

Lexique RGPD

- « **Analyse d'impact des risques** » (**AIPD**): il s'agit d'une procédure destinée à évaluer si un traitement de données à caractère personnel comporte des risques pour les droits et les libertés de la personne dont les données sont traitées et à évaluer la manière dont ces risques peuvent être maîtrisés.
- « **Autorité de protection des données (APD)** » : depuis le 25 mai 2018, la Commission de la protection de la vie privée (CPVP) a cédé sa place à la nouvelle Autorité de protection des données (ADP). Nous vous invitons à visiter le site Internet de l'Autorité de protection des données : www.autoriteprotectiondonnees.be
- « **Catégorie de données** » : les acteurs de la santé sont autorisés légitimement à collecter certaines catégories de données personnelles telles que les données d'identification (nom, prénom, date de naissance, numéro de registre national, adresse, numéro de téléphone), les données relatives à la situation familiale (situation matrimoniale, nombre d'enfants), les données relatives à la vie professionnelle (profession, conditions de travail), les données de santé (historique médical, historique des soins, diagnostics médicaux, traitements prescrits, nature des actes effectués, résultats d'examens de biologie médicale et tout élément de nature à caractériser la santé du patient) et les données relatives aux habitudes de vie.
- « **Délégué à la protection des données** » (**DPO**) : il est chargé d'assurer la mise en conformité réglementaire avec les exigences du RGPD au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme. Sa désignation est obligatoire dans certains cas.
- « **Destinataire** » : c'est « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers* ».
- « **Donnée à caractère personnel** » ou « **donnée personnelle** » (**DCP**) : elle est définie comme « *toute information se rapportant à une personne physique identifiée ou identifiable* », c'est-à-dire une « *personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

- « **Données sensibles** » : la collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions.
- « **Données de santé** » : elles désignent 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* ».
- « **Finalité** » : il s'agit des finalités pour lesquelles les données sont traitées. Elles doivent être déterminées, explicites et légitimes.
- « **Licéité** » : il s'agit du terme juridique qui s'emploie pour désigner le caractère de ce qui est conforme au droit. Conformément au RGPD, le traitement des données doit être licite, c'est-à-dire qu'il doit répondre au moins à une des conditions de l'article 6 et de l'article 9 pour ce qui concerne le traitement des données sensibles.
- « **Mesures de sécurité techniques et organisationnelles** » : il s'agit des mesures garantissant un niveau de sécurité adapté au risque.
- « **Personne concernée** » : il s'agit de la personne physique (par opposition à une personne morale, société privée, un organisme ou encore une autorité publique) identifiée ou identifiable à laquelle se rapporte une information.
- « **Référent à la protection des données** » : si la désignation d'un délégué à la protection des données n'est pas requise pour tous les prestataires de soins, la désignation d'une personne référente pour la protection des données est vivement encouragée. Cette personne serait en charge d'assurer la mise en conformité réglementaire du RGPD et aurait notamment pour mission de veiller à sensibiliser l'équipe de soins et les autres membres du cabinet à la protection des données, à tenir et à mettre à jour le registre des activités de traitement, à être la personne de référence pour toutes questions relatives à la protection des données et à être la personne de référence pour centraliser les fuites de données et en faire rapport à l'autorité de protection des données.
- « **Registre des activités de traitement** » : il s'agit d'un outil interne qui permet aux responsables de traitement et sous-traitants de recenser l'ensemble des traitements de données réalisés et de disposer d'une vue d'ensemble de ce qu'il est fait avec les données. Ce registre permet ainsi de faciliter la mise en conformité de ces traitements avec les exigences du RGPD.

- « **Responsable de traitement** » (RT) : il s'agit de « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* ».
- « **Responsable conjoint de traitement** » : si les finalités et les moyens du traitement sont déterminés par plusieurs entités juridiques distinctes, celles-ci seront alors considérées comme responsables conjoints du traitement qu'elles mettent en œuvre.
- « **Sous-traitant** » (ST) : il s'agit de « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* ».
- « **Traitement** » : attention, il n'y a **pas lieu de confondre le « traitement des données personnelles » avec le « traitement médical » sensu stricto**. La notion de « traitement » au sens du RGPD s'entend largement comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ». Il s'agit donc de toute action réalisée sur des données personnelles, et ce dès la collecte de données.