Les fiches pratiques Syndex

Janvier 2019

RGPD : un nouveau droit à faire respecter pour les élus

Depuis le 14 mai 2018, le réglement général sur la protection des données (RGPD) s'impose à toutes les structures gérant des informations à caractère personnel. Cela concerne les représentants des salariés, qui ont leur mot à dire sur les procédures appliquées par leur entreprise et sont eux-mêmes sousmis à des obligations.

#1 SUPPRESSION DES DÉCLARATIONS PRÉALABLE AUPRÈS DE LA CNIL CONTRE UN POUVOIR DE SANCTION RENFORCÉE

Issu du règlement européen du 27 avril 2016 sur la protection des données, le RGPD introduit de nouvelles dispositions. Tout en reprenant les principes déjà applicables, il met fin aux déclarations préalables auprès de la CNIL. L'idée majeure de ce texte est de responsabiliser les détenteurs de données personnelles en les obligeant à rapporter la preuve qu'ils ont respecté la loi. Les entreprises doivent donc mettre en place un système d'autocontrôle continu de façon à être en mesure de prouver qu'elles respectent les règles de protection des données.

Le pouvoir d'enquête et le pouvoir de sanction de la CNIL sont renforcés. Ainsi la CNIL vérifie que les caractéristiques des traitements concernés sont bien conformes à la loi et au droit européen et peut désormais condamner les entreprises à une amende.

#2 QUELS SONT LES PRINCIPES QUE L'EMPLOYEUR DOIT RESPECTER ?

Les entreprises doivent être en mesure de prouver qu'elles ont tout mis en œuvre pour respecter les principes de la protection des données. L'article 5 du RGPD fixe les sept grands principes relatifs au traitement des données à caractère personnel (cf. encadré p.2). Cette nouvelle mission concerne au premier chef les représentants du personnel qui doivent s'assurer que ces principes sont bien respectés. Particulièrement la finalité, l'information et l'accès aux données à caractère personnel par le salarié (art. 13 et suivants du RGPD). La protection des données personnelles devient un droit fondamental pour les salariés.

#3 LA CONSULTATION DU CE OU DU CSE

Le Code du travail impose d'informer et consulter les représentants du personnel préalablement à la mise en œuvre ou la modification de certains traitements automatisés :

- l'information-consultation du CE ou du CSE porte sur les traitements automatisés de gestion du personnel et à leur modification, préalablement à leur introduction dans l'entreprise (C. trav., art. L. 2312-38) ;
- les représentants du personnel doivent également être informés de la désignation d'un correspondant à la protection des données à caractère personnel et de la désignation d'un délégué à la protection des données (DPO). Cette désignation, obligatoire uniquement dans les entreprises qui traitent des données à grande échelle, est largement recommandée à toutes les entreprises par la CNIL ;
- la consultation doit prévoir les éléments qui justifient le recours à une collecte de données (cf. encadré p.2) ;
- les IRP doivent également être informées et consultées sur les chartes informatique et interne de protection des données personnelles, documents généralement annexés au règlement intérieur.

Le comité a la possibilité de se faire assister d'un expert technique pour analyser les conséquences de la mise en place du RGPD et de ses conséquences sur les conditions de travail ; Syndex a développé un partenariat avec l'Arete à cette fin.

SANCTIONS

La violation du RGPD peut conduire à une amende pouvant aller jusqu'à 10 M€ ou 2% du chiffre d'affaires mondial de l'exercice précédent. Pour les infractions les plus graves cette amende peut aller jusqu'à 20 M€ ou 4% du chiffre d'affaires. Plusieurs sanctions ont été délivrées par la CNIL depuis la mise en place du RGPD.

Exemples de sanctions

- Biométrie : la CNIL a prononcé une sanction de 10 000 euros à l'encontre d'une société d'assistance pour avoir notamment mis en œuvre illégalement un système biométrique à des fins de contrôle des horaires des salariés.
- Collecte des données : la CNIL a prononcé une sanction de 50 millions d'euros à l'encontre de Google, pour avoir insuffisamment informé les internautes sur l'utilisation et la conservation des données collectées.

#4 LES CE ET CSE CONCERNÉS PAR LE RGPD

Les traitements informatisés mis en œuvre par les institutions représentatives du personnel dans la gestion des activités du CE/CSE doivent également se conformer au RGPD. Et, comme les entreprises, les CE/CSE doivent pouvoir prouver la mise en conformité à ce nouveau règlement.

Le RGPD implique pour les CE et CSE de renforcer les clauses contractuelles applicables aux prestataires externes et sous-traitants impliqués dans les traitements de données personnelles (devoir de conseil, obligations de sécurité, gestion des failles et incidents, coresponsabilité, etc.).

Dans cette optique, la CNIL a prévu d'éditer un référentiel concernant les instances représentatives. Dans l'attente de ce référentiel, la CNIL a décidé de maintenir les anciennes dispenses afin de permettre aux CE/CSE d'orienter leurs premières actions de mise en conformité (dispense n°10 traitant de l'activité des institutions représentatives du personnel). Nous recommandons de prendre contact directement avec la CNIL ou un partenaire spécialisé, tel que l'Arete, pour vous accompagner sur le sujet.

#5 UN ENJEU SYNDICAL À SAISIR

À travers la collecte (big data) et l'exploitation (Intelligence artificielle) des données par l'entreprise, c'est la place de l'homme et de la femme dans le travail de demain qui est en jeu. Les représentants du personnel ont un rôle primordial à jouer, la protection des données devient donc une nouvelle mission du CE/CSE.

Il s'agit de s'emparer du sujet au plan collectif comme au plan individuel, à travers le CE/CSE ou la négociation d'accords collectifs permettant de négocier :

- un code de bonne conduite au sein de l'entreprise ;
- la mise en place d'une commission de veille ;
- l'accès aux certifications des prestataires, aux études d'impact ou le déclenchement d'un audit ;
- le contrôle de la mise en place opérationnelle des dispositifs pour vérifier qu'ils ne sont pas utilisés à d'autres fins ;
- la mise en conformité de fichiers locaux (par exemple le cas des managers de proximité qui peuvent constituer des fichiers à leur seule destination contenant des données personnelles de leurs collaborateurs) ;
- ou dans le cadre du pouvoir disciplinaire de l'employeur, les griefs qui pourraient être utilisés à l'encontre d'un salarié qui viendrait, par exemple, s'appuyer sur des données personnelles d'un client, doivent avoir fait l'objet d'une autorisation préalable de la part du client, d'utiliser ses données personnelles.

LES SEPT PRINCIPES RELATIFS AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL (ART. 5 DU RGPD)

LÉGALITÉ. Les données doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée. L'entreprise doit justifier sur quelle base légale elle souhaite collecter les données des salariés : obligations découlant du contrat de travail, Intérêt légitime de l'entreprise, etc.

FINALITÉ. Les données à caractère personnel ne peuvent être collectées que pour un usage déterminé, explicite et légitime et ne peuvent pas être traitées ultérieurement d'une manière incompatible avec ces finalités. (ex. : la géolocalisation initialement mise en place pour la sécurité utilisée pour contrôler des salariés).

PROPORTIONNALITÉ ET PERTINENCE DES DONNÉES. Seules doivent être traitées les informations adéquates, pertinentes et nécessaires au regard des objectifs poursuivis. La question à se poser : existe-t-il d'autres possibilités ?

EXACTITUDE DES DONNÉES. Les données collectées doivent être non seulement exactes mais aussi, si nécessaires, tenues à jour.

CONSERVATION DES DONNÉES LIMITÉE. Les informations ne peuvent être conservées de façon indéfinie. Une durée de conservation précise doit être déterminée en fonction de la finalité de chaque fichier.

SÉCURITÉ, D'INTÉGRITÉ ET CONFIDENTIALITÉ DES DONNÉES. L'employeur, responsable du traitement, est astreint à une obligation de sécurité. (garantir la confidentialité des données, éviter leur divulgation, leur perte, destruction ou dégâts d'origine accidentelle).

RESPECT DES DROITS DES PERSONNES. Lors de l'informatisation de leurs données, les salariés concernés ou les candidats à un emploi doivent être clairement informés des objectifs poursuivis (caractère obligatoire ou facultatif des réponses, destinataires des données, modalités d'exercice de leurs droits d'accès, de rectification et d'opposition).

Syndex
22, rue Pajol - CS 30011 - 75876 Paris cedex 18
Tel : 01 44 79 13 00 / contact@syndex.fr
Fiches pratiques Syndex - Janvier 2019
Ont contribué à ce numéro :
C. Bel ; Serge Gauthronet (Arete)
Directeur de la publication : O. Laviolette
Crédits photos : L. Villeret

www.syndex.fr

syndex
L'EXPERTISE ENGAGÉE

Ce numéro a été réalisé en partenariat avec l'**ARETE**
3-5 rue de Metz - 75010 Paris
Tél : 01 40 22 12 12