Webinaire du 25 mars 2021 Par Eric Barby

Archivage numérique et RGPD

« Le RGPD est un puits sans fond », les nouvelles obligations en matière de droit des cookies engagent les entreprises à effectuer de sérieuses analyses d'impact pour le 25 mai 2021.

Le cœur du problème

Toute donnée numérique archivée ou échangée par document contient des données personnelles (DP)**.** Dès lors, toute entreprise concernée par cet élément doit se conformer au RGPD. Que cela concerne de l'archivage de données (data pure, information numérique) ou de l'archivage de documents (qui contiennent tous au moins un nom, une adresse, un identifiant…), l'entreprise manipule des DP. Même un enregistrement audio archivé tombe sous la régulation du RGPD.

L'autre problème concerne le peu de documentation fournie par la CNIL. On trouve sur son site un document de 2005 dont la typologie est obsolète et en marge des usages réels employés par les professionnels → (archives « courantes », « intermédiaires » et « définitives")

En pratique

Le RGPD c'est :

- **4 OBLIGATIONS**

-Information : Il faut, avec toute personne interne comme externe à l'entreprise, les surabonder d'informations au sujet de leurs propres DP et de la manière dont elles sont gérées. Il s'agit donc de rédiger des politiques de gestion des DP. Les cookies, mentions, enregistrements audio et vidéos entre collaborateurs et clients etc.

-Organisation : Il faut donc s'organiser autour de la data. Le RGPD prescrit une conduite à tenir concernant la manière de gérer les DP. (DPO, règles de bonne conduite, règles de sous-traitance, droit des personnes, et démarches telles que privacy)

-Technologie : Il faut prendre des mesures de sécurité informatique pour se prémunir de toute intrusion. D'où le rôle essentiel du DSI.

-Registre : Il faut constituer des registres des opérations de traitement de données.

- **4 SANCTIONS**

-Pénale **-Administrative et financière**

-Injure à l'image de marque **-Suspension du service par la CNIL**

- **1 PRINCIPE**

On ne garde pas les données au-delà de la durée nécessaire de la finalité de leur traitement. Dès qu'un traitement de DP est mis en place, il faut savoir quelle en est la durée prescrite de conservation, afin de s'organiser en conséquence.

Cas particulier des données statistiques : on peut conserver des données à des fins statistiques, à condition de les anonymiser. Dès lors, elles ne sont plus concernées par le RGPD. Attention à ne pas confondre *pseudonymisation* (déplacement de la référence personnelle à une suite de chiffre par exemple) et *anonymisation* (cryptage définitif et irréversible des DP).

➔ Tout cela est utile à **l'apport de preuves de conformité au RGPD** en cas de contrôle par la CNIL, qui peut exiger la consultation des registres, des politiques etc. Elle cherchera à savoir si, respectant ces principes, l'entreprise respecte le principe d'« accountability », à savoir « l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données. » (Site officiel de la CNIL)

Concernant l'archivage

Chacune des 4 obligations possède sa propre particularité à ce sujet :

-Information : Consiste en la vérification que l'entreprise a une politique RGPD (ce dont s'occupe le DPO, ou le référent RGPD). Dans les politiques salariés/candidats/clients/prospects/fournisseurs, dans les informations sur les cookies, dans les CGU/CGV/CGS → il faut qu'on retrouve des informations liées à l'archivage. Le point essentiel étant la durée de rétention des DP, qui doit être renseignée très précisément. Aussi, le droit d'accès pour un individu à ses propre DP est central, étant donné que de plus en plus de gens les réclament.

-Organisation : Une *procédure d'accès* doit décider du droit d'accès des particuliers à leurs données (effacement, gestion, consultation). Attention à bien différencier « DP » et « document », afin de ne pas fournir TOUTES les informations présentes sur un document, sous prétexte que le nom d'un salarié y apparaît une fois.

Aussi, une *politique de durée de conservation* est essentielle. Le problème n'est pas tant la durée prescrite par la CNIL, l'usage ou la profession, mais bien la réalité de la mise en œuvre de la conservation et de la suppression de données. Il s'agit de s'assurer que les données sont bien supprimées, et que la gestion des sauvegardes de données est conforme au RGPD.

De plus, il faut correctement *contractualiser les relations entretenues avec les prestataires* : afin de s'assurer que ces derniers sont bien conformes au RGPD. S'assurer également de la

localisation des données, qui posent un problème hors UE. En somme, il s'agit de bien circonscrire le cadre des responsabilités, dont les prestataires tenteront de se dédouaner.

Enfin, la *privacy by design* (article 25 du RGPD) prescrit qu'il faut protéger les DP dès la conception d'un nouveau projet d'archivage. Donc, protéger les DP doit être fait dès la mise en œuvre d'un projet impliquant le traitement de DP. C'est là que les conseils d'un DPO sont précieux et essentiels.

-Technique : Dans la mise en place des mesures appropriées, tout l'enjeu est d'établir des moyens de mesurer la pertinence et l'efficacité des mesures appliquées. Cela est une exigence de la CNIL, qui demande que chaque boîte fasse sont « autocritique », en se surveillant elle-même.

Les éléments essentiels aux mesures techniques sont englobés par le *PSSI* (Politique de sécurité du système d'information). Ils sont : la politique d'habilitation, la politique de log, la DLP, le PCA, le PRA, la purge et le monitoring.

Car, un salarié comme un prestataire peuvent avoir accès à des DP : il s'agit donc de le mesurer et de le tracer. Il faut s'organiser pour savoir **qui** et **quand** consulte des DP, pour régler les conflits de responsabilité en cas de problème.

-Registre : Il faut avoir un registre d'obligations de traitement. Là, il y a 2 types d'informations à communiquer au DPO :

1) *Traitement de l'archivage de données*. Le traitement déclaré des bulletins de paye n'est pas une archive à part entière, mais doit mentionner sa finalité (établissement du bulletin, envoie et conservation). Car, légalement, ces informations doivent être conservées pour le compte du salarié.

2) *Traitement de l'archivage de données à part entière.* Archiver les mails est un traitement à part entière de données dans les registres de traitement des données numériques. C'est un outil de conservation des mails, un traitement de messagerie.

Questions

- Pascal Lenoir : Avoir un système s'archivage aux normes, cela répond-il aux problèmes RGPD ?

Non, c'est disjoint. Rien de commun entre le droit de l'archive numérique et le RGPD. La seule passerelle se trouve en matière de sécurité.

- Pascal Lenoir : Y a-t-il eu des contrôles de la part de la CNIL sur la partie archivage alors ? Font-ils références aux données archivées ?

Aussi loin qu'Éric Barby le sait et l'a vécu, il dit que « non », et qu'ils vérifient surtout les durées. Ils le font dans le système d'information lui-même, mais pas dans les archives. Mais, n'exclut pas en soi la possibilité que ça arrive. Et, la CNIL peut focus les durées de conservation, rien ne l'en empêche théoriquement.