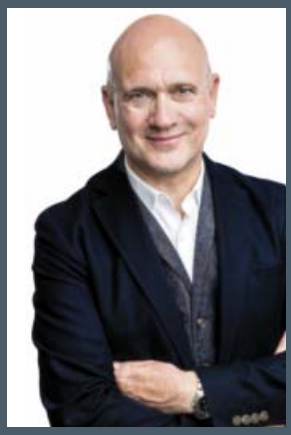
LES DÉFIS INHÉRENTS À LA MISE EN APPLICATION DU RGDP



Par Me Ghislaine ISSENHUTH, Avocat au Barreau de Paris, et Me Olivier SAMYN, Associé, Cabinet Lmt Avocats

« *PRINCIPE D'ACCOUNTABILITY* », « *PRIVACY BY DESIGN* », « *PRIVACY BY DEFAULT* », « *DPO* », « *PRIVACY IMPACT ASSESSMENT* ». LES ACTEURS AMENÉS À TRAITER DES DONNÉES PERSONNELLES SONT CONFRONTÉS À DE NOMBREUSES NOTIONS DONT L'APPRÉHENSION EST MAL AISÉE ET CE ALORS MÊME QUE LE RÈGLEMENT EUROPÉEN RELATIF À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL (« RGPD ») ENTRE EN APPLICATION DANS LES PROCHAINES SEMAINES (PRÉCISÉMENT LE 25 MAI 2018).

Le message du RGPD est fort : la responsabilité des acteurs est accrue (« *Principe d'accountability* »), ces derniers devant être à même de démontrer qu'ils traitent les données conformément aux principes édictés dans le Règlement, avec pour corollaire un alourdissement des sanctions en cas de manquement pouvant aller de 10 à 20 millions d'euros ou de 2% à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent pour une entreprise.

Les établissements de santé privés comme publics sont naturellement concernés par ces nouvelles obligations, puisqu'ils sont amenés à traiter tant des données personnelles, telles que les données administratives, que des données de santé. Le traitement des données de santé définies comme « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* » est, aux termes de l'article 9 §1 du RGPD, interdit sauf exceptions, les Etats membres pouvant à ce titre introduire des conditions supplémentaires. En France, la réforme de la loi informatiques et libertés est engagée puisque le projet de loi CNIL 3 est depuis le 6 février dernier soumis au débat parlementaire avec, pour les données de santé, le maintien de la même philosophie, à savoir un système d'autorisation préalable de la CNIL pour le traitement des données de santé et dans certains cas des formalités simplifiées par les méthodologies de référence.

UNE CONFORMITÉ À JUSTIFIER

Pour autant, la mise en conformité des pratiques

LE DROIT À LA PORTABILITÉ DES DONNÉES VA ÊTRE CONFRONTÉ À **L'ACTUEL SYSTÈME D'INFORMATION HOSPITALIER QUI N'APPARAÎT PAS ADAPTÉ AUX EXIGENCES NOUVELLES**.

des établissements de santé aux exigences du RGPD leur impose un traitement conforme aux règles de protection des données, ce qui implique le respect de l'approche « *Privacy by Default* » et « *Privacy by Design* », soit respectivement le principe de la protection des données dès la conception du traitement et le respect des cinq principes suivants : finalité de traitement déterminée et légitime, pertinence et proportionnalité des données, durée de conservation déterminée, respect du droit des personnes et mise en place de mesures de sécurité de nature à garantir la confidentialité des données.

Les établissements de santé doivent justifier du respect de ces règles par la tenue d'un registre des activités de traitement, la mise en place de procédures internes de conformité qui vont de la formation des salariés à la réalisation d'audits de conformité, en passant par la réalisation d'analyses d'impact (« *Privacy Impact Assessment* »). L'analyse d'impact doit permettre aux établissements de santé d'identifier les traitements de données qui comportent un risque élevé pour les droits et libertés des personnes concernées et nécessitent une autorisation préalable de l'autorité de contrôle. En pratique, les traitements qui auront légalement été mis en œuvre avant le 25 mai 2018 n'auront pas à faire l'objet d'une analyse d'impact sauf si le traitement a été modifié substantiellement depuis sa mise en œuvre (comme par exemple par l'allongement de la durée de conservation des données). En tout état de cause, une analyse d'impact devra être réalisée pour ces traitements dans les trois ans suivants la mise en application du RGPD. La CNIL a créé le logiciel libre PIA, outil « prêt à l'emploi » directement intégrable dans les outils internes de l'entreprise ou de l'établissement de santé, visant à faciliter la conduite des analyses par le responsable de traitement. Toutefois, l'adaptabilité de cet outil aux plateformes et serveurs employés par les réseaux hospitaliers reste à démontrer.

UNE CONFORMITÉ CONTRÔLÉE PAR LES DPD

Le chef d'orchestre du respect de ces mesures est le délégué à la protection des données (DPD) ou *Data Protection Officer* (DPO), dont la désignation est obligatoire pour l'ensemble des établissements de santé public et pour les établissements de santé privés traitant des données sensibles à grande échelle. Le DPD doit être impliqué dans le processus de décision des données, aussi sa place dans la structure doit être soigneusement étudiée, étant précisé que les établissements ont la possibilité de mutualiser un DPD entre plusieurs établissements. Ce dernier doit être facilement joignable et parler la langue de l'autorité de contrôle, son positionnement géographique en dehors de la France paraît donc difficilement envisageable.

UNE CONFORMITÉ IMPOSÉE AUX SOUS-TRAITANTS

Le respect du RGPD incombe également aux sous-traitants qui peuvent au même titre que les responsables de traitement être condamnés en cas de manquement. Un établissement peut avoir la qualité de sous-traitant lorsqu'il agit pour le compte d'un tiers, comme par exemple dans le cadre des groupements hospitaliers de territoire (GHT) qui, de par leur mission de définition des moyens et des finalités du traitement, sont les responsables de traitement. A cet égard, la revue des contrats avec les sous-traitants apparaît indispensable.

En conclusion, la mise en application du RGPD, qui a pour but de renforcer les droits des personnes dont les données sont collectées, comporte de nombreux défis dans la redéfinition des procédures internes et dans la création de nouveaux outils de conformité. L'effectivité de ces mesures sera suivie avec attention par la CNIL mais leur mise en œuvre pratique semble complexe. A titre d'exemple, le droit à la portabilité des données selon lequel les données doivent pouvoir être transmises directement d'un établissement à un autre va être confronté à l'actuel système d'information hospitalier qui n'apparaît pas adapté aux exigences nouvelles.●

LE CABINET Lmt AVOCATS

Composé de femmes et d'hommes réunis par des valeurs communes et animés par un fort esprit d'équipe, Lmt Avocats dispose de plusieurs cordes à son arc. Parmi ses principaux domaines d'expertise, citons le droit social et le droit des sociétés, la propriété intellectuelle et les technologies de l'information, le conseil aux dirigeants ou encore les arbitrages internationaux. Il a par ailleurs développé une forte compétence en matière règlementaire, contractuelle et contentieuse dans l'ensemble des domaines ayant trait aux produits de santé. S'appuyant sur des équipes bilingues et pluridisciplinaires, il assiste aussi bien des laboratoires pharmaceutiques que des fabricants de dispositifs médicaux, des assureurs, des distributeurs de produits de santé, des laboratoires de biologie, des professionnels et établissements de santé, et des agences de communication spécialisées.