Actualités

Aperçu rapide

AvoSial
AVOCATS D'ENTREPRISE EN DROIT SOCIAL

368

En questions : la gestion des données RH et le règlement européen sur la protection des données

Stéphanie Marchal,
avocat au barreau d'Annecy, membre d'AvoSial

Les données RH sont des éléments clefs de la gestion individuelle et collective du personnel de l'entreprise et de la protection de son savoir-faire. Pour pouvoir être utilement exploitées, elles doivent être enregistrées et classées dans des bases de données, nominatives ou non, selon l'usage qui en est fait. Ces données concernent principalement le recrutement, la gestion du personnel (la formation, les évaluations, la rémunération, le temps de travail, les plans de carrière et la mobilité) mais aussi l'utilisation des outils de l'entreprise par les salariés (contrôle des communications téléphoniques, des courriers, contrôle de l'activité informatique, etc.) ou encore le contrôle des accès (badge, biométrie, cartes à puce, etc.), ou du lieu de travail (vidéosurveillance, géolocalisation des véhicules des salariés, etc.).

La plupart du temps, les données initialement nominatives permettant la gestion individuelle des salariés et la mise en œuvre des obligations administratives qui y sont attachées (données quantitatives), sont en tout ou partie anonymisées et réutilsées à des fins statistiques pour une analyse plus globale du fonctionnement de l'entreprise et la détermination de ses objectifs en matière de ressources humaines (données qualfitatives).

Si le traitement des données RH statistiques issues généralement des données anomymisées est libre et ses résultats doivent, le cas échéant, être portés à la connaissance des représentants du personnel dans le cadre des consultations sur la politique sociale de l'entreprise, sur les conditions de travail et d'emploi, sur la situation économique et financière de l'entreprise ou sur les orientations stratégiques de l'entreprise, le traitement des données nominatives RH est lui, strictement encadré par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, transposant notamment la directive européenne 95/46 du 24 octobre 1995 relative à la protection des données à caractère personnel et à la libre circulation de ces données et par le Code du travail.

Par ailleurs, a été adopté le règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation des données (RGPD) [1] imposant de nouvelles obligations aux entreprises. Il entre en vigueur à compter du 25 mai 2018. La ministre de la Justice a présenté, le 13 décembre 2017, le projet de loi relatif à la protection des données personnelles qui adapte au droit de l'Union européenne la loi Informatique et libertés du 6 janvier 1978 et transpose le nouveau cadre juridique européen issu du RGPD.

1. Quelles sont les obligations actuelles de l'employeur en matière de gestion des données RH ?

Actuellement, le traitement de données nominatives RH doit être porté à la connaissance des salariés concernés, avoir fait l'objet d'une information et consultation du comité d'entreprise et, le cas échéant, du CHSCT, préalablement à sa mise en œuvre.

Ndlr : dans cette rubrique mensuelle « En questions », un avocat en droit social, membre d'AvoSial, association d'avocats d'entreprises en droit social, présente un point de vue sur un thème d'actualité et ses implications pratiques.

1. *PE et Cons. UE, règl. (UE) 2016/679, 27 avr. 2016 et PE et Cons. UE, dir. 2016/680, 27 avr. 2016.*

Sauf dans les cas de dispenses établies par la CNIL pour les catégories de fichiers courantes sans risque manifeste d'atteinte à la vie privée ou aux libertés (tels que les fichiers de gestion de paie), l'employeur qui procède au traitement de données nominatives (soit la plupart des employeurs) doit, soit déclarer chaque traitement auprès de la CNIL, soit procéder à la désignation d'un correspondant informatique et libertés (CIL).

Le CIL est chargé d'assurer de manière indépendante la conformité des traitements de données à la législation et d'en tenir une liste accessible à toute personne qui en fait la demande. Sa nomination entraîne une dispense de déclaration préalable des traitements de données à caractère nominatif.

De plus, l'employeur doit veiller à ce que tout traitement de données nominatives RH respecte les principes de conformité suivants :

– finalité : les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime ;

– proportionnalité et pertinence des données : seules doivent être traitées les informations pertinentes nécessaires au regard des objectifs poursuivis ; la mise en place d'un dispositif de contrôle des salariés ne doit pas conduire à apporter des restrictions aux droits et libertés des personnes qui ne seraient pas proportionnées au but recherché et justifiées par un intérêt légitime de l'entreprise *(C. trav., art. L. 1121-1)* ;

– durée de conservation : les informations ne peuvent être conservées que pour une durée limitée et précise, déterminée en fonction de la finalité de chaque fichier ;

– sécurité et confidentialité : l'employeur, en tant que responsable du traitement, doit prendre toutes les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation à des tiers non-autorisés ;

– respect des droits des personnes : lors de la collecte des données, les salariés ou candidats concernés doivent être clairement informés des objectifs poursuivis, du caractère obligatoire ou facultatif de la réponse, des destinataires des données et des modalités d'exercice de leurs droits d'accès, de rectification et d'opposition ;

– exclusion de principe des informations sensibles : il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale des personnes, leur état de santé ou leur orientation sexuelle ou les infractions et condamnations qu'elles ont encourues, sans avoir recueilli le consentement explicite des personnes concernées.

2. Quels sont les apports du RGPD sur la protection des données RH ?

Le règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation des données (RGPD) a été adopté le 27 avril 2016 et est entré en vigueur le 24 mai 2016. Il sera applicable à partir du 25 mai 2018. Dès lors, les traitements déjà mis en œuvre à cette date devront être mis en conformité avec ses dispositions.

Le RGPD prévoit une conformité basée sur la transparence et la responsabilisation des acteurs dans le même sens que la loi du 6 août 2004 en allégeant les formalités préalables à effectuer auprès de la CNIL et en renforçant son contrôle *a posteriori*. Cependant, le RGPD va plus loin, notamment en mettant fin à l'obligation de déclaration prévue par la Loi Informatique et Libertés et en imposant aux entreprises de pouvoir rapporter à tout moment la preuve qu'elles protègent les données personnelles. À cet effet, sont prévus :

– de nouvelles obligations, dont celles de recueillir l'accord explicite et formel des salariés pour saisir, stocker et détenir leurs données individuelles et de les informer de leur droit à portabilité des données, qui permettra à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable ;

– de nouveaux outils de conformité, tels que la tenue d'un registre des traitements mis en œuvre, la notification de failles de sécurité aux autorités et personnes concernées, la certification de traitement, l'adhésion à des codes de conduite, la désignation d'un délégué à la protection des données (*Data Protection Officer* – DPO), ou la réalisation d'études d'impact sur la vie privée.

Le DPO a vocation à remplacer le CIL.

Selon le RGPD, la désignation d'un DPO n'est obligatoire que pour les traitements de données personnelles effectués par une autorité ou un organisme publique, ou lorsque les activités de base de l'organisme consistent en des traitements qui exigent un suivi régulier et systématique à grande échelle des personnes concernées (profilage, ciblage publicitaire, etc.), ou enfin, lorsque l'activité implique le traitement à grande échelle de données sensibles.

Toutefois, une telle désignation est fortement recommandée par les experts pour les structures qui n'y sont pas contraintes mais qui collectent des données personnelles et gèrent de nombreux traitements, y compris en ce qui concerne la gestion de leurs données RH, afin de charger le DPO de documenter leur conformité.

En effet, **à compter du 25 mai 2018**, les entreprises devront notamment être en mesure d'établir :

– la « sécurisation » des données par la formalisation de toutes les protections mises en œuvre (tels que le cryptage ou le chiffrage dans les fichiers et le stockage au sein de datacenters sécurisés) ;

– un registre actualisé des traitements existants.

Le RGPD assure également la protection des données transférées en dehors de l'Union européenne, d'une part en l'autorisant sous réserve d'un encadrement avec des outils assurant un niveau de protection suffisant et d'autre part, en imposant que les données transférées en dehors de l'Union européenne restent soumises au droit de l'Union non seulement pour leur transfert mais aussi pour tout traitement et transfert ultérieur. Ainsi, en cas de centralisation des données RH, le même niveau de transparence et sécurisation devra être respecté pour l'ensemble de la gestion des données RH des groupes internationaux dont le siège se trouve en Europe.

La CNIL restera compétente pour s'assurer de la conformité des traitements de données mis en œuvre par les entreprises dont l'établissement principal se situe en France mais devra collaborer avec les autorités de protection des données des différents états membres au sein d'un Comité européen de la protection des données (CEPD) qui veillera à l'application uniforme du droit de la protection des données.

3. Quels risques et quelles solutions pour la mise en conformité des traitements de données personnelles RH ?

Actuellement, outre l'exposition à des sanctions pénales pour délit d'entrave, à défaut d'information des salariés et/ou de consultation préalable des représentants du personnel sur le traitement des données nominatives, l'utilisation de ces données et leur traitement par l'employeur pour établir une faute d'un salarié constituera un mode de preuve illicite et devra donc être écarté. Par conséquent, toute procédure disciplinaire en découlant directement sera annulée.

En outre, la responsabilité civile de l'employeur qui n'aurait pas respecté ses obligations en matière de traitement de données à ca-

ractère personnel est engagée à l'égard des salariés auxquels ces manquements ont causé un préjudice.

Enfin, l'employeur qui n'aurait ni désigné un CIL, ni déclaré un traitement de données personnelles à la CNIL ou qui n'aurait pas respecté les principes de conformité, s'expose à des peines correctionnelles pouvant aller jusqu'à 150 000 € d'amende (300 000 € en cas de récidives) et/ou 3 ans d'emprisonnement.

En vertu de l'article 83 du RGPD, les sanctions encourues se sont considérablement accrues puisque chaque autorité de contrôle (dont la CNIL) disposera du pouvoir d'imposer une amende administrative pouvant, dans certains cas « *s'élever jusqu'à 20 000 000 € ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu* ».

Si les obligations de l'employeur en matière de gestion de données RH ne seront pas fondamentalement modifiées par la mise en application du RGPD, le souci de transparence et responsabilisation accrue, la volonté de coopération et d'uniformisation et le renforcement des sanctions encourues devraient obliger la CNIL à accroître sa surveillance. En conséquence, les entreprises ont intérêt à s'assurer de la conformité de leurs traitements de données RH au règlement et, à cet effet, à faire appel aux services d'un DPO. La possibilité d'externalisation de la fonction devrait permettre à toutes les entreprises d'y avoir accès à terme, quelle que soit l'importance de leur besoin.

Annexe

Règement (UE) 2016/679, 27 avr. 2016, art. 83

Article 83 - Conditions générales pour imposer des amendes administratives

1. Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives.

2. Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j). Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants :

a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi;

b) le fait que la violation a été commise délibérément ou par négligence ;

c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ;

d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32 ;

e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant;

f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs ;

g) les catégories de données à caractère personnel concernées par la violation ;

h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation ;

i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures ;

j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42; et

k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

3.Si un responsable du traitement ou un sous-traitant viole délibérément ou par négligence plusieurs dispositions du présent règlement, dans le cadre de la même opération de traitement ou d'opérations de traitement liées, le montant total de l'amende administrative ne peut pas excéder le montant fixé pour la violation la plus grave.

4.Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu :

a) les obligations incombant au responsable du traitement et au sous-traitant en vertu des articles 8, 11, 25 à 39, 42 et 43;

b) les obligations incombant à l'organisme de certification en vertu des articles 42 et 43 ;

c) les obligations incombant à l'organisme chargé du suivi des codes de conduite en vertu de l'article 41, paragraphe 4.

5. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu :

a) les principes de base d'un traitement, y compris les conditions applicables au consentement en vertu des articles 5, 6, 7 et 9 ;

b) les droits dont bénéficient les personnes concernées en vertu des articles 12 à 22 ;

c) les transferts de données à caractère personnel à un destinataire situé dans un pays tiers ou à une organisation internationale en vertu des articles 44 à 49 ;

d) toutes les obligations découlant du droit des États membres adoptées en vertu du chapitre IX ;

e) le non-respect d'une injonction, d'une limitation temporaire ou définitive du traitement ou de la suspension des flux de données ordonnée par l'autorité de contrôle en vertu de l'article 58, paragraphe 2, ou le fait de ne pas accorder l'accès prévu, en violation de l'article 58, paragraphe 1.

6. Le non-respect d'une injonction émise par l'autorité de contrôle en vertu de l'article 58, paragraphe 2, fait l'objet, conformément au paragraphe 2 du présent article, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

7.Sans préjudice des pouvoirs dont les autorités de contrôle disposent en matière d'adoption de mesures correctrices en vertu de l'article 58, paragraphe 2, chaque État membre peut établir les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire.

8. L'exercice, par l'autorité de contrôle, des pouvoirs que lui confère le présent article est soumis à des garanties procédurales appropriées conformément au droit de l'Union et au droit des États membres, y compris un recours juridictionnel effectif et une procédure régulière.

9.Si le système juridique d'un État membre ne prévoit pas d'amendes administratives, le présent article peut être appliqué de telle sorte que l'amende est déterminée par l'autorité de contrôle compétente et imposée par les juridictions nationales compétentes, tout en veillant à ce que ces voies de droit soit effectives et aient un effet équivalent aux amendes administratives imposées par les autorités de contrôle. En tout état de cause, les amendes imposées sont effectives, proportionnées et dissuasives. Les États membres concernés notifient à la Commission les dispositions légales qu'ils adoptent en vertu du présent paragraphe au plus tard le 25 mai 2018 et, sans tarder, toute disposition légale modificative ultérieure ou toute modification ultérieure les concernant.

L'information en continu

Cotisations et contributions sociales

369 AGS : taux maintenu à 0,15 % au 1er janvier 2018

AGS, conseil d'administration, 12 déc. 2017

Décision a été prise par le conseil d'administration de l'AGS, le 12 décembre 2017, de maintenir inchangé le taux de la cotisation AGS au 1er janvier 2018, à 0,15 % donc.

Sécurité sociale

370 Plafond de la sécurité sociale : montants pour 2018

A. 5 déc. 2017 : JO 9 déc. 2017, texte n° 13

Par arrêté, sont confirmées les valeurs **mensuelle (3 311 €)** et **journalière (182 €)** du plafond de la sécurité sociale s'appliquant aux cotisations et aux contributions de sécurité sociale dues au titre des périodes courant à compter du 1er janvier 2018.

Des montants que nous avions récemment annoncé, de même que nous avions rendu compte des autres plafonds – calculés par la rédaction – applicables selon la périodicité de la paie *(JCP S 2017, act. 356)* :

- **année : 39 732** € ;
- trimestre : 9 933 € ;
- quinzaine : 1 656 € ;
- semaine : 764 € ;
- horaire (pour une durée inférieure à 5 heures) : 25 €

EN BREF

RESTRUCTURATIONS D'ENTREPRISES. Un délégué interministériel est nommé. Auparavant dirigeant d'une grande entreprise industrielle, **Jean-Pierre Floris** aura pour mission d'animer, de coordonner et d'optimiser l'accompagnement par l'État des restructurations d'entreprises. Il pilotera le réseau régional des commissaires au redressement productif et sera chargé de faire des propositions pour optimiser l'accompagnement dans les territoires. Il devra également identifier les filières pouvant être confrontées à des mutations industrielles afin d'agir à temps aux côtés des entreprises pour leur permettre de se repositionner *(D. 8 déc. 2017 : JO 9 déc. 2017, texte n° 179 ; Min. Trav. et Min. Éco., 8 déc. 2017, communiqué conjoint).*