-3 du code du travail

8. **Information des personnes**

Il incombe au responsable de traitement de s'assurer du respect des principes de transparence et de loyauté à l'égard des personnes dont les données peuvent être traitées dans les conditions prévues par les articles 12, 13 et 14 du RGPD.

Ainsi, dès le stade de la collecte des données personnelles, les personnes concernées doivent être informées de **l'existence du traitement, de ses caractéristiques et des droits dont elles disposent** en vertu de la réglementation applicable en matière de protection des données à caractère personnel.

Des modèles d'information sont disponibles sur le site de la CNIL et peuvent être consultés dans la rubrique « RGPD : exemples de mentions d'information ».

Si le RGPD n'impose aucune forme spécifique, une information écrite doit être privilégiée de manière à pouvoir justifier de son contenu, ainsi que du moment où elle a été délivrée.

Par ailleurs dans le cadre d'une relation de travail, le responsable de traitement doit aussi veiller à respecter ses autres obligations de transparence issues de la législation sociale à laquelle il est soumis.

Le code du travail impose ainsi aux employeurs d'informer individuellement leurs salariés dans certaines situations.

De la même manière, il appartient aux responsables de traitement de s'assurer, au regard de la réglementation qui leur est applicable, du respect de l'éventuelle obligation d'informer et/ou de consulter les instances représentatives du personnel compétentes.

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 « Comprendre mes droits » sur le site de la CNIL) :

– le **droit de s'opposer au traitement** de leurs données, sous réserve qu'il soit prévu en application des dispositions de l'article 21 du RGPD.

En ce qui concerne les traitements de gestion du personnel :

– le droit d'opposition n'existe pas lorsque le traitement répond à une obligation légale, s'il est nécessaire à l'exécution d'un contrat ou est, exceptionnellement, fondé sur le consentement du salarié (dans la mesure où, dans ce dernier cas la personne concernée pourra retirer le consentement au traitement de ses données) ;
– en revanche, le droit d'opposition pourra être exercé, à charge pour la personne d'invoquer des raisons tenant à sa situation particulière, 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 ;
– le **droit d'accès, de rectification** et, dans des conditions particulières, **d'effacement** des données qui les concernent ;
– le **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) ;
– le **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.

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
	Assurer une disponibilité des données
Sécuriser les sites web	Utiliser le protocole TLS et vérifier 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

Catégories	Mesures
	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	Les relations avec les prestataires qui traitent des données au nom et pour le compte du responsable de traitement (l'organisme employeur) doivent faire l'objet d'un accord écrit. Cet accord doit contenir une ou des clauses spécifiques relatives aux obligations respectives des parties résultant du traitement des données à caractère personnel. L'accord doit notamment prévoir les conditions de restitution et de destruction des données. Il incombe au responsable de traitement de s'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.). Pour plus de précisions, vous pouvez vous reporter au guide de la sous-traitance et aux exemples des clauses de sous-traitance.
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
	Encadrer de manière stricte les zones de commentaires libres
	Tester sur des données fictives ou anonymisées
Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnus
	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 relative à 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 le traitement qu'il met en œuvre est susceptible de présenter un risque élevé pour les droits et les libertés des personnes concernées.

Il conviendra tout d'abord de se référer :

– à la liste des traitements pour lesquels une analyse d'impact n'est pas requise ;

Types d'opérations de traitement	Exemples
Traitements, mis en œuvre uniquement à des fins de ressources humaines et dans les conditions prévues par les textes applicables, pour la seule gestion du personnel des organismes qui emploient moins de 250 personnes, à l'exception du recours au profilage.	Les traitements permettant : – la gestion de la paye, l'émission des bulletins de salaire ; – la gestion des formations ; – la gestion du restaurant d'entreprise, la délivrance des chèques-repas ; – le remboursement des frais professionnels ; – le suivi des entretiens annuels d'évaluation ; la tenue des registres obligatoires ; – l'utilisation des outils de communication (messagerie électronique, téléphonie, vidéoconférences, outils collaboratifs en ligne) sans recours au profilage ni à la biométrie ; – le contrôle du temps de travail (sans dispositif biométrique, sans données sensibles ou à caractère hautement personnel) ;
Traitements mis en œuvre aux seules fins de gestion des contrôles d'accès physiques, en dehors de tout dispositif biométrique. **A l'exclusion des traitements des données qui révèlent des données sensibles ou à caractère hautement personnel.**	Les traitements ayant pour finalité : – la mise en place d'un dispositif par badge sans biométrie pour entrer dans les locaux d'un organisme à des fins de sécurité ; – la mise en place d'un dispositif de contrôle du temps de travail effectué par les salariés, à l'exclusion de toute autre finalité ;

– puis, à la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

Types d'opérations de traitement	Exemples
Traitements établissant des profils de personnes physiques à des fins de gestion des ressources humaines	Les traitements ayant pour finalité : – traitements visant à faciliter le recrutement, notamment grâce à un algorithme de sélection ; – traitements visant à proposer des actions de formations personnalisées grâce à un algorithme ; – traitement visant détecter et à prévenir les départs de salariés sur la base de corrélations établies entre divers facteurs ;
Traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés	Les traitements ayant pour finalité : – l'analyse des flux de courriels sortants afin de détecter d'éventuelles fuites d'information (dispositifs dits de « *Data Loss Prevention* ») ; – la vidéosurveillance portant sur les employés manipulant de l'argent ; – la vidéosurveillance d'un entrepôt stockant des biens de valeur au sein duquel travaillent des manutentionnaires ; – la fonction de chronotachygraphe des véhicules de transport routier.

– si le traitement mis en œuvre n'est pas présent sur l'une de ces listes, il faut alors s'interroger sur la nécessité d'effectuer une AIPD.

Pour ce faire, il convient de s'appuyer sur les 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).

Conformément à ce texte, la réalisation d'une AIPD est obligatoire dès lors qu'au moins deux des neuf critères sont remplis :

– évaluation ou notation d'une personne ;
– prise de décision automatisée ;
– surveillance systématique ;
– traitement de données sensibles ou à caractère hautement personnel ;
– traitement à grande échelle ;
– croisement ou combinaison d'ensembles de données ;
– données concernant des personnes vulnérables ;
– utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles ;
– traitements qui empêchent les personnes d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

A noter : les lignes directrices du CEPD précisent que les **employés peuvent être considérés comme des personnes concernées vulnérables** en raison du déséquilibre des pouvoirs accru qui existe entre elles et le responsable du traitement (l'employeur).

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 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.