Principes clés pour un traitement licite de données personnelles

Tout **responsable de traitement** de données personnelles **(ci-après « le RT »)**, et à fortiori de données personnelles de santé, doit, sous peine de **sanctions**, respecter un certain nombre de **principes clés**, qui conditionnent la **légalité** dudit traitement.

Principe 1 – LA FINALITE

DEFINIR ET RESPECTER LES OBJECTIFS DU FICHIER

Avant de collecter des données personnelles, le RT doit **établir précisément la finalité** pour laquelle un traitement va être réalisé, *i.e.* ce à quoi les données collectées lui serviront. Cette finalité devra être **respectée pendant toute la durée du traitement**: tout traitement ultérieur réalisé dans un objectif autre que celui déclaré constitue un détournement de finalité, interdit par la loi Informatique et Libertés (IFL).

Principe 2 – LA PROPORTIONALITE

VERIFIER LA PROPORTIONALITE ET LA PERTINENCE DES DONNEES

Le RT ne peut collecter que des données qui sont strictement nécessaires à la réalisation de la finalité du traitement qu'il a déclaré. Le **principe de minimisation des données**, repris par le Règlement Européen, lui interdit de collecter des données excédant celles dont il a réellement besoin pour réaliser son objectif.

Principe 3 – LA TEMPORALITE

NE CONSERVER LES DONNEES QUE POUR UNE DUREE LIMITEE

Le RT ne peut **conserver les données collectées que pour une durée limitée**, qu'il doit préalablement définir. Cette durée ne peut excéder celle **nécessaire pour l'accomplissement des finalités** pour lesquelles les données sont traitées, et doit tenir comptes des éventuelles obligations légales de conservation des données (Voir notre fiche ***« Archivage versus Stockage des données de santé »***). **A l'expiration du délai prévu, le RT doit impérativement effacer lesdites données** (sauf exception légale), sous peine de **sanctions pénales** (délit).

Principe 4 – LA TRANSPARENCE

DECLARER LES TRAITEMENTS ET INFORMER LES PERSONNES

Le RT doit agir de manière loyale et transparente, ce qui implique:

- **Vis-à-vis des autorités, de mettre en œuvre les formalités préalables** (déclaration, autorisation auprès de la CNIL), ou lorsque le Règlement Européen sera applicable, de se conformer aux obligations que lui impose le **principe d'*accountability*** (Voir notre fiche ***« Le principe d'accountability et ses conséquences en matière de santé »***)
- **Vis-à-vis des personnes concernées, de les informer** de l'existence d'un traitement et de sa/ses finalité(s), de son identité, des destinataires des données, des droits dont ils disposent et de la manière dont ils peuvent les exercer, du caractère obligatoire ou facultatif des réponses, de la durée de conservation des données et des transferts éventuels de données en dehors de l'UE.

Principe 5 – LE CONSENTEMENT

RECUEILLIR LE CONSENTEMENT DE LA PERSONNE

Avant de traiter les données personnelles d'une personne, le RT doit recueillir son consentement, sauf si une des dérogations prévues à l'article 7 de la loi IFL - ou à l'article 8 en cas de données sensibles telles que les données de santé– est applicable (Voir notre fiche ***« Les données sensibles »***).

En pratique, cette obligation, couplée au principe de **Privacy By Design** introduit par le Règlement Européen, impose donc au fabricant de **prévoir, dès la conception d'un DM connecté, une procédure permettant à la personne concernée de donner ou de retirer, à tout moment, son consentement au traitement de ses données**.

Principe 6 – LES DROITS

RESPECTER LES DROITS DES PERSONNES SUR LEURS DONNEES

Le RT doit informer les personnes concernées des droits dont elles disposent sur les données traitées et de la manière dont elles peuvent les exercer.

Conformément au principe de **Privacy By Design**, des mécanismes doivent être prévus dès la conception du moyen de collecte pour permettre aux personnes de mettre en œuvre leurs droits (Voir notre fiche ***« Comment respecter les droits des personnes dont les données de santé sont traitées ? »***)

Principe 7 – LA SECURITE ET LA CONFIDENTIALITE

ASSURER LA SECURITE ET LA CONFIDENTIALITE DES DONNEES

Le RT doit prendre toutes les mesures nécessaires pour garantir la sécurité et la confidentialité des données, c'est-à-dire pour éviter qu'elles ne soient endommagées, déformées, ou que des tiers non-autorisés y aient accès. Pour plus de détails, voir notre fiche ***« La sécurité et la confidentialité des données de santé, quelles obligations? »***

Cette fiche présente de façon simple et synthétique une réalité juridique complexe.
Elle ne remplace donc pas l'avis d'un professionnel du droit, ni n'engage la responsabilité de ses auteurs.

Voir toutes nos autres fiches e-santé sous ce lien : http://www.sea-avocats.fr/e-sante.htm