RGPD : une nécessaire vigilance s'impose

Audrey PROBST
Avocat of counsel
Fromont Briens

Le comité social et économique n'échappant pas aux règles du RPGD, son président doit participer au respect de la réglementation et à la diffusion des bonnes pratiques.

RGPD ET CSE

Depuis l'entrée en vigueur du Règlement européen n° 2016/679 du 27 avril 2016 « *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* » (RGPD), et sa transposition en droit français par la loi du 20 juin 2018 [(1)], le comité social et économique (CSE) doit adapter ses pratiques aux fins de se conformer aux obligations prescrites par ce règlement. En effet, si les comités d'entreprise avaient été dispensés par la Cnil de déclaration préalable, les CSE n'échapperont pas totalement au RGPD.

Le RGPD s'applique en effet « *au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* ». La définition retenue par le RGPD est particulièrement large dans la mesure où une donnée à caractère personnel est définie comme « *toute information se rapportant à une personne physique identifiée ou identifiable* », et qu'un traitement est réalisé par « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ». Autrement dit, la simple collecte et la conservation, même non automatisées, d'informations se rapportant à des per-

(1) L. n° 2018-493, 20 juin 2018, relative à la protection des données personnelles.

sonnes physiques identifiables entrainent l'application des obligations imposées par le RGPD.

Le CSE est donc bien évidemment concerné.

Il est en effet amené à traiter des données à caractère personnel, collectées dans le cadre de la gestion des activités sociales et culturelles (ASC), de l'administration du personnel qu'il emploie, voire dans celui d'enquêtes qu'il peut être amené à décider en matière de santé et de sécurité. L'application du RGPD sera plus rarement concernée par l'exercice des prérogatives économiques du CSE, les données traitées dans ce cadre n'étant pas, en principe, individuelles. Selon la taille des entreprises, le CSE peut donc avoir à traiter des données à caractère personnel de plusieurs dizaines, de plusieurs centaines, voire de plusieurs milliers de personnes (âge, adresse des salariés et des membres de leur famille, état de santé, informations bancaires…).

Quel est alors le rôle du président du CSE et que doit-il faire ?

RÔLE DU PRÉSIDENT

Le président du CSE est-il pleinement responsable de l'application du RGPD au sein du CSE ? On peut légitimement se poser la question.

En effet, le président du CSE, par ailleurs représentant de l'employeur, ne peut pas s'immiscer dans les attributions du CSE en tant que délégation du personnel. Aux termes de l'article L. 2325-18 du Code du travail, il ne participe pas au vote lors des consultations du CSE en tant que délégation du personnel.

Rappelons également que le CSE dispose du monopole de la gestion des activités sociales et culturelles et que toute interférence de l'employeur dans ce domaine constitue un délit d'entrave. Le CSE peut donc librement choisir telles ou telles activités [(2)], sans que son président ne puisse s'y opposer (il ne participe en effet pas aux votes qui les valident).

Cela ne dispense toutefois pas ce dernier, en tant que membre du CSE, de veiller à l'application du RGPD, qui relève en effet du fonctionnement interne du CSE. Le président du CSE a donc son mot à dire.

(2) Voir par exemple Cass. soc., 8 janv. 2002, n° 00-10.818.

Remarque

Il pourrait également être co-responsable, au même titre que les autres membres du CSE, en cas de violation du règlement.

Le président du CSE a donc intérêt à s'assurer du respect du RGPD, d'autant que les personnes concernées sont généralement les salariés de l'entreprise qu'il représente. Il va ainsi devoir assumer les deux casquettes.

Il lui reviendra donc :

– d'une part, en tant que représentant de l'employeur, de veiller, par exemple, à ce que les salariés soient dûment informés de l'éventuelle transmission de leurs données au CSE (information sur la finalité de cette communication, sur la nature des informations les concernant et des modalités prévues pour s'opposer, le cas échéant, à cette transmission) ;

– d'autre part, de sensibiliser les membres du CSE à l'importance du respect des principes du RGPD afin d'assurer les droits des salariés et la sécurité de leurs données, voire s'opposer à des pratiques qui manifestement les violeraient.

METTRE EN ŒUVRE LE RGPD AU SEIN DU CSE

Principes à respecter

L'application du RGPD au sein du CSE suit les mêmes principes que ceux applicables à tout organisme similaire. En substance, le RGPD entraine l'obligation de respecter les principes suivants.

Licéité du traitement

Le traitement de données à caractère personnel suppose en premier lieu que cette gestion soit licite, c'est-à-dire qu'elle repose :

– soit sur le consentement libre et éclairé de la personne concernée ;

– soit sur l'exécution d'un contrat ;

– soit sur le respect d'une obligation légale ;

– soit sur l'exécution d'une mission d'intérêt public ;

– soit sur la poursuite de l'intérêt légitime du CSE.

Le fondement du traitement doit pouvoir être à chaque fois identifié. Bien souvent, il répondra à la poursuite de l'intérêt légitime du CSE dans le cadre de la gestion des activités sociales et culturelles.

Finalité du traitement

La finalité du traitement doit être déterminée, explicite et légitime.

À titre d'exemple, il pourra s'agir de la gestion des activités (chèques cadeaux, billetterie, sports, voyages…), de la crèche, l'adhésion à des clubs, l'historique des commandes, l'historique de l'utilisation des subvention…

« Minimisation » des données collectées

Il est ici question de faire application de l'ancien principe de proportionnalité au regard de la finalité recherchée. Bien évidemment, les données collectées doivent être strictement nécessaires à l'objectif poursuivi. Si certaines données anciennement collectées par le CSE n'apparaissent pas nécessaires, il conviendra naturellement de les effacer et de ne plus en collecter de similaires.

Durée de conservation des données

Le CSE devra être vigilant et correctement identifier, pour chaque traitement, la durée de conservation des données qui ont été collectées, laquelle ne pourra pas être supérieure à celle durant laquelle le bénéficiaire est susceptible de bénéficier de la prestation, augmenté des délais de prescription et des délais de procédure en cas de contentieux. Une conservation des données au-delà de ces délais seraient excessive et injustifiée.

Sécurité des données à caractère personnel

En application de l'article 32 du RGPD, le CSE doit mettre en œuvre « *les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ».

Cela suppose d'analyser le risque traitement par traitement, dans la mesure où il peut différer d'un traitement à l'autre. En cas de violation de données, la Cnil devra en être informée dans les 72 heures, et la ou les personnes concernées, sans délai, si la violation présente un risque élevé pour les droits et libertés (coordonnées bancaires, données sensibles…).

Transparence et information des personnes concernées

Les personnes concernées par le traitement de leurs données à caractère personnel doivent être informées de toute une série d'éléments, qui diffère selon que la collecte a eu lieu directement auprès d'elles, ou par l'intermédiaire d'un autre responsable de traitement. La liste des informations à fournir est fixée aux articles 13 et 14 du RGPD.

Respect des droits des personnes concernées

Comme tout responsable de traitement, le CSE devra veiller au respect :

– du droit d'opposition ;

– du droit d'accès et de rectification ;

– du droit à la portabilité des données ;

– du droit à l'effacement de ses données (droit à l'« *oubli* »).

Le respect de ces droits suppose d'avoir, au préalable, identifié les traitements opérés et les données collectées. À défaut, le CSE pourrait être dans l'impossibilité, par exemple, de transférer, à la demande d'un salarié, l'ensemble de ses données au CSE de son nouvel employeur…

Actions clé à mener

Désigner un délégué à la protection des données (DPD ou DPO)

Selon les dispositions de l'article 37 du RGPD, un DPD (DPO en anglais) doit être désigné, notamment lorsque « *les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées* », ou lorsque « *les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9* [ndlr : dont l'appartenance syndicale, les données concernant la santé, l'orientation sexuelle….] *et de données à caractère personnel relatives à des condamnations pénales et à des infractions* ».

La problématique revient à s'interroger sur ce que recouvre un « *traitement à grande échelle* ».

La réponse à cette question varie d'un CSE à l'autre en fonction :

– du nombre de personnes concernées (effectif salarié de l'entreprise) ;

– du volume de données traitées (types de traitement mis en œuvre, nombre et catégorie de données collectées) ;

– de la durée ou de la permanence de l'activité de traitement ;

– et de la répartition géographique du traitement.

En conséquence, il apparait difficile, pour les CSE d'entreprises d'une taille conséquente, gérant des activités sociales et culturelles en nombre et nécessitant le traitement de données à caractère personnel, d'échapper à la désignation d'un DPO, tant d'un point de vue juridique que pour des questions pratiques. Le DPO se chargera en effet d'assurer la conformité des traitements au RGPD et de répondre aux demandes des personnes concernées et le cas échéant de la Cnil.

Remarque

Sous réserve de ne pas se retrouver en situation de conflit d'intérêts, le DPO désigné pourra, éventuellement, être le même que celui mis en place dans l'entreprise.

En pratique, le DPO sera désigné par une délibération du CSE. À notre sens, le président pourra prendre part au vote, la désignation du DPO relevant du fonctionnement interne du CSE.

Il n'existe pas de profil type du DPO, qui peut être un salarié du CSE ou un intervenant externe, et être désigné pour une durée déterminée (celle des mandats, par exemple) ou pour une durée indéterminée.

En revanche, il devra être choisi *« sur la base de ses qualités professionnelles et, en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir* [ses] *missions »* [3]. Il conviendra donc de bien vérifier son niveau de compétences, notamment juridique, et de sa maîtrise des systèmes d'information.

On veillera également, bien évidemment, à lui accorder les moyens suffisants pour exercer sa mission (temps, moyens matériels et humains, informations adéquates et accès aux données, indépendance).

(3) RGPD, art. 37.5.

Remarque

La désignation du DPO auprès de la Cnil peut se faire directement en ligne sur le site Internet *cnil.fr*.

Tenir le registre des activités de traitements

Entreprises de 250 salariés et plus

Le CSE doit tenir un registre des activités de traitement comportant, conformément aux dispositions de l'article 30 du RGPD, les informations suivantes :

– le nom et les coordonnées du responsable du traitement et, le cas échéant, du DPD ;

– les finalités des traitements ;

– une description des catégories de personnes concernées et des catégories de données à caractère personnel ;

– les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées ;

– le cas échéant, les transferts de données à caractère personnel vers un pays tiers ;

– les délais prévus pour l'effacement des différentes catégories de données ;

– une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre.

Entreprises de moins de 250 salariés

Elles bénéficient d'une dérogation en ce qui concerne la tenue de registres. Seuls doivent y être inscrits les traitements de données suivants :

– les traitements non occasionnels ;

– les traitements susceptibles de comporter un risque pour les droits et libertés des personnes ;

– les traitements qui portent sur des données sensibles.

Un registre de traitement des activités de traitements devrait donc en principe exister au sein des CSE, et pourra servir, en cas de contrôle de la Cnil, à démontrer la conformité des traitements au RGPD.

L'élaboration du registre est donc une étape importante à ne pas négliger.

DISPENSE D'ANALYSE D'IMPACT À RÉALISER

Aux termes de l'article 35 du RGPD, lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

En application de l'article 35.5 du RGPD, la Cnil a cependant dispensé les CSE de l'obligation de réaliser une analyse d'impact [4]. Les obligations du CSE sont donc allégées sur ce point.

L'ensemble de ces questions, relevant du fonctionnement interne du CSE, devraient être étudiées au plus tôt afin de mettre en œuvre une organisation conforme au RGPD. En tant que membre du CSE, le président doit bien évidemment également s'emparer de cette question.

(4) Délib. CNIL n° 2019-118, 12 sept. 2019, portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise.