Les changements provoqués par le Règlement Général sur la Protection des Données (RGPD)

NEWCHALLENGES

Séminaire OBES à Paris, le 13 septembre 2019

Avec le soutien financier de la Commission européenne

European Commission

CFE-CGC AGRO

Le cas particulier du transfert de données hors de l'UE

- Dans ce cas, il faudra vérifier si le pays vers lequel les données sont transférées dispose d'une législation de protection des données et si elle est reconnue adéquate par la Commission européenne.

- Une carte du monde présentant les législations de protection des données est disponible sur le site de la CNIL.

- A défaut, l'entreprise devra encadrer juridiquement ses transferts pour assurer la protection des données à l'étranger.

Un challenge : assurer le respect de nouveaux droits pour les salariés : droit d'accès, de rectification, d'opposition, d'effacement (droit à l'oubli), droit à la portabilité et à la limitation du traitement.

- Le RGPD impose de mettre à la disposition des salariés les moyens d'exercer effectivement leurs droits via un formulaire de contact sur un site web, un numéro de téléphone ou encore une adresse de messagerie.

- Le droit à l'oubli est le droit pour une personne d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant. Les motifs justifiant l'exercice de ce droit sont limitativement énumérés par l'article 17 du RGPD. De façon générale, le RGPD impose de procéder à la suppression des données dès lors qu'elles ne sont plus utiles au regard des finalités pour lesquelles elles ont été collectées. Il est recommandé au-delà de la fixation de délais de suppression des données selon les fichiers, de prévoir des mécanismes de suppression automatique ou des alertes sur les outils utilisés pour la conservation des fichiers. En ce qui concerne plus particulièrement le recrutement, les informations sur les candidats non retenus doivent être supprimées sauf s'ils acceptent de rester dans le « vivier » de l'entreprise (durée de conservation limitée à 2 ans).

- Le droit à limitation d'un traitement s'entend de la faculté pour une personne de demander à ce que le responsable du traitement ne puisse se servir de certaines données collectées.

- Le droit à la portabilité qui est une nouveauté introduite par le RGPD constitue le droit pour une personne d'obtenir, voire de réutiliser, les données la concernant pour ses besoins personnels mais il implique la réunion de 3 conditions :
  - les données personnelles ont été fournies par la personne elle-même ;
  - les données sont traitées de manière automatisée, sur la base du consentement de l'intéressée ou pour l' exécution d'un contrat ;
  - la portabilité ne doit pas porter atteinte aux droits et libertés de tiers.

Le nouveau défi de sécurisation des données

- Différentes actions doivent être mises en place : mises à jour des antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes, ou chiffrement des données dans certaines situations.

- L'entreprise victime d'une violation de données (des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées ou il a été constaté un accès non autorisé à des données) doit le signaler à la Cnil dans les 72 heures si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées. Cette notification s'effectue en ligne sur le site internet de la Cnil.

- Il faut aussi notifier à la ou les personnes concernées que leurs données ont été potentiellement mises en danger.

A noter : S'il n'est pas possible d'identifier précisément les personnes susceptibles d'être impactées par les failles de sécurité, il faut notifier au public ce qui peut s'avérer très grave en termes d'image.

Une échelle des sanctions renforcée et encadrée

- Les responsables de traitement et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement : avertissement, mise en demeure, injonction de cesser le traitement, suspension des flux de données etc.

- Les amendes administratives peuvent s'élever, selon la catégorie de l'infraction, à 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, à 2 % jusqu'à 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

- Ce dernier montant doit être rapporté au fait que, pour les traitements transnationaux, la sanction sera conjointement adoptée par l'ensemble des autorités de régulation concernées, donc potentiellement pour le territoire de toute l'Union européenne.

- Dans ce cas, une seule et même décision de sanction décidée par plusieurs autorités de protection sera infligée à l'entreprise.

Des contrôles renforcés de la part de la CNIL

- La CNIL doit désormais procéder à des vérifications dans les locaux des organismes, en ligne, sur audition et sur pièces.

- La décision de réaliser un contrôle s'effectuera sur la base du programme annuel des contrôles, des plaintes reçues par la CNIL, des informations figurant dans les médias, ou pour faire suite à un précédent contrôle.

- La principale nouveauté réside dans le fait que les contrôles effectués sur des acteurs internationaux s'effectueront dans un contexte de coopération très poussée qui conduira à une décision harmonisée à portée européenne.

- Les principes fondamentaux de la protection des données restent pour l'essentiel inchangés (loyauté du traitement, pertinence des données, durée de conservation, sécurité des données, etc.). Ils continueront donc à faire l'objet de vérifications rigoureuses par la CNIL.

- En revanche, pour ce qui est des nouvelles obligations ou des nouveaux droits résultant du RGPD (droit à la portabilité, analyses d'impact, etc.), les contrôles opérés auront essentiellement pour but, dans un premier temps, d'accompagner les entreprises vers une bonne compréhension et la mise en œuvre opérationnelle des textes. En présence d'organismes de bonne foi, engagés dans une démarche de conformité et faisant preuve de coopération avec la CNIL, ces contrôles n'auront normalement pas vocation à déboucher, dans les premiers mois, sur des procédures de sanction sur ces points.

Les conséquences du RGPD sur les Syndicats et les CSE

Les Comités sociaux et économiques (CSE) et syndicats de salariés sont toujours dans l'attente de la production de référentiels RGPD par la Commission nationale de l'informatique et des libertés (CNIL). En attendant, la CNIL reste flexible quant à la mise en conformité.

Contexte et évolution (1/2)

- Avant l'application du Règlement Général européen sur la Protection des Données personnelles (RGPD) en France, le Comité social et économique (CSE) d'une entreprise ou d'un établissement avait obtenu une dispense de déclaration des données personnelles auprès de la Commission nationale de l'informatique et des libertés (CNIL). Mais depuis le 25 mai 2018 l'entrée en vigueur du RGPD, ces dispositions de la CNIL n'ont plus de valeur juridique.

- Aujourd'hui, la protection des données conditionnée par le RGPD vise aussi le CSE. En effet, dans le cadre de ses missions et attributions (notamment pour les actions sociales et culturelles), le CSE est amené à collecter et traiter des données personnelles, notamment les données des salariés relatives à leur vie familiale et personnelle ainsi que leur santé : nom, prénom, adresse, situation familiale, fonction, coordonnées téléphoniques et adresse mail, situation de santé, activités sociales et culturelles, etc. Par ailleurs, un certain nombre d'informations personnelles relatives aux salariés lui sont transmise dans le cadre des consultations obligatoires (rémunérations, etc.).

Contexte et évolution (2/2)

- Le CSE doit donc être en conformité avec le RGPD quant au traitement de ces données :
  - Recueillir le consentement des salariés quant au traitement de leurs données personnelles ;
  - Informer les salariés quant à leurs droits ;
  - Mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément ;
  - Tenir un registre de traitement ;
  - Prévoir les mesures destinées à assurer la confidentialité des données traitées ;
  - Désigner un délégué à la protection des données personnelles au sein du CSE.

- En conséquence, le CSE doit définir des règles précises pour toutes les données personnelles recueillies et les rendre publics aux salariés. Le CSE doit alors protéger l'ensemble de ses informations. Il doit assurer aux salariés qu'elles ne seront pas accessibles à des personnes non autorisées. Le CSE s'engage par ailleurs à ne pas faire un usage détourné de ces données. Autrement dit, chacune d'elles répond à une finalité. Le CSE ne dispose pas du droit d'exploiter ces données à d'autres fins. Il doit y avoir été autorisé par la ou les personnes en question.

La mise en place progressive du registre des activités de traitement

- L'article 30 du RGPD prévoit la mise en place d'un registre des activités de traitement. Ce registre permet de recenser les traitements de données et de disposer d'une vue d'ensemble de ce que fait le CSE avec les données personnelles. Il s'agit d'un document dans lequel seront consignées l'ensemble des données personnelles. La CNIL propose à titre d'exemple, un modèle de registre (annexe 1). Le format de ce document est libre. Il peut être conçu numériquement ou être présenté dans une forme plus manuscrite. Ce registre est un outil de pilotage et de démonstration de la conformité du CSE au RGPD.

- Le registre des activités de traitements de données permet de recenser les traitements de données et de disposer d'une vue d'ensemble des données personnelles.

- <u>3 étapes pour élaborer le registre des activités de traitement :</u>
  - Désigner un délégué à la protection des traitements,
  - Recenser et regrouper les traitements de données par activité,
  - Remplir chaque fiche d'activité détaillant le traitement des données.

Le rôle du délégué à la protection des données (DPD)

- Afin d'actualiser le registre des activités de traitement des données personnelles et veiller au bon respect du RGPD, le CSE peut désigner un délégué à la protection des données (DPD). Cette mesure n'est pas obligatoire mais fortement conseillé dans les entreprises gérant beaucoup de données personnelles. La désignation d'un DPD peut s'avérer utile dans le cadre de la mission d'information et de conseil du CSE auprès du responsable du traitement ou du sous-traitant.

- Actuellement, aucune heure de délégation supplémentaire n'est prévue pour le délégué à la protection des données. Il est à craindre que ce nouveau dispositif entraîne encore un peu plus de responsabilité et de charge de travail pour les élus, surtout le Délégué désigné. Ce travail risque fort de prendre du temps, surtout dans les mois à venir, alors que pour bon nombre d'élus, le passage en CSE est en cours.

Le consentement du salarié

- Le RGPD pose comme condition de solliciter le consentement dans salariés pour la collecte de leurs informations. Les représentant du personnel doivent définir la façon d'obtenir cet accord, que ce soit un document écrit et signé par le salarié, voire une case à cocher lors de la consultation du site internet. Dans tous les cas, le moyen utilisé doit clairement indiquer à la personne concernée qu'elle accepte le traitement de ses données.

- <u>Ainsi, les salariés sont en mesure d'exiger de la part du CSE :</u>
  - L'accès aux informations les concernant ;
  - La rectification de leurs données personnelles ;
  - La suppression de leur profil le cas échéant.

- Pour cela, le CSE doit clairement expliquer aux salariés la ou les procédures à suivre. C'est à cette condition que la réglementation sera la mieux observée.

- Le CSE a l'obligation de mettre en place un règlement intérieur qui détermine ses modalités de fonctionnement, ses règles et celles de ses rapports avec les salariés pour l'exercice de ses missions. Afin d'être en conformité, un grand nombre de CE/CSE insèrent une clause spécifique pour la protection des données dans le règlement intérieur.

L'information-consultation du CSE dans l'application du RGPD

- Les employeurs et directions des ressources humaines doivent aussi se mettre en conformité concernant le traitement des données personnelles des salariés. A ce titre, le élus du CSE peuvent être sollicités dans la mise en conformité de la société. Cela peut notamment se faire via l'information-consultation CSE (lors de la réalisation d'une analyse d'impact d'un traitement particulier notamment) et/ou la signature d'un accord d'entreprise notamment avec les délégués syndicaux.

- <u>Exemples des possibilités d'implication des syndicats et représentants du personnel :</u>
  - Charte informatique (et contrôle de l'utilisation du matériel informatique par les salariés) ;
  - Règlement intérieur (contrôle des accès aux locaux, vidéosurveillance, géolocalisation, usage du téléphone, contrôle des horaires de travail, utilisation de badges, code de conduite, etc.) ;
  - Accord relatif à la transmission de données personnelles entre la société et le CSE/CE.

- Ces pratiques ne sont pas obligatoires mais sont recommandées afin de permettre à l'entreprise une mise en conformité progressive, sans conflit interne.

Les conséquences du RGPD en matière de publicité des accords collectifs

Depuis le 1er septembre 2017, les accords collectifs doivent être rendus publics et publiés dans une base de données nationale, accessible par internet à l'adresse suivante

https://www.legifrance.gouv.fr/initRechAccordsEntreprise.do

Cette base de données nationale a pour objectif de faciliter l'accès aux dispositions contenues dans les accords et conventions collectifs et ainsi renforcer le rôle de la négociation d'entreprisse.

Les accords soumis à cette obligation nouvelle de publicité

- Les conventions et accords collectifs conclus depuis le 1er septembre 2017 doivent être rendus publics et versés dans une base de données nationale, accessible depuis Légifrance. Cette obligation s'applique quel que soit le niveau de la négociation : entreprise, établissement, interentreprises, groupe ou branche.

A noter : Il est fait application de l'article L2231-5-1 du Code du travail.

- Par exception, depuis le 1er avril 2018, les accords de performance collective, les accords d'épargne salariale (intéressement, participation, plans d'épargne d'entreprise, interentreprises et Perco), ainsi que les accords déterminant le contenu du PSE ne sont plus soumis à l'obligation de publication.

- Cependant, cette obligation s'applique aux accords de rupture conventionnelle collective alors même qu'ils comportent des informations économiques et sociales sur l'entreprise.

La possibilité de publication dans une version anonyme

- En application des articles L 2231-5-1 et D 2231-7 du Code du travail, la partie en charge du dépôt de l'accord ou de la convention a l'obligation de joindre à celui-ci une version publiable de la convention ou de l'accord collectif dans un format informatique aisément réutilisable.

- Cette version doit être anonymisée, c'est-à-dire expurgée des prénoms et noms des négociateurs et signataire. La raison sociale de l'entreprise, son numéro de SIREN, le nom des organisations syndicales signataires, la qualité de leurs représentants doivent, cependant, figurer dans l'accord ou la convention.

- Après réception du dossier de dépôt, la Direccte transmet la version publiable du texte à la Direction de l'information légale et administrative (DILA) pour publication sur le site Légifrance (www.teleaccords.travail-emploi.gouv.fr).

Les pièces à déposer

Qu'il s'agisse d'une publication intégrale ou partielle, la personne déposant l'accord ou la convention doit obligatoirement joindre au dépôt les pièces suivantes :

- la version intégrale et signée de l'accord ;
- sa version publiable anonymisée ;
- une copie du courrier, du courrier électronique ou du récépissé ou d'un avis de réception daté de notification du texte à l'ensemble des syndicats représentatifs à l'issue de la procédure de signature.

Dans certains cas particuliers, des informations et documents complémentaires doivent être fournis :

- lorsque l'entreprise a des implantations distinctes, le texte déposé est accompagné de la liste de ces établissements et de leurs adresses respectives ;
- lorsque les parties décident que certains passages de l'accord ne doivent pas être publiés, elles doivent joindre un acte de publication partielle ;
- concernant les accords soumis à référendum, le procès-verbal du résultat de la consultation doit être annexé ;
- le dépôt de pièces complémentaires est également nécessaire dans des cas spécifiques (exemple : accord sur les salaires effectifs).

- Ces pièces sont déposées de préférence au format PDF, à l'exception de la version publiable anonymisée de l'accord qui doit l'être au format docx (www.teleaccords.travail-emploi.gouv.fr).

A noter : La liste des pièces devant obligatoirement accompagner le dépôt de la convention ou l'accord collectif est fixée à l'article D 2231-7 du Code du travail.

La publication partielle

- L'article L 2231-5-1 du Code du travail permet aux signataires d'un accord de groupe, interentreprises, d'entreprise ou d'établissement de décider, une fois l'accord conclu, de ne pas en publier certaines parties.

Cette décision de publication partielle doit être formalisée par un acte motivé et signé :

- côté salariés : par la majorité en nombre des organisations syndicales signataires
- côté employeur : par le représentant légal du groupe, de l'entreprise ou de l'établissement pour les accords conclus à ces niveaux et par les représentants légaux des entreprises concernées pour les accords interentreprises (il est fait application de l'article R 2231-1-1 du Code du travail).

- L'acte de publication partielle, la version publiable du texte ainsi que sa version intégrale signée sont joints au dépôt.

- La convention ou l'accord collectif sera publié avec l'indication que la publication est partielle.

A noter : Depuis le 1er avril 2018, les accords de branche, professionnels ou interprofessionnels ne peuvent plus bénéficier de cette faculté ; ils doivent être publiés dans leur intégralité.

La protection des intérêts de l'entreprise

- Par le biais d'une décision unilatérale, l'employeur peut occulter les éléments portant atteinte aux intérêts stratégiques de l'entreprise.

- Il utilise la faculté qui lui est offerte par l'article L 2231-5-1 d Code du travail.

- Cette faculté est particulièrement intéressante pour les accords dont les modalités d'adoption ne permettent pas la conclusion d'un acte de publication partielle.