LA RESPONSABILITÉ DU SOUS-TRAITANT, AVANT ET APRÈS RGPD : UNE JURISPRUDENCE DE PLUS EN PLUS SÉVÈRE !

La protection des données personnelles en France date de 1978, et pourtant ce n'est que depuis le RGPD en 2018 que ce sont révélées les vraies lacunes des entreprises au regard de leurs obligations en matière de protection des données.

L'évolution technologique et du numérique poussent les entreprises à faire appel à des partenaires qualifiés pour gérer leur traitement de données personnelles. La technicité de certaines matières l'impose.

C'est en ce sens que la réglementation est de plus en plus précise sur la responsabilisation des acteurs de la donnée et de leur qualification.

DES NOTIONS QUI ÉVOLUENT

L'une des questions essentielles que doit se poser une entité lorsqu'elle traite des données personnelles, c'est de savoir si elle les traite en qualité **de responsable de traitement** ou en qualité **de sous-traitant**.

L'article 4-7 du RGPD définit le responsable de traitement comme toute personne physique ou morale, autorité publique, service ou organisme qui détermine seul ou conjointement, les finalités et les moyens du traitement de données personnelles. Le CEPD (Comité Européen de la Protection des Données anciennement G29) dans ses dernières lignes directrices du 2 septembre 2020 (Guidelines 07/2020), précise qu'il s'agit principalement des ***« moyens essentiels »*** tels que : type de données, tiers autorisés, durée du traitement et effacement des données…

Le sous-traitant quant-à-lui est désigné comme étant toute personne physique ou morale, autorité publique, service ou organisme qui traite les données personnelles pour le compte du responsable de traitement (article 4-8 du RGPD), susceptible pour autant d'avoir une certaine marge de manœuvre dans la mise en place technique du traitement. Le CEPD précise à ce titre qu'il peut être décisionnaire des ***« moyens non essentiels »*** du traitement.

Avant l'entrée en vigueur du RGPD, seul le responsable de traitement était maître de la protection des données personnelles. Il devait s'assurer de la bonne mise en œuvre du traitement mais également de déterminer et vérifier la bonne application des mesures de sécurité par les sous-traitants qu'ils désignaient.
Sa responsabilité vis-à-vis de la CNIL et des conséquences était entière.

C'est ce qu'a notamment rappelé la CNIL dans **sa sanction à DARTY le 8 janvier 2018** (délibération n°SAN-2018-001), en reprécisant que si le sous-traitant avait pris l'initiative d'ajouter un moyen de traitement non défini par DARTY, cela ne présentait pas un caractère suffisant pour considérer EPITCA comme responsable de traitement. C'était bien DARTY qui déterminait la finalité et les moyens essentiels du traitement, celui des données personnelles de ses clients, EPTICA ne les traitant pas pour son compte. DARTY devait donc assumer l'entièreté des conséquences d'une mauvaise mise en œuvre des traitements.
En l'espèce, DARTY utilisait un logiciel développé par le sous-traitant EPTICA pour sa gestion des demandes de service-après-vente. Or il apparaissait que l'URL à partir de laquelle les clients pouvaient déposer leur demande de service après-vente permettait d'accéder à d'autres fiches clients, juste en modifiant le numéro d'identifiant dans l'URL.

Nombre de responsables de traitement étaient dépassés par cette responsabilisation accrue face à des technologies qu'ils ne maitrisaient pas au contraire du sous-traitant. C'est dans ces conditions que le RGPD **a imposé de nouvelles obligations au sous-traitant** afin que celui-ci soit considéré comme responsable de ses actions sur les traitements, quand bien même celles-ci soient commanditées par le responsable.

UN CONTRAT OBLIGATOIRE

Le RGPD n'a pas laissé le choix aux parties d'improviser dans la répartition de leur rôle et de leurs obligations.

Il a imposé au responsable et au sous-traitant qui entendent s'accorder sur un traitement de données, **d'établir un contrat écrit**, qui doit comprendre les mentions listées à l'article 28 (3°) du RGPD.

En pratique, ce contrat fait cruellement défaut. Il est pourtant indispensable.

Si dans un premier temps, il doit définir clairement : l'objet, la durée, la nature, la finalité du traitement, les catégories de données à caractère personnel, les catégories de personnes concernées, la chaine de sous-traitance possible ainsi que les instructions claires du responsable de traitement… **il doit également contenir et garantir la sécurité du traitement mais également la gestion juridique des responsabilités entre les intervenants.**

Cette sécurité juridique est cruciale, d'autant que la responsabilité des différents acteurs du traitement de la donnée personnelle est de plus en plus importante.

LE SOUS-TRAITANT N'EST PLUS À L'ABRI DES SANCTIONS

Le RGPD a élargi les obligations du sous-traitant qui ne se limitent plus au simple respect des conditions de sécurité du traitement et des données personnelles mais précise les nouveaux impératifs auxquels il est soumis, à savoir :

- L'obligation de transparence et de traçabilité
- L'obligation de sécurité **renforcée** du traitement
- L'obligation d'assistance, d'alerte et de conseil

Au fur et à mesure des années, les actes ont remplacé les principes.

La jurisprudence suit de plus en plus cette mouvance et ne laisse plus la possibilité au sous-traitant de s'exonérer de ses responsabilités.

Ce fut notamment le cas dans la décision de la **Cour d'appel de Paris, « SARL MISE A JOUR INFORMATIQUE c/ SARL E.X.M. EURO ET EXPERTISE MONETIQUE », du 7 février 2020,** (n°18/03616) où les juges du fonds ont rappelé que les causes d'exonération, notamment au titre de la force majeure, devaient être réduites à des événements strictement imprévisibles et qu'en l'état de la technologie et des savoir-faire techniques d'un sous-traitant en informatique, un virus informatique *« ne présente ni un caractère imprévisible, ni un caractère irrésistible et ne constitue donc pas un cas de force majeure ni même un fait fortuit exonératoire de responsabilité. »*

Cette jurisprudence a pour écho **la décision exemplaire de la commission restreinte de la CNIL du 27 janvier 2021** (délibération non publique), qui a condamné à la fois un responsable de traitement et un sous-traitant respectivement à 150 000€ et 75 000€ d'amende, pour ne pas avoir pris les mesures nécessaires à la protection d'un site à la suite d'une attaque par bourrage d'identifiants *(credential stuffing)*.

L'exemplarité n'est pas dans l'amende, qui n'est pas des plus élevées, **elle se reflète dans la condamnation à la fois du sous-traitant et du responsable de traitement**. En effet, si jusque-là le sous-traitant pouvait répondre civilement de sa responsabilité devant les juridictions judicaires, il n'était jamais condamné par la CNIL.

Dans cette affaire, la CNIL a reçu plusieurs notifications de violations de données entre juin 2018 et janvier 2020, en lien avec un site internet marchand. La CNIL a mené son enquête et constaté, auprès du responsable du traitement et du sous-traitant que ces derniers, avaient manqué à leur obligation de préserver la sécurité des données personnelles des clients, prévue par l'article 32 du RGPD.
Les sociétés ont tardé à mettre en place des mesures permettant de lutter efficacement contre ces attaques répétées. Elles avaient décidé de concentrer leur stratégie sur le développement d'un outil permettant de détecter et de bloquer les attaques lancées à partir de robots. Or, selon la CNIL, plusieurs autres mesures produisant des effets plus rapides auraient pu être envisagées afin d'empêcher de nouvelles attaques ou d'en atténuer les conséquences négatives.
Du fait de ce manque de diligence, les données d'environ 40 000 clients du site web ont été rendues accessibles à des tiers non autorisés.

Cette décision invite fortement les parties à revoir leur contrat afin de neutraliser les risques de tels partages de responsabilité.

En pratique cela se traduit notamment par l'obligation pour le sous-traitant de rechercher les solutions techniques et organisationnelles *« les plus appropriées »* pour assurer la sécurité des données et de les conseiller au responsable de traitement, qui faute de suivre ses instructions verra sa responsabilité engagée ; à charge pour le sous-traitant de le prévoir contractuellement.

Côté responsable de traitement, cette décision engendre la nécessité de borner plus sévèrement les obligations de son partenaire et d'exiger la rédaction d'une clause selon laquelle le sous-traitant tiendrait à disposition du responsable toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD et permettre la réalisation d'audit de sécurité.

Ces décisions sont le début d'une longue liste. Assurément.

Elles traduisent une volonté forte d'impliquer les sous-traitants dans la sécurité des traitements pour lesquels ils sont sollicités et celle de responsabiliser encore plus le responsable de traitement, premier garant de la protection des données personnelles et qui doit s'assurer d'avoir des sous-traitants techniquement et juridiquement fiables… et cela commence par la voie contractuelle !

Les consultants en données personnelles de DPO Consulting Bourgogne-Franche-Comté sont à votre disposition pour la reprise de vos contrats et plus généralement pour votre mise en conformité RGPD.
N'hésitez pas à prendre contact.

Stéphanie BROGGINI
Consultante DPO Bourgogne-Franche-Comté
stephanie.broggini@dpo-consulting.com