DECRYPTAGE : LE MENSUEL DU CREAI

Thème : Système d'information

Novembre 2017

Protection des données personnelles : les règles applicables au 25 mai 2018

Texte de référence :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

Le 1er numéro de « DECRYPTAGE », nouvelle publication mensuelle du CREAI, est consacré à la présentation des principales dispositions du règlement européen sur la protection des données personnelles et à ses conséquences sur l'organisation des établissements et services sanitaires, sociaux et médico-sociaux qui, au travers notamment des dossiers de l'usager, traitent des données personnelles relatives à des personnes physiques.

Ce règlement européen entrera en vigueur le 25 mai 2018 et les structures sont invitées à anticiper d'ores et déjà cette réforme.

Les points importants de ce règlement sont en synthèse :

- L'information aux familles et aux usagers sur leurs nouveaux droits
- Le principe de responsabilité de la structure en charge du traitement des données
- La désignation de référent de délégué à la protection des données

SOMMAIRE

A – le contexte général d'adoption du règlement européen

L'évolution rapide des technologies et de la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel, l'ampleur de leur collecte et de leur partage connaissant un accroissement exponentiel.

Ainsi, les autorités publiques et les acteurs privés utilisent de plus en plus les données à caractère personnel. Parallèlement, les citoyens de l'Union Européenne, à travers notamment le déploiement des réseaux sociaux, rendent des informations les concernant accessibles publiquement.

Dans un tel contexte, l'Union Européenne, sur le fondement de la Charte des droits fondamentaux de l'Union Européenne, selon laquelle « toute personne a droit à la protection des données à caractère personnel la concernant », devait renforcer la réglementation applicable en la matière.

Le choix du recours à un Règlement européen, qui s'impose directement dans l'ordonnancement juridique des Etats de l'Union, a pour objectif d'assurer sur l'ensemble du territoire de l'Union Européenne un niveau cohérent et élevé de protection des personnes physiques.

Ainsi, le Règlement européen doit permettre de garantir la sécurité juridique et la transparence aux opérateurs économiques, un même niveau d'obligations et de responsabilités pour les responsables des traitements de données afin d'offrir aux personnes physiques de tous les Etats membres un même niveau de droits opposables.

A ce titre, afin de garantir pleinement les droits des citoyens européens, le règlement précise qu'il s'applique au traitement des données personnelles de citoyen se trouvant sur le territoire de l'Union européenne, par un responsable du traitement ou d'un sous-traitant qui ne serait pas établi sur le territoire européen.

B – Quelques définitions

L'appropriation des principales mesures du Règlement européen et de leurs conséquences à venir dans le domaine des données personnelles nécessite de définir au préalable quelques concepts.

1. La notion de « données personnelles »

Le Règlement s'applique à toute donnée concernant une personne physique identifiée ou identifiable.

Une personne physique est réputée être « identifiable » dès lors qu'elle peut être identifiée, directement ou indirectement, par référence à un identifiant (nom, numéro d'identification..) ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, psychique, sociale…

2. La notion de « données en santé »

Le règlement européen donne une définition large et précise des données personnelles en santé, à savoir les données relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services ou de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.

La notion de données personnelles en santé vise également toute information concernant notamment un handicap, des risques de maladie, les antécédents médicaux ou un traitement clinique.

3. La notion de « traitement » des données

Le règlement européen définit le « traitement de données personnelles » comme toute opération appliquée à des données à caractère personnel, tel que la collecte, l'enregistrement, la structuration, la conservation de telles données.

4. La notion de « responsable du traitement »

Le responsable du traitement est toute personne physique ou morale qui seule, ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

C – Les principes fondamentaux du Règlement européen

Le Règlement européen pose les grands principes suivants:

- Licéité, loyauté et transparence : les données personnelles doivent être traitées de façon licite, loyale et transparente.
- Limitation des finalités : les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.
- Minimisation des données : les données personnelles doivent être traitées de façon adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.
- Exactitude : les données personnelles traitées doivent être exactes et, si nécessaire, tenues à jour. A ce titre, toutes les mesures raisonnables doivent être prises pour que les données inexactes, au regard des finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder.
- Limitation de la conservation : les données personnelles doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.
- Intégrité et confidentialité : les données personnelles doivent être traitées de façon à garantir une sécurité appropriée, y compris contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.
- Responsabilité : le responsable du traitement est responsable du respect de ces principes et doit être en mesure de démontrer qu'il les a respectés.

D – Les droits des personnes physiques dans le cadre du traitement de leurs données

Le Règlement européen reconnaît un certain nombre de droits aux personnes physiques dans le cadre du traitement de leurs données personnelles.

1. Une information claire et concise

Tout responsable de traitement doit, lors de la collecte de données personnelles, prendre les mesures nécessaires pour fournir une information concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée à un enfant.

Ces informations sont fournies par écrit. Toutefois, si la personne en fait la demande, ces informations peuvent être fournies à l'oral, dans la mesure où l'identité de la personne concernée peut être démontrée par d'autres moyens.

2 Une liste exhaustive des informations à communiquer

Les informations qui doivent être communiquées à la personne physique sont les suivantes :

- L'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement,
- Les coordonnées du délégué à la protection des données (cf. infra),
- Les finalités du traitement auquel sont destinées ces données ainsi que la base juridique du traitement (consentement, mission de santé ou sociale, intérêt légitime, contrat…),
- Les intérêts légitimes poursuivis par le responsable du traitement des données ou par un tiers,
- Les destinataires ou les catégories de destinataires des données à caractères personnels,
- La durée de conservation des données à caractère personnel ou, si cela n'est pas possible, les critères utilisés pour déterminer cette durée (ex : la durée de prise en charge dans un établissement ou service),
- le droit pour la personne physique de demander au responsable du traitement l'accès à ses propres données personnelles,
- le droit pour la personne physique de rectifier les données personnelles la concernant inexactes,
- le « droit à l'oubli », c'est-à-dire le droit à l'effacement, dans les meilleurs délais, de données personnelles concernant une personne physique
- le droit d'introduire une réclamation auprès d'une autorité de contrôle (La Commission Nationale Informatique et Liberté – CNIL – en France)
- le droit de retirer son consentement au traitement de données personnelles,
- des informations sur le fait de savoir si la fourniture de données personnelles est demandée sur le fondement d'une disposition règlementaire ou contractuelle, ou si elle conditionne la conclusion d'un contrat, et si la personne concernée est tenue de fournir les données personnelles, ainsi que les conséquences éventuelles de la non-fourniture de ces données,
- l'existence d'une décision automatisée, y compris un profilage, et en pareils cas, les informations concernant la logique sous-jacente et les conséquences de ce traitement pour la personne concernée.

IMPORTANT

Le règlement européen prévoit des dispositions spécifiques aux données en santé. Ainsi, il énonce comme principe l'interdiction du traitement de données à caractère personnel concernant la santé, sauf si notamment une des conditions suivantes est remplie :

- La personne concernée a donné son consentement explicite à leur traitement
- Le traitement est nécessaire pour la prise en charge sanitaire ou sociale de la personne

Ainsi, les établissements et services sociaux, médico-sociaux et sanitaires sont fondés à utiliser des données personnelles en santé sans le consentement préalable des usagers qu'elles accompagnent. Toutefois, une information préalable de ces derniers sur leurs différents droits est vivement conseillée.

E – La responsabilisation des acteurs en charge du traitement des données

Le règlement européen fait naître de nouvelles responsabilités pour les responsables de traitement de données personnelles, fondées sur différents principes.

1. Le principe de responsabilité

Le responsable du traitement des données doit mettre en œuvre les mesures techniques et organisationnelles nécessaires pour s'assurer et être en mesure de démontrer que le traitement des données est effectué conformément aux dispositions du Règlement européen.

Ces mesures, réexaminées et actualisées si nécessaire, doivent tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes physiques. La notion de risque doit tenir compte des degrés de probabilité et de gravité.

2. Le principe de protection des données dès la conception

Des mesures techniques et organisationnelles appropriées, telle que la « pseudonymisation », doivent être mises en œuvre par le responsable du traitement des données, tant au moment de la détermination des moyens qu'au moment du traitement lui-même.

La définition de ces mesures doit tenir compte de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques que présente le traitement pour les droits et libertés des personnes physiques.

3. Le principe de protection des données par défaut

Des mesures techniques et organisationnelles appropriées doivent être mises en œuvre par le responsable du traitement des données pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.

Ce principe s'applique non seulement à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, mais aussi à leur durée de conservation et à leur accessibilité.

4. Le principe de coresponsabilité

Lorsque deux responsables du traitement ou plus déterminent ensemble les finalités et les moyens du traitement, ils sont considérés comme les responsables conjoints du traitement. Ils doivent alors définir de façon transparente leurs obligations respectives afin d'assurer les exigences des règles édictées par le règlement européen.

5. Le principe de sécurité des traitements

Le responsable du traitement des données, et le cas échéant son sous-traitant, doivent, compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes physiques concernées, mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque y compris :

- La pseudonymisation et le chiffrement des données
- Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement,

- Des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique
- Une procédure visant à tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

IMPORTANT

La conséquence de cette responsabilisation des acteurs est la suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes.

Quant aux traitements soumis actuellement à autorisation, le régime d'autorisation pourrait être maintenu par le droit national (par exemple en matière de santé) ou être remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

Un projet de loi doit être présenté au Parlement pour préciser les modalités de mise en œuvre du régime de l'autorisation dans les semaines à venir. Le présent document « DECRYPTAGE » sera modifié en conséquence.

F – Les obligations liées à la violation des données et le renforcement des sanctions

Le principe de responsabilité a pour corollaire de rendre obligatoire le signalement de toute violation des données constatées par le responsable du traitement. Par ailleurs, les sanctions en cas de non-respect du règlement européen sont renforcées.

1. L'obligation de déclaration de toute violation

a) L'information de l'autorité de contrôle compétente

En cas de violation d'une donnée à caractère personnel, le responsable du traitement doit informer l'autorité de contrôle compétente (à ce jour, la CNIL) dans les meilleurs délais, et si possible 72 heures au plus tard après en avoir pris connaissance. Si la notification n'a pas lieu dans les 72 heures, les motifs du retard devront être expliqués dans la notification.

Cette notification doit :

- Décrire la nature de la violation des données y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation,
- Préciser le nom et les coordonnées du délégué à la protection des données ou d'un autre contact auprès duquel des informations supplémentaires peuvent être obtenues
- Décrire les conséquences probables de la violation des données
- Décrire les mesures prises, ou que le responsable du traitement propose de prendre, pour remédier à la violation des données à caractère personnel, y compris le cas échéant, les mesures prises pour en atténuer les éventuelles conséquences négatives.

Dans la mesure où il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées échelonnées.

b) L'information des personnes physiques concernées

Quand une violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation des données à la personne concernée dans les meilleurs délais.

Cette communication devra décrire, en des termes clairs et simples, la nature de la violation et contenir les éléments suivants :

- le nom et les coordonnées du délégué à la protection des données ou d'un autre contact auprès duquel des informations supplémentaires peuvent être obtenues
- les conséquences probables de la violation des données
- les mesures prises, ou que le responsable du traitement propose de prendre, pour remédier à la violation des données à caractère personnel, y compris le cas échéant, les mesures prises pour en atténuer les éventuelles conséquences négatives.

Toutefois, cette communication n'est pas nécessaire si une des conditions suivante est remplie :

- Des mesures de protection techniques et organisationnelles ont été mises en œuvre et ont été appliquées aux données personnelles affectées par la violation. Il s'agit de mesures qui rendent les données personnelles incompréhensibles pour toute personne qui n'est pas autorisée à y accéder, telle que le chiffrement,
- Des mesures ont été prises ultérieurement qui garantissent que le risque élevé pour les droits et libertés des personnes n'est plus susceptible de se matérialiser,
- La communication exigerait des efforts disproportionnés. Dans ce cas, il doit être procédé à une communication publique

2. Le renforcement du régime de sanctions

Les amendes administratives, en cas de non-respect du règlement européen, peuvent s'élever, selon la catégorie de l'infraction, jusqu'à 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, de 2% à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

G – L'obligation de recourir à des analyses d'impact

1. Contexte et contenu d'une analyse d'impact

Lorsque le traitement de données est susceptible d'engendrer des risques élevés pour les droits et libertés des personnes physiques, le responsable du traitement doit effectuer avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données personnelles.

Cette analyse d'impact doit tenir compte des éléments suivants :

- Une description du traitement et de ses finalités,
- Une évaluation de la nécessité et de la proportionnalité du traitement,
- Une appréciation des risques sur les droits et libertés des personnes concernées
- Les mesures envisagées pour traiter ces risques et se conformer au règlement

IMPORTANT

Le Règlement européen précise qu'une analyse d'impact est en particulier requise pour :

- Les traitements de données permettant de prendre des décisions à l'égard d'une personne sur la base d'une évaluation systématique et approfondie d'aspects personnels
- Le traitement à grande échelle de données sensibles

L'autorité de contrôle doit publier une liste des types d'opérations de traitement pour lesquelles une analyse d'impact sera requise. Au regard des dispositions du Règlement européen et de la nature des données traitées par les établissements et services sociaux, médico-sociaux et sanitaires, ils seront dans l'obligation de réaliser de telles études.

2. Le recours à une consultation préalable

Le responsable du traitement devra consulter l'autorité de contrôle (la CNIL) préalablement au traitement de données quand une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

Si l'autorité de contrôle estime que le traitement envisagé est de nature à constituer une violation du règlement européen, elle doit fournir dans un délai de 8 semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement.

H – La désignation d'un délégué à la protection des données

1. Contexte de désignation d'un délégué à la protection des données

Un délégué à la protection des données doit être désigné par le responsable du traitement des données personnelles quand notamment :

- les activités de base du responsable du traitement consistent à effectuer des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées
- les activités du responsable du traitement consistent en un traitement à grande échelle de données « sensibles », telles que les données en santé.

Un groupe d'entreprise (et donc d'établissements et/ou d'association) peut désigner un seul délégué à la protection des données à condition qu'il soit facilement joignable à partir de chaque lieu.

2. Les qualités du délégué à la protection des données

Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données.

Il peut être un membre du personnel du responsable du traitement ou exercer ses missions sur la base d'un contrat de service.

Soumis au secret professionnel ou à une obligation de confidentialité dans l'exercice de ses missions, il peut exécuter d'autres missions et tâches dans la mesure où elles n'entraînent pas de conflit d'intérêt.

Le responsable du traitement des données doit publier les coordonnées du délégué à la protection des données et les communiquer à l'autorité de contrôle.

3. Les fonctions et le statut du délégué à la protection des données

Le délégué à la protection des données doit être associé à toutes les questions relatives à la protection des données à caractère personnel.

A ce titre, le responsable du traitement doit l'aider à exercer ses missions en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement.

Le responsable du traitement doit veiller à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice de sa mission et ne peut être relevé de ses fonctions ou pénalisé pour l'exercice de ses missions.

Le délégué à la protection des données doit faire directement rapport au niveau le plus élevé de la direction du responsable du traitement. Par conséquent, un directeur d'association ou d'établissement public ne peut exercer la fonction de délégué à la protection des données de sa structure.

Par ailleurs, le délégué à la protection des données peut être sollicité par toute personne concernée au sujet de toutes questions relatives au traitement de leurs données personnelles et à l'exercice de leurs droits.

3. Les missions du délégué à la protection des données

Le délégué à la protection des données doit exercer les missions suivantes :

- Informer et conseiller le responsable du traitement ainsi que les salariés qui procèdent au traitement sur les obligations qui leur incombent en matière de protection des données,
- Contrôler le respect du règlement européen, y compris concernant la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant,
- Dispenser des conseils, sur demande, relatif à l'analyse d'impact et vérifier l'exécution de celle-ci
- Faire office de correspondant avec l'autorité de contrôle et coopérer avec cette dernière. A ce titre, le délégué devra faciliter l'accès par l'autorité de contrôle aux documents et informations dans le cadre de l'exercice des missions et des pouvoirs de cette autorité.

Dans le cadre de ses missions, le délégué doit tenir compte du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités de traitement.

I – Les différentes étapes de mise en conformité avant le 25 mai 2018

LA CNIL a mis en ligne un guide en ligne pour aider les structures à répondre aux nouvelles obligations issues du règlement européen, dont DECRYPTAGE vous présente une synthèse. https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf

1. Désigner un pilote

Ce pilote sera soit le délégué à la protection des données, soit une personne qui, disposant de relais internes, serait chargée de la mise en conformité au règlement européen. Il devra piloter la gouvernance des données personnelles de la structure.

2. Cartographier vos traitements de données personnelles

Afin de mesurer l'impact du règlement européen sur l'activité de l'établissement ou du service et répondre aux exigences de ce dernier, il sera nécessaire de procéder aux recensements suivants :

- Les différents traitements des données personnelles
- Les catégories de données personnelles recensées
- Les objectifs poursuivis par les opérations de traitement des données
- Les acteurs (internes et externes) qui traitent ces données, notamment les prestataires sous-traitants
- L'origine et la destination des données

Pour chaque traitement de données personnelles, il conviendra de se poser les questions suivantes : Qui ? Quoi ? Pourquoi ? Quand ? Comment ? Jusqu'à quand ?

3. Tenir un registre

Il conviendra de mettre en place un registre permettant de s'assurer de la conformité du traitement des données au regard des dispositions du règlement européen et de sa licéité.

Ce registre devra notamment mentionner :

- Le nom et les coordonnées du responsable de traitement,
- Les différents traitements de données personnelles,
- Les catégories de données personnelles traitées,
- Les différentes catégories de personnes concernées,
- Les objectifs poursuivis par les opérations de traitement des données
- Les acteurs internes et externes qui traitent ces données
- Les durées de conservation
- La description générale des mesures de sécurité techniques et organisationnelles

Ce registre doit permettre au responsable du traitement d'identifier les actions à mener en priorité.

4. Prioriser les actions

Suite à l'identification des données personnelles traitées au sein de l'organisme, il conviendra d'identifier les actions à mener pour être en conformité avec les dispositions du règlement européen et de les prioriser au regard des risques que font peser les traitements de données sur les libertés des personnes concernées.

5. La gestion des risques : l'étude d'impact

Dans la mesure où le responsable de traitement des données aura un doute sur un risque lié au traitement de données sur les droits et la vie privée des personnes, il devra mener une étude d'impact (cf. supra).

6. Organiser les processus internes

Afin de garantir en permanence un haut niveau de protection des données personnelles, il est nécessaire de mettre en place des procédures internes permettant de s'assurer de la protection des données à tout moment et tenant compte des évènements qui peuvent survenir tout au long du traitement des données.

La mise en place de ces processus internes nécessite notamment de :

- Prendre en compte la protection des données personnelles dès la conception d'un traitement
- Organiser la remontée d'information en construisant notamment un plan de formation et de communication auprès du personnel
- Traiter les réclamations et les demandes des personnes concernées sur l'exercice de leurs droits
- Anticiper les violations de données et prévoir le cas échéant les procédures de notification à l'autorité compétente et aux personnes concernées dans les meilleurs délais.

7. Documenter et garantir la conformité

Le responsable du traitement des données devant prouver la conformité aux dispositions du Règlement, un dossier permettant de démontrer cette conformité doit être élaboré.

Ce dossier devra comporter notamment :

- Le registre
- Les études d'impact
- Les mentions d'informations auprès des personnes
- Les modalités d'exercice des droits des personnes (consentement si il est requis, droit d'accès, de rectification et de suppression)
- Les contrats de sous-traitance
- Les procédures internes en cas de violation des données
- Les politiques de sécurité informatique.