Etude d'impact en France

«Les conséquences du RGPD en matière de publication et consultation des accords collectifs»

Avant-propos

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'entreprise.

---

1) 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 qui dispose :

Les conventions et accords de branche, de groupe, interentreprises, d'entreprise et d'établissement sont rendus publics et versés dans une base de données nationale, dont le contenu est publié en ligne dans un standard ouvert aisément réutilisable.

Après la conclusion de la convention ou de l'accord, les parties peuvent acter qu'une partie de la convention ou de l'accord ne doit pas faire l'objet de la publication prévue au premier alinéa. Cet acte, ainsi que la version intégrale de la convention ou de l'accord et la version de la convention ou de l'accord destinée à la publication, sont joints au dépôt prévu à l'article L. 2231-6. A défaut d'un tel acte, si une des organisations signataires le demande, la convention ou l'accord est publié dans une version rendue anonyme, dans des conditions prévues par décret en Conseil d'Etat.

Les conditions d'application du présent article sont définies par décret en Conseil d'Etat ».

Par exception, depuis le 1er avril 2018, les accords de performance collective, les accords d'épargne salariale (intéressement, participation, plans d'épargne d'entreprise,

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

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.

2) 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).

3) 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.

De plus, 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 projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

- 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.

4) Les possibilités de 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.

Cependant, 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.

5) Des questions toujours en suspens

Des questions demeurent cependant sur la nature de l'acte de publication.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

En effet, l'acte de publication partielle n'étant pas un accord collectif, sa négociation ne serait pas soumise au droit commun de la négociation collective et concernerait les seules organisations syndicales signataires de l'accord (en ce sens *RJS 11/18 783 chron. Jeansen et Thuleau, « La publicité des accords collectifs, entre transparence et secret »).*

Enfin, ni la loi ni les dispositions réglementaires ne précisent les modalités d'adoption de l'acte de publication partielle dans le cas d'un accord conclu avec des représentants du personnel non mandatés par des organisations syndicales ou ratifié par les 2/3 du personnel sur la base d'une proposition de l'employeur. Un tel acte ne semble pas envisageable pour ces accords au regard des modalités de signature prévues par les textes.

Cependant, aucun texte de Loi n'est pour l'heure venu trancher ces questions et apporter des réponses aux interrogations qu'elles suscitent.

6) 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 du 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.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

Etude d'impact en France

«Les entreprise et la RDGP, enjeux, défis et conséquences»

Avant-propos

Le règlement général relatif à la protection des données 2016/679 du 27 avril 2016 (RGPD), qui est entré en vigueur depuis le 25 mai 2018, substitue au régime de formalités préalables prévu par la loi informatique et libertés, un système fondé sur la responsabilité des acteurs qui devront démontrer la conformité de leurs traitements à ce règlement à tout moment.

1) La particularité du règlement : une application directe et immédiate depuis le 25 mai 2018 dans tous les pays de l'UE sans nécessiter, contrairement à une directive, de transposition dans les différents Etats membres. Les traitements déjà mis en œuvre à cette date doivent être mis en conformité avec ses dispositions.

La Commission nationale informatique et libertés (Cnil), sur son site et dans plusieurs guides pratiques, analyse l'impact de l'entrée en vigueur de ce texte notamment pour les entreprises. Notre étude de cas reprendra donc le contenu des indications données par la CNIL concernant les relations entre les salariés et leur entreprise.

A noter :

Le RGPD s'applique à de multiples domaines et ne prévoit pas de règles particulières en matière de droit du travail laissant aux Etat-membres le soin de définir, sur ce point, les adaptations qu'ils jugent nécessaires. Le projet de loi relatif aux données personnelles définitivement adopté par le Parlement le 14 mai 2018 et modifiant la loi informatique et libertés (loi 78-17 du 6 janvier 1978) ne contient que peu de dispositions spécifiques aux relations de travail si ce n'est en matière de traitement de certaines données.

Notre étude d'impact vise donc à présenter les changements introduits par le RGPD en comparaison avec la législation antérieure.

2) Le passage de la notion de formalités préalables (déclaration, autorisations) contenue dans l'ancienne directive 95/46/CE du 24 octobre 1995 à une logique de conformité, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement de la CNIL via le nouveau règlement européen.

Les responsables de traitements doivent mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, dès la conception du produit ou du service et de façon continue, c'est-à-dire être en mesure de démontrer la conformité de leurs traitements tout moment.

La conséquence de cette responsabilisation des acteurs est la suppression des obligations déclaratives préalables.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

En effet, avant leur introduction dans l'entreprise, le CSE doit être informé sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci (article L 2312-38 du Code du travail).

Cette suppression des obligations déclaratives est susceptible de poser des difficultés en cas de litige. L'absence de déclaration obligatoire à la CNIL permettait à un salarié sanctionné ou licencié de se prévaloir de l'irrecevabilité de la preuve des faits qui lui étaient reprochés tirée d'un dispositif de contrôle non déclaré. Cela n'est désormais plus le cas.

3) Les établissements concernés par le RGPD : tout organisme, quels que soient sa taille, son pays d'implantation et son activité, peut être concerné.

En effet, le RGPD s'applique à toute organisation (publique ou privée), quels que soient sa taille, son pays d'implantation ou son activité dès lors qu'elle traite des données personnelles pour son compte ou non, et que :

- elle est établie sur le territoire de l'Union européenne ;
- son activité cible directement des résidents européens.

Exemple : une société établie en France, exportant l'ensemble de ses produits en dehors de l'Union européenne doit respecter le RGPD.

Le RGPD vise aussi les sous-traitants qui gèrent des données personnelles pour le compte d'autres organismes (des entreprises par exemple).

Les sous-traitants sont soumis à des obligations particulières : protection des données personnelles et de la vie privée dès la conception de leur service ou de leur produit, conseil auprès de leurs clients, tenue d'un registre des activités de traitement effectuées pour le compte de leurs clients. Le contrat de sous-traitance doit prévoir une clause spécifique sur la protection des données personnelles.

4) Les données concernées sont des données dites personnelles c'est à dire toute information permettant d'identifier directement (nom, prénom, par exemple) ou indirectement (numéro client, numéro de téléphone, numéro d'immatriculation pour la gestion d'un parking, donnée biométrique, etc.) une personne.

Une personne peut être identifiée à partir d'une seule donnée (ex : numéro de sécurité sociale) ou à partir du croisement d'un ensemble de données (personne vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association).

A noter :

Les adresses IP et Mac constituent des données personnelles (*Cass. 1e civ. 3-11-2016 n° 15-22.595 FS-PB).*

La collecte de certaines données doit donner lieu à une vigilance particulière, notamment celles ayant trait aux ayants-droit des salariés dans la mesure où elles peuvent renseigner sur leur orientation sexuelle.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

La notion de fichier recouvre tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique (ex : dossiers classés par ordre alphabétique ou chronologique).

Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement).

A noter :

Un fichier ne contenant que des coordonnées d'entreprises (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « compagnieA@email.fr ») n'est pas un traitement de données personnelles. Par ailleurs, un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent également être protégés.

Un traitement de données personnelles doit avoir un objectif, une finalité. Il n'est pas possible de collecter ou traiter des données personnelles simplement au cas où cela pourrait s'avérer utile un jour.

5) Les personnes visées par le RGPD

- Le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement et sur lequel reposent les obligations prévues par le règlement.

- La personne concernée par un traitement est celle à laquelle se rapportent les données objet du traitement.

- Le destinataire d'un traitement est toute personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers, ce dernier s'entendant de toute personne autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.

6) Les principes mis en place par le RGPD

Le règlement repose sur les principes selon lesquels les données à caractère personnel doivent être :

- traitées de manière licite, loyale et transparente au regard de la personne concernée ;

- collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ;

- adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

- exactes et tenues à jour ;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle (intégrité et confidentialité).

A noter :

Des actions concrètes doivent être mises en œuvre afin de respecter les principes mis en place par le RGPD :

- désigner un pilote ;
- recenser les fichiers ;
- repérer les traitements à risque ;
- respecter le droit des personnes ;
- sécuriser les données ;
- s'assurer, en cas de sous-traitance que le prestataire respecte le RGPD ;
- désigner un délégué à la protection des données

7) Le délégué à la protection des données (DPO) est obligatoire pour les organismes publics et les entreprises dont l'activité de base amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données dites sensibles ou relatives à des condamnations pénales et infractions.

Cependant, même si l'entreprise n'est pas formellement dans l'obligation de désigner un DPO, la CNIL recommande de désigner une personne disposant de relais internes, chargée de s'assurer de la mise en conformité au règlement européen.

Il est en charge de la conformité en matière de protection des données au sein de son organisme et est principalement chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- de contrôler le respect du règlement et du droit national en matière de protection des données ;
- de conseiller l'entreprise sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Le DPO peut être désigné en interne parmi les salariés de l'entreprise ou en externe. Il peut aussi être mutualisé entre plusieurs organismes ou au sein d'associations ou fédérations professionnelles.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

A noter :

La notion de traitement à grande échelle n'est pas définie par le RGPD c'est pourquoi la CNIL a donné des illustrations à cette notion de « traitement à grande échelle » : les traitements gérant les données des voyageurs utilisant les transports en commun ou ceux relatifs aux données de leurs clients administrés par les banques, les compagnies d'assurance, les opérateurs téléphoniques ou fournisseurs d'accès internet.

8) Le recensement des données pose l'obligation de tenir un registre des traitements des données personnelles.

Bien que cela ne concerne que les entreprises d'au moins 250 salariés, la CNIL en préconise la réalisation de manière plus large.

L'objectif est d'identifier les activités principales de l'entreprise qui nécessitent la collecte et le traitement de données (exemples en ce qui concerne la gestion des ressources humaines : le recrutement, la gestion de la paie, la formation, les déclarations sociales obligatoires, la gestion des badges et des accès, etc.).

Pour chaque activité, il faut répertorier :

- le responsable du traitement ;
- l'objectif poursuivi ;
- les catégories de données utilisées (exemple pour la paie : nom, prénom, date de naissance, salaire, etc.) ;
- les personnes ayant accès aux données (le destinataire - exemple : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs) ;
- la durée de conservation de ces données (durée pendant laquelle les données sont utiles d'un point de vue opérationnel et durée de conservation en archive).

Le registre est placé sous la responsabilité du dirigeant de l'entreprise.

Selon la CNIL, il n'est pas nécessaire de répertorier dans ce registre les traitements purement occasionnels tels les fichiers constitués pour une opération événementielle ponctuelle comme l'inauguration d'une boutique.

9) L'objectif assigné au responsable des traitements est de pouvoir prouver à tout moment que les traitements qu'il gère sont conformes à la réglementation.

Il est donc important de pouvoir déterminer la pertinence des données collectées et ce en vérifiant différents points :

- les circonstances de collecte des données : y-a-t-il eu consentement des personnes concernées ? Dans la négative la collecte répond-elle à des obligations particulières (collecte nécessaire au contrat, respect d'une obligation légale, par exemple le traitement de données relatives aux salariés pour les communiquer à la sécurité sociale ou l'administration fiscale…) ? ;
- la nature de l'information délivrée aux personnes faisant l'objet de la collecte et du traitement : celles-ci ont-elles été informées de la finalité du traitement et de leurs droits ? ;

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

- la nature des données collectées au regard de la finalité du traitement : seules les données strictement nécessaires au traitement peuvent être collectées et traitées.
- L'information relative au fait que seules les personnes habilitées ont accès aux données dont elles ont besoin et que les données ne sont pas conservées au-delà de ce qui est nécessaire.

10) Les cas spécifiques des traitements de données impliquant une vigilance accrue

Cela vise les traitements ayant pour objet ou pour effet :

- L'évaluation d'aspects personnels ou la notation d'une personne ;
- Une prise de décision automatisée ;
- La surveillance systématique de personnes : télésurveillance, surveillance des réseaux sociaux des salariés, analyse des pages des réseaux sociaux des candidats à un emploi, outils de gestion du temps de présence (badge, par exemple), systèmes de géolocalisation ;
- Le traitement de données sensibles. Sont concernées les données révélant l'origine prétendument raciale ou ethnique, portant sur les opinions politiques, philosophiques ou religieuses, relatives à l'appartenance syndicale, concernant la santé ou l'orientation sexuelle, les données génétiques ou biométriques, les données d'infraction ou de condamnation pénale ;
- Le traitement de données concernant des personnes vulnérables (exemple : mineurs) ;
- Des usages innovants ou l'application de nouvelles technologies (exemple : objet connecté) ;
- L'exclusion du bénéfice d'un droit, d'un service ou contrat.

Lorsque le traitement de données répond à au moins 2 de ces 9 critères, une analyse d'impact sur la protection des données (PIA : Privacy Impact Assesment) doit être conduite. La CNIL a mis en place un logiciel facilitant la conduite et la formalisation d'analyses d'impact : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

A noter :

L'article 8 du projet de loi relatif à la protection des données personnelles adopté par le Parlement le 14 mai 2018 interdit le traitement des données sensibles. Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne seront cependant pas soumis à cette interdiction notamment les traitements conformes à des règlements types établis par la CNIL mis en œuvre par les employeurs et portant sur des données biométriques strictement nécessaires au contrôle de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions confiées aux salariés, aux stagiaires ou aux prestataires.

Dans un souci de simplicité et d'accompagnement, la CNIL n'exigera pas la réalisation immédiate d'une analyse d'impact pour les traitements existants qui ont régulièrement fait l'objet d'une formalité préalable auprès de la CNIL avant le 25 mai 2018 (récépissé, déclaration de conformité à certaines normes, autorisation, avis de la CNIL), ou qui ont été consignés au registre d'un correspondant informatique et libertés.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

Les entreprises concernées disposent d'un délai de 3 ans à compter du 25 mai 2018 pour effectuer cette étude d'impact. Cette tolérance ne s'applique pas aux traitements, antérieurs au 25 mai 2018 et régulièrement mis en œuvre, mais qui ont fait l'objet d'une modification substantielle depuis l'accomplissement de leur formalité préalable.

11) 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.

12) L'information des salariés

Le support de collecte des données, quelle que soit sa nature (formulaire, questionnaire, etc.) doit comporter les informations listées ci-dessous :

- l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;
- le cas échéant, les coordonnées du délégué à la protection des données ;
- les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;
- les catégories de données à caractère personnel concernées ;
- le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel (service interne à l'entreprise, prestataire...) ;
- la durée de conservation des données ;
- les modalités selon lesquelles les intéressés peuvent exercer leurs droits (via leur espace personnel sur le site internet de l'entreprise, par un message sur une adresse email dédiée, par un courrier postal à un service identifié…) ;
- en cas de transfert de données hors de l'Union européenne, l'indication du pays concerné, l'existence ou l'absence d'une décision d'adéquation rendue par la Commission européenne ou la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition.

De plus, il est impératif que ces informations soient transmises :

- dès la collecte des données dans le cas où celle-ci sont recueillies directement auprès du salarié (lors de l'embauche, par exemple) ;

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

- au maximum un mois après cette collecte si les données sont recueillies de façon indirecte, auprès d'une autre source.

En revanche, ces informations n'ont pas à être fournies si le salarié en dispose déjà.

A noter :

Concernant les relations entre l'entreprise et ses salariés, la CNIL préconise d'informer ces derniers à chaque fois qu'il leur est demandé des informations (exemples : mises à jour de données administratives, demande de formation, formulaire d'entretien d'évaluation etc.) ou lors de la mise en place d'un dispositif de surveillance, selon des modalités à déterminer selon l'organisation de l'entreprise (note de service, avenant au contrat de travail, information sur l'Intranet, courrier joint au bulletin de paie etc.)

13) Garantir et renforcer les droits des salariés sur leurs données : 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 projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

14) La sécurisation des données vise les mesures à prendre, informatiques ou physiques, et dépend de la sensibilité des données traitées et des risques qui pèsent sur les personnes en cas d'incident.

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.

15) Un encadrement et un renforcement de l'échelle des sanctions impliquant que 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.

16) Le contrôle opéré par la CNIL du respect du RGPD depuis le 25 mai 2018 23 consiste à procéder à des vérifications dans les locaux des organismes, en ligne, sur audition et sur pièces. Les modalités de déclenchement des contrôles restent également les mêmes : 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.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

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.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

Etude d'impact en France

«Avec le RGPD, la protection des données s'applique aussi aux syndicats»

Avant-propos

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.

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.).

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.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

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.

3 étapes pour élaborer le registre des activités de traitement :

- 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.

Ainsi, les salariés sont en mesure d'exiger de la part du CSE :

- L'accès aux informations les concernant ;
- La rectification de leurs données personnelles ;

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

- 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.

Exemples des possibilités d'implication des syndicats et représentants du personnel :
- 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.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

ANNEXE 1

EXEMPLE DE REGISTRE

Pour faciliter la tenue du registre, la CNIL propose un modèle de registre de base destiné à répondre aux besoins les plus courants en matière de traitements de données, en particulier des petites structures.

Ce document vise à recenser les traitements de données personnelles mis en œuvre dans votre organisme **en tant que responsable de traitement**. Centralisé et régulièrement mis à jour, il vous permet de répondre à l'obligation de tenir un registre prévue par le RGPD.

Une fois ce recensement effectué, vous serez en mesure de procéder à l'analyse des traitements de données personnelles à la règlementation.

Composition du document

1) La page 2 du registre recense les informations communes à toutes vos activités de traitement.

Les coordonnées de votre organisme (ou de son représentant sur le territoire européen si votre organisme n'est pas établi dans l'Union européenne).
Les coordonnées du délégué à la protection des données (DPO) si vous en disposez.
La liste des activités de votre organisme impliquant le traitement de données personnelles.

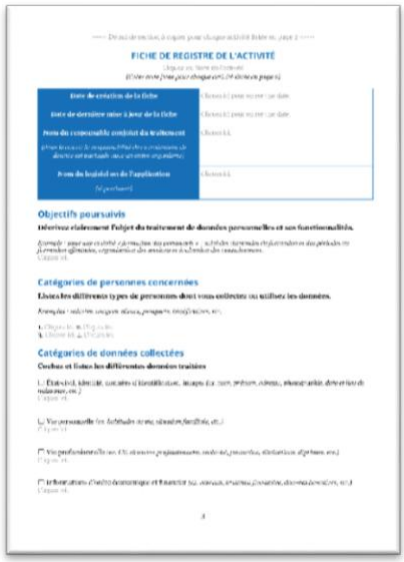

REGISTRE DES ACTIVITÉS DE TRAITEMENT DE

Activités de l'organisme impliquant le traitement de données personnelles

Activités	Désignation des activités
Activité 1	
Activité 2	
Activité 3	
Activité 4	
Activité 5	
Activité 6	
Activité 7	
Activité 8	

2) Pour chaque activité recensée, vous devrez créer et tenir à jour une fiche de registre (page 3 à 6).

Les pages suivantes constituent le modèle de fiche de registre, que vous devrez remplir pour chacune de ces activités.


FICHE DE REGISTRE DE L'ACTIVITÉ

Objectifs poursuivis

Catégories de personnes concernées

Catégories de données collectées

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

REGISTRE DES ACTIVITÉS DE TRAITEMENT DE

Cliquez ici. Nom de l'organisme

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	Nom : Cliquez ici. Prénom : Cliquez ici. Adresse : Cliquez ici. CP : Cliquez ici. Ville : Cliquez ici. Téléphone : Cliquez ici. Adresse de messagerie : Cliquez ici.
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	Nom : Cliquez ici. Prénom : Cliquez ici. Société (si DPO externe) : Cliquez ici. Adresse : Cliquez ici. CP : Cliquez ici. Ville : Cliquez ici. Téléphone : Cliquez ici. Adresse de messagerie : Cliquez ici.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

Activités de l'organisme impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

Activités	Désignation des activités
Activité 1	Cliquez ici. ex. Gestion de la paie
Activité 2	Cliquez ici. ex. Gestion des prospects
Activité 3	Cliquez ici. ex. Gestion des fournisseurs
Activité 4	Cliquez ici. ex. Vente en ligne
Activité 5	Cliquez ici. ex. Sécurisation des locaux
Activité 6	Cliquez ici.
Activité 7	Cliquez ici.
Activité 8	Cliquez ici.

Vous devrez créer et tenir à jour une fiche de registre par activité.
Le modèle de fiche de registre est disponible sur la page suivante, copier / coller autant de fois la sélection qu'il y a d'activité listée.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

----> Début de section à copier pour chaque activité listée en page 2 <----

FICHE DE REGISTRE DE L'ACTIVITÉ

Cliquez ici. Nom de l'activité

(Créer cette fiche pour chaque activité listée en page 2)

Date de création de la fiche	Cliquez ici pour entrer une date.
Date de dernière mise à jour de la fiche	Cliquez ici pour entrer une date.
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	Cliquez ici.
Nom du logiciel ou de l'application *(si pertinent)*	Cliquez ici.

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.
Cliquez ici.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

Catégories de données collectées

Cochez et listez les différentes données traitées

- État-civil, identité, données d'identification, images *(ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)*
Cliquez ici.

- Vie personnelle *(ex. habitudes de vie, situation familiale, etc.)*
Cliquez ici.

- Vie professionnelle *(ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)* Cliquez ici.

- Informations d'ordre économique et financier *(ex. revenus, situation financière, données bancaires, etc.)* Cliquez ici.

- Données de connexion *(ex. adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)*
Cliquez ici.

- Données de localisation *(ex. déplacements, données GPS, GSM, …)*
Cliquez ici.

- Internet *(ex. cookies, traceurs, données de navigation, mesures d'audience, …)*
Cliquez ici.

- Autres catégories de données *(précisez)* :
Cliquez ici.

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

☐ Oui ☐ Non

Si oui, lesquelles ? :
Cliquez ici.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

Cliquez ici. Jours, Cliquez ici. Mois, Cliquez ici. Ans, Autre durée : Cliquez ici.

Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (par exemple, 3 ans à compter de la fin de la relation contractuelle).
Cliquez ici.

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Destinataires internes

(Exemples : entité ou service, catégories de personnes habilitées, direction informatique, etc.)

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

Organismes externes

(Exemples : filiales, partenaires, etc.)

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

Sous-traitants

(Exemples : hébergeurs, prestataires et maintenance informatiques, etc.)

1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

9) Oui ☐ Non

Si oui, vers quel(s) pays :

Cliquez ici.

Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD). Consultez le site de la CNIL.

Mesures de sécurité

Cochez et décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

- Contrôle d'accès

des utilisateurs

Décrivez les mesures :

Cliquez ici.

- Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs),* les données enregistrées
(exemple : identifiant, date et heure de connexion, etc.) et leur durée de conservation :

Cliquez ici.

10) Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.) Décrivez les mesures :

Cliquez ici.

11) Sauvegarde des données

Décrivez les modalités :

Cliquez ici.

- Chiffrement des données

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057

Décrivez les mesures (*exemple : site accessible en https, utilisation de TLS, etc.)* :

Cliquez ici.

- Contrôle des sous-

traitants Décrivez les

modalités :

Cliquez ici.

- Autres mesures :

Cliquez ici.

----> Fin de section à copier pour chaque activité listée en page 2 <----

Le projet est cofinancé par la DG Emploi de la Commission européenne. Accord no. VS / 2019/0057