Vérifier la conformité d'un organisme à la règlementation sur les données en matière RH
Commentaire du référentiel relatif à la gestion des ressources humaines, JO 15 avril 2020

Par une délibération du 21 novembre 2019[1], la Commission Nationale de l'Informatique et des Libertés (CNIL) a adopté un référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel. Celui-ci a été publié au Journal officiel le 15 avril 2020. C'est l'occasion d'un rappel à l'ensemble des organismes privés et publics, des principes applicables à ce type de traitements.

Comment l'employeur ou son DPO peut-il mettre ou vérifier la conformité l'organisme, privé ou public, à la règlementation relative à la protection des données à caractère personnel[2] en matière de ressources humaines ? Plusieurs étapes à respecter.

Etape 1 - Contrôler la finalité de chaque traitement. Tout traitement doit, pour mémoire, répondre à un objectif précis et être justifié au regard des activités de l'organisme ; les finalités doivent être déterminées, explicites et légitimes[3].

La CNIL indique qu'un traitement de gestion du personnel peut être mis en œuvre pour les finalités suivantes :

- Recrutement,
- Gestion administrative des personnels,
- Gestion des rémunérations et accomplissement des formalités administratives afférentes,
- Mise à disposition du personnel d'outils professionnels,
- Organisation du travail,
- Suivi des carrières et de la mobilité,
- Formation,
- Tenue des registres obligatoires, rapports avec les instances représentatives du personnel (IRP),
- Communication interne,
- Gestion des aides sociales,
- Réalisation des audits, gestion du contentieux et du précontentieux.

Etape 2 - Contrôler l'identification (et documentation) de la base légale de chaque traitement, pour chacune des finalités. Le responsable de traitement est tenu de déterminer, pour chaque finalité de chaque traitement, la base légale applicable[4]. En matière de ressources humaines, celle-ci peut inclure :

- Le respect d'une obligation légale ;
  Ex : gestion des élections professionnelle, organisation des réunions des IRP, déclaration sociale nominative (DSN), tenue d'un registre unique du personnel.

- L'exécution d'un contrat si et seulement si la personne concernée y est partie, ou de mesures précontractuelles prises à sa demande ;
  Ex : Traitement des candidatures et entretiens, gestion du dossier professionnel des employés, établissement des rémunérations et mise à disposition des bulletins de salaires.

- La réalisation de l'intérêt légitime poursuivi par l'organisme et le destinataire des données (l'organisme devra, pour y avoir recours, effectuer et documenter la balance des intérêts entre

[1] 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, JORF n°0092 du 15 avril 2020.
[2] Il s'agit de mettre en conformité l'organisme aux dispositions du Règlement général sur la protection des données (RGPD) et de la loi Informatique et Liberté du 6 janvier 1978 modifiée (LIL).
[3] Article 5, al.1b, du RGPD.
[4] Article 6, al.1, du RGPD. Sur la méthode pour identifier la base légale appropriée, voir le commentaire CNIL, « La licéité du traitement : l'essentiel sur les bases légales prévues par le RGPD », 2 décembre 2019, accessible sur : https://www.cnil.fr/fr/la-liceite-du-traitement-lessentiel-sur-les-bases-legales-prevues-par-le-rgpd.

l'intérêt légitime qu'il poursuivi d'une part, et les droits et libertés fondamentaux de la personne concernée d'autre part) ;

Ex : CV-thèque, gestion des annuaires internes et organigrammes, suivi et maintenance du parc informatique, mise en œuvre des dispositifs de sécurité des réseaux, gestion de la messagerie électronique professionnelle, intranet, gestion des agendas, évaluation professionnelle des personnels, gestion des compétence, organisation des formations.

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

  Ex : traitements liés au recrutement dans le secteur public.

- Le consentement de la personne concernée, si celui-ci est libre, spécifique, éclairé et univoque **et** que l'acceptation ou le rejet d'une proposition n'entraine aucune conséquence sur leur situation. Le recours à cette base légale doit être exceptionnel étant donné que les employés sont considérés comme des « personnes vulnérables » au sens du RGPD, compte tenu du lien de dépendance qui découle de la relation employeur / salarié.

  Ex : enregistrement d'un clip promotionnel dans un espace de travail faisant apparaitre des employés identifiables.

Etape 3 - Vérifier que seules sont traitées les données personnelles pertinentes et strictement nécessaires au regard des besoins de gestion du personnel. Conformément au principe de minimisation des données[5], l'organisme doit veiller à ne collecter que les données pertinentes et strictement nécessaires au regard de ses propres besoins de gestion du personnel. Ainsi, par exemple, la CNIL rappelle que le numéro de sécurité sociale peut être demandé à une personne embauchée pour effectuer les formalités déclaratives de début de contrat, mais ne peut l'être au candidat avant validation définitive de sa candidature.

Les données collectées pour une finalité déterminée, ne peuvent en aucun cas être réutilisées à d'autres fins.

Etape 4 - Contrôler la licéité du traitement des données sensibles, s'il en existe. Les données 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, ainsi que les données relatives aux infractions, condamnations pénales et mesures de sûreté connexes, ou les données concernant des personnes mineurs, doivent faire l'objet d'une vigilance renforcée[6].

Etape 5 - Vérifier qu'une mise à jour régulière des données à caractère personnel est prévue et effective. La CNIL rappelle dans le référentiel que « *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* ». Cette vérification est rendue ainsi indispensable par le principe d'exactitude des données[7].

Etape 6 - Vérifier que sont mises en place, et documentées, des habilitations pour l'ensemble des destinataires des données. Seules doivent pouvoir accéder aux données, les personnes habilitées à en connaitre au regard de leurs attributions. En matière RH, il peut s'agir :

- Des personnes habilitées chargées de la gestion du personnel ou de la paie,
- Des personnes 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 salariés concernés.

[5] Article 5, al.1c, du RGPD.
[6] V. les articles 9 et 10 du RGPD, et les articles 6 et 44 à 46 de la LIL.
[7] Article 5, al.1d, du RGPD.

Peuvent en outre être destinataires de ces données[8] RH, par exemple :

- Les IRP, pour les données strictement nécessaires à leurs missions,
- Les organismes gérant les différents systèmes d'assurance (sociales, chômage, retraite…) ;
- Les entités chargées de l'audit et contrôle financier de l'organisme,
- Les prestataires auxquels des activités sont sous-traitées,
- Les entités en charge de l'action culturelle et sociale (ex : CSE), si le bénéficiaire en fait la demande.

Si recours est fait à un sous-traitant, celui-ci doit présenter des garanties suffisantes[9]. En outre, si des transferts de données ont lieu hors de l'Union européenne, ils doivent respecter les règles qui y sont applicables[10].

Etape 7 - Vérifier que les données sont conservées le temps strictement nécessaire à la réalisation des finalités poursuivies. La durée de conservation des données, sous une forme permettant l'identification des personnes concernées, doit être fixée au regard de la finalité de cette conservation, et en amont du traitement. Deux durées distinctes peuvent être prévues pour la base active d'une part, et l'archivage intermédiaire (avec accès restreint) d'autre part.

En matière RH, les durées de conservation indicatives données par la CNIL sont les suivantes :

Activités de traitement	Détails du traitement	Base active	Archivage intermédiaire	Texte de référence
Gestion de la paie	Bulletin de salaires	1 mois	5 ans (50 ans en version dématérialisée)	L.3243-4 (D.3243-8) du code du travail
	Eléments nécessaires au calcul de l'assiette	1 mois	6 ans	L.243-16 du code de la sécurité sociale
	Saisie des données calculées (DSN)	Temps nécessaire à l'accomplissement de la DSN	6 ans	L.243-16 du code de la sécurité sociale
	Ordre de virement pour paiement	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 de commerce
Registre unique du personnel		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 des délits)	L.2411-5 du code du travail
	Données relatives aux sujétions particulières ouvrant droit à congés spéciaux ou à crédit d'heures de délégation	Temps de la période de sujétion de l'employé concerné	6 ans (prescription pénale des délits)	L.2142-1-3 du code du travail

Etape 8 - Contrôler l'information effective des personnes concernées (et sa documentation). Les personnes concernées par les traitements en matière de gestion des ressources humaines (qu'il s'agisse de

[8] Est destinataire des données selon le référentiel, « *tout organisme qui reçoit la communication des données* » (v. aussi l'article 4, al.9 du RGPD).
[9] Sur le recours à un sous-traitant, v. le guide du sous-traitant édité par la CNIL, accessible sur : https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf.
[10] V. les articles 44 et suivants du RGPD ; CNIL, « Transférer des données hors de l'UE », accessible sur : https://www.cnil.fr/fr/transferer-des-donnees-hors-de-lue.

salariés, de stagiaire, de vacataires, de collaborateurs ou même de candidats non encore embauchés), doivent être informés des traitements de leurs données à caractère personnel. Il convient de contrôler que cette information est effective, et qu'elle inclue les mentions visées par les articles 12, 13 et 14 du RGPD[11].

L'information doit inclure, notamment, une mention relative à :

- L'existence du traitement,
- Ses caractéristiques : finalités, base légale identifiée pour chaque finalité de chaque traitement, durée de conservation des données (ou les critères pour la déterminer),
- Les droits dont dispose la personne concernée.

Etape 9 - Contrôler l'effectivité de l'exercice des droits des personnes concernées. Les droits des personnes concernées qui doivent être garantis, en matière de gestion des ressources humaines, sont les suivants :

- Droit d'opposition au traitement :
  Existe lorsque la personne concernée invoque des raisons tenant à sa situation particulière, si 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 ;
  N'existe pas quand le traitement répond à une obligation légale, une obligation contractuelle ou est, exceptionnellement, fondé sur le consentement (la personne concernée peut dans ce cas retirer son consentement).

- Droit d'accès, de rectification, d'effacement (dans des conditions particulières) ;

- Droit à la limitation du traitement, par exemple lorsque la personne conteste l'exactitude de ces données ;

- Droit à la portabilité
  Existe seulement pour les données fournies par la personne sur la base de son consentement ou d'un contrat. Conseil : Préciser directement dans l'information, les traitements concernés par ce droit à la portabilité.

Etape 10 - Vérifier la mise en place par l'organisme des mesures de sécurité listées par la CNIL (ou la justification du défaut de mise en place). L'organisme est tenu de prendre toutes les précautions utiles au regard des risques présentés par son traitement, pour préserver la sécurité des données à caractère personnel. Sur ce point, la CNIL fournit dans son référentiel, la liste des mesures que l'organisme doit mettre en place pour préserver la disponibilité, la confidentialité et l'intégrité des données traitées en matière RH.

L'organisme doit adopter ces mesures, listées dans le référentiel, par exemple en matière de sensibilisation des utilisateurs, authentification, gestion des habilitations, traçabilité des accès et gestion des incidents, sécurisation des postes de travail et de l'informatique mobile, protection du réseau informatique interne, sauvegarde, archivage, gestion de la sous-traitance, protection des locaux, etc.[12]

A défaut, il doit justifier de leur équivalence ou du fait de ne pas avoir besoin ou pouvoir y recourir[13].

Etape 11 - Contrôler la réalisation des AIPD rendues nécessaires pour certains traitements RH. Une analyse d'impact relative à la protection des données (AIPD) est requise chaque fois que le responsable de

[11] Pour des modèles d'information, v. CNIL, « RGPD : exemples de mentions d'information », accessible sur : https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation.
[12] Le tableau étant détaillé, nous ne le reproduisons pas directement dans ce flash info. Se reporter au tableau des pages 13 à 15 du référentiel directement.
[13] Sur la question de la sécurité, v. plus largement le Guide de la sécurité des données personnelles, accessible sur : https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf.

traitement met en œuvre un traitement susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées[14].

En matière RH, la CNIL a déjà eu l'occasion de rappeler qu'une AIPD n'est pas nécessaire pour les 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), et pour les traitements mis en œuvre aux seules fins de gestion des contrôles d'accès physiques, en dehors de tout dispositif biométrique (à l'exclusion des traitements des données qui révèlent des données sensibles ou à caractère hautement personnel)[15].

Elle est en revanche obligatoire pour les traitements établissant des profils de personnes physiques à des fins de gestion des ressources humaines et pour ceux ayant pour finalité de surveiller de manière constante l'activité des employés concernés[16].

Elle l'est également, lorsque deux des neufs critères suivants sont réunis :

- Evaluation 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'ensemble de données,
- Données concernant des personnes vulnérables (sachant que les employés peuvent être considérés, selon le CEPD, comme des personnes concernées vulnérables),
- Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles,
- Traitement qui empêche les personnes d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

Les AIPD nécessaires devront être réalisées en partenariat avec le DPO désigné, le cas échéant[17].

Etape 12 - En fonction des AIPD réalisées, vérifier l'identification par l'organisme des mesures suffisantes pour réduire les risques à un niveau acceptable. Si le responsable de traitement ne parvient pas, dans le cadre d'une AIPD, à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable, il est tenu de consulter la CNIL préalablement à la mise en œuvre du traitement[18].

…Si l'ensemble de ces conditions sont remplies, alors les traitements RH mis en place par votre organisme sont certainement en conformité avec la règlementation applicable en matière de protection des données personnelles.

Qu'en est-il si votre organisme ne respecte pas l'ensemble de ces lignes directrices ?

Pas d'inquiétude : la CNIL précise que des mesures s'écartant du référentiel peuvent tout à fait, selon les situations, être prises par un organisme. Il lui revient seulement, dans ce cas, de justifier l'existence du besoin d'un tel écart, et de prendre toutes les mesures appropriées pour garantir la conformité de cet écart aux principes de protection des données.

[14] Article 35 du RGPD.
[15] CNIL, Liste des traitements pour lesquels une analyse d'impact n'est pas requise, 22 octobre 2019 (délibération n°2019-118 du 12 septembre 2019), accessible sur : https://www.cnil.fr/fr/liste-traitements-aipd-non-requise.
[16] CNIL, Liste des traitements pour lesquels une analyse est requise, 6 novembre 2018 (délibération n°2018-327 du 11 octobre 2018), accessible sur : https://www.cnil.fr/fr/liste-traitements-aipd-requise.
[17] Pour effectuer l'AIPD, v. plus généralement les outils méthodologiques proposés par la CNIL accessibles sur : https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd.
[18] Article 36 du RGPD.

Marine DOISY, Avocate au barreau de Paris, collaboratrice du cabinet Vigo, membre du réseau international d'avocats GESICA.

Emmanuel DAOUD, Avocat au barreau de Paris, associé du cabinet Vigo, membre du réseau international d'avocats GESICA.