DS AVOCATS

FLASH INFO - CORONAVIRUS

17 avril 2020

#RGPD - Adoption par la CNIL du référentiel relatif à la gestion des ressources humaines

Par publication au Journal Officiel du 15 avril 2020 de sa délibération n°2019-160 du 21 novembre 2019, la CNIL a adopté un **référentiel relatif aux traitements de données personnelles mis en œuvre aux fins de gestion des ressources humaines (« RH »)**.

S'inscrivant dans une logique visant à aider les organisations dans leurs actions de conformité, la CNIL propose un cadre de référence qui applique les principes du RGPD aux traitements de données personnelles, nombreuses et parfois sensibles, couramment mis en œuvre dans le cadre de la gestion du personnel.

Dans les limites de son champ d'application, ce référentiel a vocation à remplacer les recommandations, dispenses, normes simplifiées et packs de conformité produits par la CNIL avant l'entrée en application du RGPD (notamment les dispenses de déclaration en matière de gestion de paie, ainsi que la norme simplifiée NS-46 relative aux traitements de données dans le domaine RH).

Il convient de préciser que ce référentiel **n'a pas une nature contraignante**. Les responsables de traitement peuvent donc s'écarter des préconisations qui y figurent (par exemple, en appliquant des durées de conservation différentes de celles suggérées par le référentiel, en identifiant d'autres bases légales pour tel ou tel traitement spécifique, etc.), à condition toutefois de pouvoir justifier leur choix et de les documenter, sous leur responsabilité.

Nous proposons ci-après une synthèse des points structurants abordés par ce nouveau référentiel de la CNIL, qui concerne aussi bien les entités de droit privé que de droit public :

1. Les traitements de données personnelles visés par le référentiel
2. Précisions sur les bases légales applicables aux traitements RH
3. Identification des catégories de données personnelles concernées
4. Identification des destinataires de données
5. Suggestions de durées de conservation
6. Rappel des droits des personnes concernées au titre du RGPD
7. Recommandations en matière de sécurité des données et d'analyses d'impacts relatives à la protection des données (AIPD)

1. Les traitements de données personnelles visés par le référentiel

Ce référentiel couvre les traitements **couramment** mis en place par les organismes-employeurs dans le cadre de la gestion de leur personnel, pour les finalités suivantes :

- Le recrutement ;
- La gestion administrative des personnels
- La gestion des rémunérations et l'accomplissement des formalités administratives afférentes ;
- La mise à disposition du personnel d'outils professionnels ;
- L'organisation du travail ;
- Le suivi des carrières et de la mobilité;
- La formation ;
- La tenue des registres obligatoires,
- Les rapports avec les instances représentatives du personnel ;
- La communication interne ;
- La gestion des aides sociales ;
- La réalisation des audits et la gestion du contentieux et du précontentieux.

Certains traitements sont toutefois **exclus du champ d'application** du référentiel en raison de leur spécificité et de sensibilité. Il s'agit principalement:

- **Des 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** (profilage, analyses algorithmiques visant à prédire le comportement ou la productivité des salariés, etc.), ou encore les traitements dits de **« Big Data »** ;
- Des traitements ayant pour objet ou pour effet le **contrôle individuel de l'activité des salariés** (vidéosurveillance, dispositifs d'écoute et enregistrement des conversations téléphoniques, etc.) ou faisant l'objet d'un **encadrement spécifique** (contrôle d'accès aux locaux de travail à l'aide des dispositifs biométriques, dispositif d'alertes professionnelles).

Ce sont néanmoins ces derniers traitements, exclus du périmètre du référentiel, qui comportent le plus de risques du point de vue de la protection des données personnelles.

Tout responsable de traitement / employeur qui souhaiterait mettre en œuvre de tels dispositifs devra donc s'assurer de la conformité de sa démarche à la réglementation en vigueur en procédant à sa propre analyse, sous sa responsabilité exclusive.

2. Précisions sur les bases légales applicables aux traitements RH

Pour l'ensemble des traitements concernés par le référentiel, la CNIL propose des bases légales applicables en fonction des différentes finalités poursuivies, sous forme de tableau synthétique.

Les bases légales les plus couramment utilisées pour les traitements RH sont, classiquement :

- 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 (le contrat de travail), soit de **mesures précontractuelles** prises à sa demande ;
- 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.

La CNIL rappelle à cette occasion que le **consentement** des personnes concernées n'est applicable que **de façon résiduelle dans un contexte RH** : les employés ne sont en effet 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.

Le tableau proposé par la CNIL ne couvre évidemment pas l'intégralité des finalités pouvant être poursuivies par les traitements RH concernés par le référentiel.

Si ce référentiel pourra constituer un **outil d'aide à la décision** pour les responsables de traitements (en particulier afin de les aider à renseigner leur registre des traitements, voire pour procéder à une analyse d'un traitement dans le cadre d'une analyse d'impact), ces derniers devront toutefois mener une analyse au cas par cas quant au choix de la base légale applicable, et documenter les arbitrages retenus conformément au principe d'*accountability*.

A titre d'illustration, les traitements en matière de **recrutement** cités dans le référentiel ne sont mis en œuvre qu'à des fins (i) de traitement des candidatures (CV et lettre de motivation) et de gestion des entretiens, sur la base légale de mesures précontractuelles prises à la demande du candidat, et (ii) de constitution d'un CV-thèque, sur la base de l'intérêt légitime du responsable de traitement.

Mais les traitements relatifs au recrutement sont souvent mis en œuvre pour des finalités plus fines et dans des contextes plus complexes que ceux envisagés par la CNIL.

Les organisations peuvent par exemple procéder à des tests d'évaluation des candidats (tests de personnalité, tests graphologiques, etc.), avoir recours à des prestataires / sous-traitants spécialisés, utiliser les réseaux sociaux professionnels et autres *jobboards* partenaires, procéder à des enquêtes ou prises de références auprès d'anciens employeurs, partager les CV à fort potentiel au sein du groupe d'entreprises…autant de situations nécessitant de la part du responsable de traitement une analyse quant au choix de la base légale applicable, et plus généralement un encadrement spécifique afin d'être en conformité avec la règlementation en vigueur.

3. Identification des catégories de données personnelles concernées

La CNIL propose une liste des données personnelles susceptibles d'être collectées et traitées par les employeurs pour les finalités RH envisagées dans son référentiel.

Elle rappelle le principe fondamental de **minimisation** (art. 5-1.c) du RGPD), selon lequel l'employeur 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.

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 (on ne peut en effet pas collecter des données « au cas où »).

Le référentiel de la CNIL rappelle également que 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** (NIR, dont l'utilisation est strictement encadrée par la loi) ;
- Des **données relatives aux infractions, condamnations pénales et mesures de sûreté connexes** ;
- 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.

Le tableau ainsi proposé par la CNIL pourrait notamment permettre aux responsables de traitement de procéder à des analyses d'écart pour éventuellement ajuster leurs processus de collecte de données en la limitant au strict nécessaire, et vérifier la pertinence des catégories de données renseignées dans la partie « RH » de leur registre des traitements.

4. Identification des destinataires de données

Le référentiel de la CNIL rappelle que les données personnelles doivent uniquement être rendues accessibles aux personnes **habilitées** à en connaitre au regard de leurs attributions.

Il peut s'agir :

- **Des personnes accédant aux données pour le compte de l'employeur** (destinataires « internes », tels que par exemple le personnel en charge de la gestion du personnel et de la paie, le personnel, le service sécurité, etc.), dont il convient de s'assurer qu'elles disposent d'une habilitation pour avoir accès aux données dans le cadre de leurs fonctions ;
- **Des destinataires « externes » de données**, au nombre desquels peuvent notamment figurer :
  - **Les IRP**, 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** (Groupes de protection sociale, URSSAF, CPAM, Trésor Public, etc.) ;
  - **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.

Lorsqu'un destinataire de données est localisé dans un pays situé en dehors de l'Union européenne, le responsable de traitement devra alors veiller à **encadrer le transfert de données** conformément à la règlementation en vigueur. La CNIL rappelle ainsi que toute transmission de données en dehors de l'UE doit être fondée :

- Sur une décision d'adéquation ; **ou**
- Etre encadrée par des règles internes d'entreprise (« BCR »), des clauses types de protection des données (CCT de la Commission Européenne), un code de conduite ou un mécanisme de certification approuvé par la CNIL ; **ou**
- Etre 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

Dans le contexte RH, de tels transferts de données en dehors de l'UE sont souvent constatés au sein de **groupes internationaux** qui disposent pour nombre d'entre eux d'outils mutualisés en matière de gestion de leur personnel. Il conviendra dans cette hypothèse de veiller à avoir mis en place des mécanismes de type BCR si l'organisation et la maturité en termes de conformité au RGPD du groupe le permettent, ou à tout le moins d'encadrer ces transferts par des conventions de flux ou de partage de données entre les différentes filiales concernées.

Le recours à des **solutions de gestion RH** éditées par des grands comptes (de type ADP, Workday, etc.) implique également le plus souvent des transferts de données à l'international, notamment pour des raisons de maintenance du service externalisé à l'étranger. Il conviendra donc de bien veiller à ce que les contrats conclus avec de tels sous-traitants soient conformes à l'article 28 du RGPD, et prévoient un encadrement des transferts de données concernés.

5. Suggestions de durées de conservation

Le référentiel de la CNIL propose des illustrations pratiques des **durées de conservation** pouvant, selon le contexte, être retenues par les organismes concernés pour les seuls traitements ayant trait à:

- La gestion de la paie ;
- La gestion du Registre unique du personnel ;
- La gestion des mandats des représentants du personnel ;

Il convient de noter que la CNIL n'a pas repris dans ce référentiel les durées de conservation qu'elle préconisait avant l'adoption du RGPD, notamment en matière de recrutement.
Le travail est donc bien évidemment insuffisant, et il incombera à tout responsable de traitement de compléter ce référentiel en définissant des durées de conservation pour l'ensemble des traitements, y compris RH, mis en œuvre au sein de son organisation.

Il est à ce titre recommandé de concevoir une **politique ou un document interne** recensant, et au besoin justifiant les arbitrages, les durées de conservation applicables pour l'ensemble des traitements de données personnelles.

6. Rappel des droits des personnes concernées au titre du RGPD

La CNIL rappelle dans son référentiel les principaux droits dont disposent les salariés/personnes concernées dans un contexte RH :

- Le **droit d'opposition** au traitement de leurs données, lequel:
  - 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) ;
  - 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.

En cas de demande d'exercice de ses droits émanant d'un salarié, d'un ancien salarié, d'un intérimaire ou d'un stagiaire, tendant à l'accès à ses données personnelles détenues par l'entreprise, leur modification, leur effacement, leur portabilité (par exemple vers un nouvel employeur), ou encore la limitation ou l'opposition à un traitement effectué sur ses données personnelles, il conviendra systématiquement de se référer à la **procédure ou méthodologie de**

gestion des droits des personnes concernées, qui figure parmi la documentation indispensable à déployer afin d'assurer sa conformité au RGPD.

7. Recommandations en matière de sécurité des données et d'analyses d'impacts relatives à la protection des données (AIPD)

Le référentiel de la CNIL propose des **recommandations en matière de mesures de sécurité** à mettre en œuvre *a minima* afin de garantir la sécurité et la confidentialité des données RH.

Il ne s'agit là que de **préconisations**, les bonnes pratiques en matière de sécurité devant naturellement être adaptés au contexte métier de l'organisme concerné et de sa propre gouvernance en terme de sécurité des systèmes d'information, voire en fonction des instructions d'un client lorsqu'il s'agit d'un prestataire (sous-traitant) amené à traiter des données personnelles de ses salariés.

En sus des mesures préconisées par la CNIL, il est par ailleurs indispensable de prévoir une **procédure de gestion des violations de données personnelles**, afin de pouvoir efficacement remonter les incidents donnant lieu à une fuite ou une altération des données, et de respecter les délais de notification règlementaires à la CNIL et/ou aux personnes concernées.

Enfin, la CNIL propose **une liste de traitements RH (i) pour lesquels une AIPD n'est pas requise, et (ii) pour lesquels une AIPD est impérative**.

Rappelons à ce sujet qu'en toute hypothèse et pour chaque traitement susceptible de comporter un risque pour les droits et libertés d'une personne concernée, il conviendra de procéder systématiquement à une réflexion en se basant si possible sur une **procédure documentée de gestion des AIPD** qui prendra en considération les critères établis par le Comité Européen à la Protection des Données (CEPD) dans ses lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) (qui précisent d'ailleurs que les employés doivent 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…).

Conclusion

Si l'adoption de ce référentiel est bienvenue en ce qu'il peut constituer une boite à outil pour les entreprises dans leur démarche de conformité de leurs traitements RH, il ne saurait en aucun cas, comme nous l'avons vu, couvrir l'intégralité des situations.

Les entreprises devront donc poursuivre leurs actions de conformité, notamment sur la base de ce nouveau cadre de référence (i) en affinant la cartographie de leurs données et traitements si besoin en ajustant leur processus de collecte, (ii) en procédant à des modifications du volet RH de leur registre des traitements, (iii) en mettant à jour leurs contrats (contrat de travail, contrat fournisseur, etc.) et autre documentation (politique de confidentialité, chartes informatiques, notices d'information du personnel, etc.), (iv) en concevant ou adaptant leurs procédures internes (procédure de gestion des demandes d'exercice de droit, procédure de gestion des violations de données, procédure de gestion des AIPD, etc.), (v) et ce afin de construire une véritable gouvernance des données leur permettant d'assurer un maintien en condition opérationnelle de leur conformité RGPD.

Thibaud Le Conte des Floris,
Collaborateur
leconte@dsavocats.com

Pour plus d'information, notre équipe se tient mobilisée pour répondre à vos questions :

Catherine Verneret,
Associée
verneret@dsavocats.com

Bertrand Potot
Associé
potot@dsavocats.com

Sylvain Staub,
Associé
staub@dsavocats.com

Antoine Gravereaux,
Associé
gravereaux@dsavocats.com