RGPD

QUELLES SONT LES OBLIGATIONS DU CSE ?

Bons d'achat, voyages, réductions tarifaires en matière de spectacles ou de sports, secours… Dans le cadre du fonctionnement des activités sociales et culturelles au profit des salariés, le CSE collecte, utilise des informations personnelles et doit se conformer au Règlement général sur la protection des données (RGPD). Un mode d'emploi à l'attention de tous les élus de CSE…

Dans un monde surconnecté au sein duquel les données et leur traitement se multiplient à un rythme effréné, les enjeux de la protection des données à caractère personnel prennent tout leur sens. Paiements sur Internet, réseaux sociaux, marketing, dématérialisation, digitalisation, questionnaires en ligne… Nous sommes profilés de façon toujours plus précise. Et aujourd'hui, plus que jamais, la préservation de la vie intime est devenue un véritable enjeu, notamment en ce qui concerne la collecte des données personnelles sur Internet et leur exploitation à des fins mercantiles. Le constat fut le suivant : il n'y avait plus de visibilité sur l'utilisation de ce qui était fait de nos données, ni pourquoi, ni par qui. Le consentement qui devrait être la base d'un grand nombre de traitements n'était que trop peu souvent respecté, de la même manière que les droits et libertés des individus. Alors comment est apparu le Règlement général sur la protection des données (RGPD) ?

Le saviez-vous ?

La Cnil propose sur son site un modèle de registre de traitement de données, dont la construction répond aux besoins standards d'un organisme. Chacun peut l'étoffer en fonction de sa politique.

Comprendre l'apparition du RGPD

Dépassées par l'évolution des normes technologiques, les anciennes directives européennes et législations nationales (en France, la loi Informatique et Liber-


Par Ronan Darchen, cofondateur Alinea


Rémy Poulain, juriste social Alinea

tés) sur la protection de la vie privée ne s'avéraient plus efficaces et ne permettaient plus d'assurer un traitement satisfaisant des données à caractère personnel. Face à l'utilité économique de nos données, de leur collecte et de leur transfert pour les entreprises, un règlement européen était devenu indispensable. Ainsi, le RGPD a été adopté par le Parlement européen en 2016 et est entré en vigueur le 25 mai 2018. Il érige un cadre légal de la protection des données à caractère personnel pour l'Europe. Le RGPD s'inscrit dans la continuité de la loi française Informatique et Libertés de 1978 en établissant des règles sur la collecte et l'utilisation des données sur le territoire français. En réalité, il ne s'agit pas d'interdire ou d'empêcher les évolutions technologiques liées à la data. Il s'agit, en revanche, de responsabiliser les acteurs en les invitant à mettre en place la documentation nécessaire permettant de démontrer leur conformité aux exigences sur la protection des données, droits et libertés des personnes physiques et les intérêts de tous.

Le RGPD a été conçu autour de trois objectifs : renforcer les droits des personnes dont les données sont recueillies et les droits qu'elles peuvent exercer (par exemple : les rectifier ou les effacer), responsabiliser les acteurs traitant des données (responsables de traitement, sous-traitants) qui doivent désormais être en mesure de démontrer la conformité de leurs traitements avec les dispositions du règlement européen à tout moment, sous le contrôle et avec l'accompagnement de la Commission nationale de l'informatique et des libertés (Cnil). Et enfin, dernier objectif : garantir une régulation grâce à une coopération renforcée entre les autorités de la protection. Mais on ne peut appréhender la mise en place du RGPD si on ignore ce que recouvre la notion de « donnée personnelle ».

Qu'est-ce qu'une donnée personnelle ?

La Cnil définit à l'article 4 du RGPD une donnée à caractère personnel comme *« toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement »*.

Il s'agit donc d'une information associée à un individu et/ou pouvant permettre son identification, et ce, peu importe que ces informations soient confidentielles ou publiques : noms, prénoms, photos, adresse électronique (e-mail), adresse IP, empreintes digitales, vidéos, enregistrements, mots de passe, numéros d'identifiant, numéro de sécurité sociale, plaque d'immatriculation, etc.

La compilation de ces différentes données peut permettre à des tiers d'établir une position géographique, des préférences ou des comportements de personnes ciblées ; ce qui constitue une potentielle atteinte à leur vie privée. C'est pourquoi une structure ne doit pas rechercher ▶▶

CONSERVATION DES DONNÉES

Une illustration avec un cas pratique

Dans le cadre de la rénovation de son parc informatique, une société confie au CSE l'organisation d'une donation d'ordinateurs au bénéfice de salariés choisis selon des critères définis par les élus (niveau de revenus, bénéficiaires d'aides sociales, charges de famille…). La liste des bénéficiaires et de ceux sur la liste d'attente se retrouve en libre accès sur l'Intranet de l'entreprise. Des éléments permettant d'identifier les collaborateurs, et notamment leurs charges de famille, sont alors au vu et au su de tous. Il faut donc retirer cette liste de l'Intranet. En réalité, seuls les membres du CSE chargés de l'opération doivent y avoir accès.

▶▶ ni détenir d'informations personnelles sans pouvoir le justifier auprès de la Cnil ; elles servent impérativement un objectif professionnel (sondages, mises à jour de fichiers RH, etc.).

Toutes les données personnelles se valent-elles ?

La réponse est non. Parmi toutes les données à caractère personnel qui peuvent exister, certaines bénéficient d'une protection particulière car elles touchent à des informations qui peuvent donner lieu à des agissements discriminatoires ou à la persistance des préjugés : la personne peut se retrouver à tort « cataloguée » à mauvais escient. Cette catégorie particulière regroupe les données sensibles, une catégorie particulière qui regroupe les opinions politiques, les croyances religieuses, les sensibilités philosophiques, l'orientation sexuelle, l'engagement syndical ou lié au militantisme associatif, l'appartenance ethnique, la situation médicale, les condamnations et infractions pénales, les données biométriques, les informations génétiques. Elles font l'objet d'un cadre protecteur renforcé. Pour saisir toute l'importance accordée à la protection de ces données sensibles, il suffit de lire l'article 226-19 du Code pénal qui prévoit jusqu'à cinq ans de prison et 300 000 euros d'amende *« le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé »* ce type de données. Si le texte ne parle pas de données sensibles, c'est bien d'elles qu'il s'agit. Ainsi, rappelle la Cnil, la règle générale est l'interdiction du traitement.

La loi a cependant prévu des exceptions : nécessité pour la sauvegarde de la vie humaine, si les informations ont été manifestement rendues publiques par la personne concernée ; si un consentement a été donné dans le cadre d'une *« démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée »* (source Cnil). Ou encore si cela est justifié par l'intérêt public et autorisé par la Cnil. De fait, des données personnelles peuvent ne plus l'être, si des processus irréversibles les ont rendues anonymes. Cela peut se matérialiser par un visage flouté ou nom masqué. Dès lors, ces données perdent leur statut de « donnée personnelle » et ne sont plus « RGPD dépendantes ». Tout l'enjeu est évidemment d'être certain que ce qui est annoncé comme irréversible l'est vraiment. Une donnée personnelle, qu'elle soit récoltée, étudiée, utilisée ou stockée, voire si elle transite par toutes ces étapes, est considérée comme traitée. Le format n'importe pas aux yeux de la Cnil : que ce soit sur support manuscrit ou numérique, ces informations sont détenues, ce qui implique la mise en place d'une politique

> **Le RGPD a été conçu autour de 3 objectifs : renforcer les droits des personnes dont les données sont recueillies et les droits qu'elles peuvent exercer (rectifier ou effacer) ; responsabiliser les acteurs traitant des données qui doivent désormais être en mesure de démontrer la conformité de leurs traitements avec les dispositions du règlement européen à tout moment, sous le contrôle et avec l'accompagnement de la Cnil ; garantir une régulation grâce à une coopération renforcée entre les autorités de la protection »**

© jcomp / Freepik

RGPD adéquate. Des données personnelles peuvent être traitées dans le cadre de la diffusion d'une enquête au sein du personnel dans l'optique de négocier un accord d'entreprise, de mettre en place des équipements dans la société (crèche d'entreprise, installations sportives, par exemple). Bref, les CSE sont aussi concernés !
Nom, prénom, date de naissance, sexe, famille, adresse postale, courriel, coordonnées bancaires, quotient familial, avis d'imposition… En sa qualité de responsable de traitement, le CSE doit être en mesure de démontrer la conformité du traitement des données collectées aux dispositions du RGPD du 27 avril 2016 et à la loi Informatique et Libertés du 6 janvier 1978 à tout moment. Les CSE sont en effet garants de toutes les données à caractère personnel, dès leur collecte, ainsi que de l'usage qui en sera fait, afin d'éviter leur accès à des personnes non autorisées. Mais parfois les élus se trouvent démunis face à cette réglementation qui leur semble opaque. Alors, comment adopter les bons réflexes pour être « RGPD compatibles » ? Un traitement à caractère personnel couvrira toute opération portant sur des données personnelles, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion, ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Mise en conformité du CSE : les grands principes

Le CSE doit garantir aux salariés que les données personnelles recueillies ne seront pas accessibles à des personnes non autorisées et qu'il n'en sera fait aucun usage à des fins détournées. À ce titre, l'application du RGPD leur impose le respect de 5 grands principes pour protéger ces données :

- D'abord, le principe de finalité : le CSE ne peut conserver et utiliser les données personnelles d'une personne physique que dans un but précis, légal et légitime. Pour un CSE, la gestion des activités sociales et culturelles est un but précis et légitime mais il ne peut conserver ni recenser d'autres informations qui ne seraient pas utiles à cette fin.
- Deuxième et troisième principe : celui de proportionnalité et de la pertinence : le CSE ne peut détenir plus de données que celles nécessaires à la réalisation des prestations.
- Les élus devront aussi respecter le principe de durée de conservation limitée (le 4e). Le CSE ne peut pas garder une donnée personnelle de manière indéfinie, sa durée de conservation doit être fixée à l'avance puis supprimée au-delà de ce temps prévu. La loi sur la transparence financière des CSE exige une conservation des pièces justificatives durant dix ans mais les informations relatives aux bénéficiaires des ASC pourraient se limiter à trois ans en cohérence avec le potentiel contrôle Urssaf.
- Le quatrième principe relève de la sécurité et la confidentialité : les données détenues ne doivent pas pouvoir être accessibles à autrui et seules les personnes autorisées, habilitées par le CSE, doivent y avoir accès. Le CSE est garant des données qu'il possède et en assume la responsabilité. Il a l'obligation de renforcer le niveau de sécurité des applications supportant les traitements des ▶▶

▶▶ données personnelles. Le règlement intérieur du CSE pourra indiquer qui sont les gardiens des informations.

• Le cinquième et dernier principe est la reconnaissance du droit des personnes qui comprend le droit d'information, le droit d'accès, de modification, de suppression des données.

Les actions à mettre en place par les CSE

L'application du RGPD au sein du CSE nécessite un recensement de l'ensemble des données déjà en sa possession. Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente. Le CSE peut donc « cartographier » l'ensemble des données dont il dispose. Ainsi, la première étape consiste à recenser chaque activité ou prestation délivrée par le CSE nécessitant la collecte de données à caractère personnel et de s'assurer désormais du consentement des personnes à partager leurs données personnelles, à appliquer pour chaque activité sociale et culturelle les cinq grands principes énoncés plus haut, puis se poser la question de la destruction des données à caractère personnel dont le CSE n'a plus besoin.

Selon l'article 30 du RGPD, la tenue d'un registre au format manuscrit ou numérique, et à jour, faisant l'inventaire de tous les fichiers de données personnelles utilisés par le CSE, activité par activité, n'est pas obligatoire, mais elle est vivement préconisée. Un inspecteur de la Cnil y trouvera les noms des membres du CSE participant directement ou indirectement au traitement des données, les noms des personnes ayant un accès à ce fichier. Seront identifiés les tiers à qui les données sont éventuellement transférées (le prestataire du CSE souvent), les types de données recueillies, leur finalité et durée de conservation, les mesures de sécurisation adoptées. Les membres du CSE découvriront le bilan de leurs pratiques en matière de collecte et d'accumulation de données parfois sensibles. Tous les sous-traitants ont l'obligation d'ouvrir et d'actualiser un tel registre. Il sera ainsi aisément prouvé en cas de litige que les données partagées par le CSE ont été protégées et employées à bon escient.

Pour garantir la transparence et le consentement, le CSE doit mettre un point d'honneur à avertir les salariés dès qu'il procède à une collecte de données. Cela peut, par exemple, prendre la forme d'un bandeau informatif en introduction d'un formulaire en ligne et d'une case à cocher pour signifier son accord envers la communication de données. Le responsable du traitement sera, de plus, en mesure de prouver la régularité des procédés en cas de contrôle de la Cnil. Quel que soit le support de collecte utilisé (formulaire, questionnaire, etc.), celui-ci doit comporter l'identité et les coordonnées du responsable du traitement ou les coordonnées du délégué à la protection des données ; la mention des finalités du traitement, la durée de conservation des données ; les droits des salariés concernés à la rectification et la suppression de leurs données et les modalités selon lesquelles ils peuvent les exercer (via leur espace personnel sur le site internet de l'entreprise, par un message sur une adresse e-mail dédiée, par un courrier postal à un service identifié…).

Les droits des salariés sur leurs données sont les suivants : droit d'accès, de rectification, d'effacement, de portabilité de leurs données, d'opposition et de limitation de leur utilisation (règlement UE 2016/679 art. 15 à 18 et 20). Ce qui est important, c'est de rappeler leurs droits à vos collègues, à savoir l'accès aux informations les concernant, la possibilité de rectification des données personnelles ou leur suppression s'ils le souhaitent. Tout salarié peut aussi s'opposer à ce que son employeur adresse au CSE des données qui le concernent. Leur transmission au CSE ne peut être que facultative ; le salarié devant être alors clairement informé des conséquences d'un éventuel refus de sa part. Par exemple, l'application du tarif le plus élevé ou exclusion du bénéfice d'une prestation, dans le cadre des activités sociales et culturelles.

Sécuriser les données traitées et désigner un délégué

Le CSE doit également veiller à assurer la sécurité des données personnelles en prenant des mesures telles que la mise à jour des logiciels et de l'antivirus, le changement régulier des mots de passe, la création de différents profils utilisateurs, la sécurisation du local du comité, la vérification des contrats conclus avec les prestataires. En cas de violation des données (quand des données personnelles ont été détruites, perdues, altérées, divulguées, de manière accidentelle ou illicite ou si, encore, il a été constaté un accès non autorisé à des données), il est tenu, comme tout responsable de traitement, de le signaler à la Cnil dans les soixante-douze heures si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées (règlement UE 2016/679 art. 33). Cette notification s'effectue en ligne sur le site internet de la Cnil. Les personnes concernées dont les données ont été potentiellement mises en danger doivent être averties.

Le CSE peut aussi nommer son délégué à la protection des données (DPO : Data Protection Officer) en charge de s'assurer que l'ensemble des fiches de traitement est finalisé. Il examinera les pratiques de collecte et les mesures retenues de protection des données. Il sera un interlocuteur privilégié des autorités en situation d'inspection, et de manière générale vis-à-vis de toute personne concernée par le RGPD. En pratique, ce rôle peut être assuré par un élu du CSE (membre du bureau ou non). Rien n'interdit que le CSE s'appuie sur les compétences du DPO de l'entreprise. Au boulot, si vous n'êtes pas déjà à jour du RGPD ! ■

BON À SAVOIR

RGPD : quelles entreprises concernées ?

Le règlement s'applique à toute entreprise, publique et privée, qui traite des données personnelles pour son compte ou non, si :

• elle est établie sur le territoire de l'Union européenne ;

• et/ou si son activité cible directement des résidents européens.

Par exemple, une société établie en France qui exporte l'ensemble de ses produits en dehors de l'Union européenne doit respecter le RGPD. De même, une société établie en dehors de l'Union européenne proposant un site d'e-commerce en français livrant des produits en France doit respecter le RGPD.