RÉPONSES PRINT'STORY ÉPISODE 29

Mais au fait :

Les entreprises sont-elles toutes concernées quelle que soit leur taille ?

Le nouveau Règlement général sur la protection des données personnelles (GDPR/RGPD) sera applicable le 25 mai 2018. En France et en Europe, toutes les organisations sont concernées par ce Règlement, qu'il s'agisse d'entreprises, d'associations ou encore d'organismes publics, et ce quelles que soient leur taille et leur activité. Ainsi les TPE et PME, autant que les grandes entreprises, doivent se préparer et anticiper leur mise en conformité. De même, des entreprises situées hors des frontières européennes devront respecter le Règlement à partir du moment où elles traitent les données de résidents européens pour leur proposer des biens ou des services ou suivre leur comportement.

Il faut bien comprendre que les entreprises sont concernées, qu'elles traitent des données à caractère personnel pour leur propre compte ou pour le compte d'une autre organisation, dans le cadre d'une prestation externalisée par exemple. Les imprimeurs, petits ou grands, sont donc tous impactés, à la fois pour leurs propres traitements (RH, fichier clients, fichier fournisseurs…) et pour ceux qu'ils mettent en œuvre pour leurs clients (réception et gestion de fichiers de clients finaux, impression de documents personnalisés…).

Quel est le but de cette nouvelle règlementation ?

Adopté le 27 avril 2016, le GDPR vient remplacer la Directive 95/46 CE de 1995, transposée en France dans la loi Informatique & Libertés.

L'objectif de cette révision est d'offrir un cadre législatif harmonisé à l'ensemble des acteurs économiques dans le cadre du marché unique numérique et d'assurer un niveau élevé de protection à tous les citoyens de l'Union. Cette double exigence a conduit les institutions à modifier le texte en profondeur.

Le nouveau texte aboutit à un total changement de paradigme. Ainsi, la protection des données n'est plus une simple formalité des entreprises vis-à-vis de la CNIL. D'une part les organisations devront désormais envisager la protection des personnes et de leurs données comme une question centrale dont elles devront tenir compte en amont et au cœur de toute opération de traitement (protection des données dès la conception et par défaut). D'autre part, il est attendu une véritable responsabilisation des organisations, qui devront être en mesure de démontrer à tout moment qu'elles agissent conformément aux exigences du Règlement et notamment qu'elles mettent en œuvre les mesures techniques et organisationnelles nécessaires à son respect.

Quelles sont les obligations à respecter ?

En tant qu'imprimeur, vous êtes soumis aux obligations de toute entreprise en tant que responsable de traitement, pour les traitements que vous réalisez (ou faites réaliser) pour votre propre compte (gestion RH, clients, prospections…). Mais vous avez également des obligations complémentaires en tant que sous-traitant pour les traitements que vous réalisez pour le compte de tiers. Arrêtons-nous sur ces dernières.

L'imprimeur qui traite des données à caractère personnel pour le compte de ses clients devra leur apporter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées pour que ces traitements répondent aux exigences du Règlement et

garantissent les droits des personnes concernées. Vous devrez notamment garantir la sécurité des traitements et des données, à la fois par des mesures physiques et organisationnelles. Dans ce cadre, vous devrez imposer une obligation de confidentialité à vos salariés, prévoir la destruction des données au terme de la prestation, alerter votre client en cas de violation de la sécurité. Vous devrez également leur apporter conseils et assistance dans le respect de certaines de leurs obligations (sécurité, notification des violations…).

Dans le cadre du principe de responsabilisation, l'imprimeur devra documenter l'ensemble des traitements et des procédures mis en place pour être à même de démontrer à tout moment son respect du Règlement. Vous devrez tenir un registre de toutes les catégories d'activités de traitement effectués pour le compte du responsable du traitement. Rappelons que la tenue d'un registre est obligatoire pour toute entreprise de plus de 250 salariés et pour les entreprises de moins de 250 salariés si les traitements effectués présentent un risque pour les droits et libertés des personnes concernées, ou si les traitements ne sont pas occasionnels, ou encore s'ils portent sur des catégories particulières de données, notamment les données sensibles.

Cette nécessaire traçabilité se traduit également par l'obligation d'établir un contrat avec chacun de vos clients. Ce contrat décrit le traitement objet de la sous-traitance, sa durée, sa nature, ses finalités, le type de données et les catégories de personnes concernées, mais aussi l'ensemble de vos obligations et de celles de votre client. Vous ne devrez agir que sur instruction documentée de votre client (contrat, email, compte-rendu de réunion…) et ne pourrez faire vous-même appel à un sous-traitant sans son autorisation écrite préalable.

Comment mettre en place cette règlementation dans votre imprimerie ?

Notons que l'Europe a privilégié une approche par les risques, laissant la possibilité aux organisations d'adapter les mesures mises en œuvre au niveau de risque présenté par les traitements effectués. Une approche au cas par cas sera donc nécessaire. Par exemple, le niveau d'exigence et donc de protection ne sera pas le même pour un imprimeur qui édite des relevés d'une mutuelle, impliquant l'utilisation de données sensibles, que pour un imprimeur qui personnalise le prénom et le nom d'une personne sur un cadeau d'entreprise.

Sur un plan général, la sensibilisation de l'ensemble des directions (générale, informatique, marketing, juridique, production…) au nouvel état d'esprit imposé par le Règlement est primordiale. Idéalement, elle sera accompagnée de la désignation d'un pilote ou d'un comité de pilotage de la conformité au sein de l'imprimerie.

Dans un premier temps, ce pilote devra dresser un état des lieux en répertoriant l'ensemble des traitements de données à caractère personnel réalisés. Il identifiera les traitements internes effectués par l'imprimerie pour ses propres besoins autant que les traitements qu'elle réalise pour le compte de ses clients. Il relèvera pour chaque traitement la nature des données traitées, leur finalité, la durée de conservation… ainsi que toute information disponible (sensibilité de ces données, flux, procédures de sécurité existantes…). Cette première approche lui permettra de déterminer les écarts, les points de non-conformité qu'il faudra corriger, et ainsi de prioriser les actions à mener.

Cette cartographie sera également très utile pour établir le registre des traitements qui recensera vos clients et décrira les traitements réalisés pour leur compte.

Le pilote devra analyser, en fonction des caractéristiques de l'activité de base de l'entreprise, l'obligation ou non de nommer un délégué à la protection des données (DPO/DPD). Si certains traitements présentent des risques particuliers, une analyse d'impact devra également être envisagée. Ceci ne devrait toutefois concerner qu'une minorité d'imprimeurs.

Les procédures de sécurité physique et logique feront l'objet d'une attention toute particulière, de même que l'intégration des principes de protection dès la conception et par défaut. Pensez par exemple à limiter l'accès aux données aux seules personnes qui ont besoin d'y accéder. De même des outils de veille permettront de tester et de valider régulièrement l'efficience des mesures de sécurité mises en place.

Il vous faudra enfin réviser l'ensemble des documentations actuelles, y intégrer les registres ainsi que toutes les procédures mises en place, les compléter ou en créer si besoin…, adapter les contrats existants avec les nouvelles clauses obligatoires (nouveaux contrats ou avenants), sensibiliser et former votre personnel.

Vous êtes prêts ? N'oubliez pas que la conformité est un processus itératif et qu'il vous faudra régulièrement revisiter l'ensemble de vos traitements et procédures pour vous assurer du maintien de cette conformité.

Qui peut vous aider ?

La CNIL a mis en ligne sur son site www.cnil.fr une rubrique Règlement européen dans laquelle vous trouverez des documents et outils qui vous accompagneront dans votre démarche.

L'UNIIC, à travers son partenariat avec le SNCD, est bien entendu à votre disposition pour vous aider dans vos démarches et vous renseigner.

Réponses élaborées par Nathalie Phan Place, Déléguée Générale du SNCD

nplace@sncd.org

L'IDICG et le SNCD vous proposent une formation sur ce sujet : **Fondamentaux et mise en oeuvre du GDPR**

N'hésitez pas à contacter *Chantal Richardeau, Responsable HSE à l'UNIIC*

chantal.richardeau@uniic.org