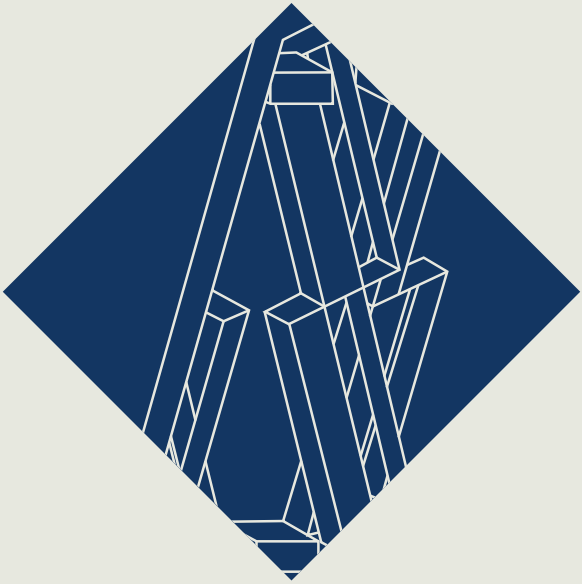
HOUDART ET ASSOCIÉS

SOCIÉTÉ D'AVOCATS



PROTECTION DES DONNÉES RGPD

SOMMAIRE

I Protection des données et RGPD 1

II Qui est concerné dans le secteur de la santé ? 4

III Quelques définitions 5

IV Les principes relatifs au traitement des données à caractère personnel 7

V Le calendrier 9

VI Comment se conformer au RGPD ? 10

VII Nos solutions et missions 11

VIII Nos actions et objectifs 17

I. PROTECTION DES DONNÉES ET RGPD

Le développement des innovations technologiques et organisationnelles dans le secteur de la santé implique le respect de règles nouvelles.

En se dotant d'une offre d'accompagnement à la protection des données, le cabinet Houdart et Associés s'engage à accompagner les acteurs concernés dans la sécurisation de leurs projets et de leurs activités au regard des exigences nouvelles du Règlement Général sur la Protection des Données (RGPD).

La protection des données personnelles est devenue un enjeu crucial pour les entreprises, les établissements et les professionnels du secteur de la santé.

1. Application du RGPD

- **Il impose aux acteurs concernés de se responsabiliser fortement au regard des garanties de sécurité des données qu'ils collectent et qu'ils traitent (Principe d'Accountability).**

Le régime de déclaration à la CNIL sera remplacé par ce principe de responsabilité qui implique davantage de contrôle et de conformité interne pour les acteurs concernés. Il ne suffira plus de simplement déclarer ses traitements pour être conforme, au contraire il faudra prouver, par la mise en place de procédures internes et d'outils de sécurité adaptés, que la conformité est respectée en cas de contrôle.

- **Il renforce les droits des personnes** concernées par le traitement des données (consentement, droit à l'oubli, droit à la portabilité, droit d'accès, etc.)

- **Il élargit le champ d'application territorial et matériel en matière de protection des données**. La protection des données concerne toutes les structures, de toutes tailles et de tous secteurs dans toute l'Union européenne. Le RGPD peut également s'appliquer à une structure se situant en dehors de l'UE dès lors que celle-ci traite des données personnelles de résidents européens.

Le RGPD concerne alors tous les responsables de traitement de données à caractère personnel **et tous les sous-traitants** intervenant sur ce type de traitement.

2. Les risques pour tout responsable de traitement et sous-traitant

- **Les risques juridiques :** Le principe d'accountability implique l'engagement de la responsabilité du responsable de traitement, voire même celle du sous-traitant. Le dispositif contractuel de chacun de ces acteurs doit être révisé afin de limiter les risques juridiques (clauses de protection, données personnelles, politique de confidentialité, mentions légales, etc.)

- **Les risques organisationnels :** L'alignement des procédures aux exigences du RGPD nécessite une opération de conduite du changement notamment auprès du personnel et des organisations internes afin de limiter le risque d'atteinte à la protection des données traitées (élaboration d'un cadre de gestion, formation, processus de contrôle et de gestion des risques).

- **Les risques techniques :** Ces risques peuvent porter atteinte à la sécurité et à l'intégrité des données (altération ou fuite des données, hacking, etc.). La sécurité informatique est un élément essentiel en matière de protection des données. Un audit technique des systèmes d'information et de sécurisation du traitement des données est indispensable.

3. Les sanctions

Les manquements aux obligations de la réglementation européenne sont sanctionnés à l'article 83 par des amendes administratives :

- Jusqu'à 10 millions d'euros, voire jusqu'à 20 millions d'euros selon le type de manquement pour tout responsable de traitement ou sous-traitant personne physique ou morale hors entreprise : associations, établissements de santé, professionnels de santé ou toute autre structure concernée par le RGPD.

- Jusqu'à 2%, voire jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent lorsqu'il s'agit d'une entreprise.

II. QUI EST CONCERNÉ DANS LE SECTEUR DE LA SANTÉ ?

Les acteurs du secteur de la santé sont concernés à double titre, dès lors que le traitement des données est caractérisé et concerne un résident de l'Union européenne et ce, quelle que soit son implantation :

- Le traitement de données à caractère personnel de leurs employés, fournisseurs, clients, prestataires, etc.

- Le traitement de données de santé spécifiques au secteur (données de santé des patients, données de santé du personnel).

La liste présentée ci-dessous n'est pas exhaustive. Une étude particulière de toutes les opérations de traitement des acteurs est nécessaire afin de déterminer leur soumission ou non au RGPD.

- **Les entreprises de toute taille traitant des données de santé** de patients ou d'utilisateurs de services (produits de santé, applications santé, intelligence artificielle, logiciels, etc.)

- **Les établissements de santé**, publics ou privés

- **Les établissements médico-sociaux** (EHPAD, centres d'action médico-sociale, etc.)

- **Les structures d'exercice collectif** (maisons de santé, centres de soins, activités de biologie, d'imagerie médicale, etc.)

- **Associations intervenant dans le champ de la santé** (associations de patients, d'usagers etc.)

- **Les professionnels de santé** traitant des données de santé de leurs patients

III. QUELQUES DÉFINITIONS

- Données à caractère personnel

Toute information se rapportant à une personne physique identifiée ou identifiable . Est réputée être une « personne physique identifiable », 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 concernant la santé

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.

- Données génétiques

Les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne en question.

- Traitement

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqué 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 tout autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

- Responsable de traitement

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 (...).

- Sous-traitant

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 de traitement.

- Violation de données à caractère personnel

Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

IV. LES PRINCIPES RELATIFS AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

(cf. Article 5 du RGPD)

- Licéité, Loyauté, Transparence

Ces trois principes impliquent la nécessité d'établir un fondement juridique valable et de bonne foi à l'égard de l'opération de traitement des données personnelles, tout en assurant la transparence liée aux finalités de ces opérations.

- Limitation des finalités de traitement

Les finalités des opérations de traitement de données personnelles doivent être déterminées, explicites et légitimes. Les finalités initiales respectant ces trois caractéristiques ne doivent pas être détournées.

- Minimisation des données

Les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités des opérations de traitement déterminées.

- Exactitude des données

Les données personnelles traitées doivent être tenues à jour à travers des mesures raisonnables, et si besoin faire l'objet de rectification ou d'effacement.

- Limitation de la conservation

La durée de conservation des données personnelles ne doit pas excéder la durée nécessaire prévue au regard des finalités déterminées des opérations de traitement. Elles peuvent être conservées plus longtemps en cas de traitement à des fins archivistiques, de recherche scientifique ou historique, ou à des fins statistiques.

- Intégrité

Les mesures de sécurité relatives au traitement des données personnelles doivent garantir la protection de celles-ci contre le traitement non autorisé ou illicite, et contre la perte, la destruction ou l'altération de ces données.

- Confidentialité

Les mesures techniques et organisationnelles relatives à la protection des données doivent garantir le respect de la confidentialité de ces données par le responsable de traitement et le sous-traitant, mais également par leur personnel ou agents.

- Responsabilité

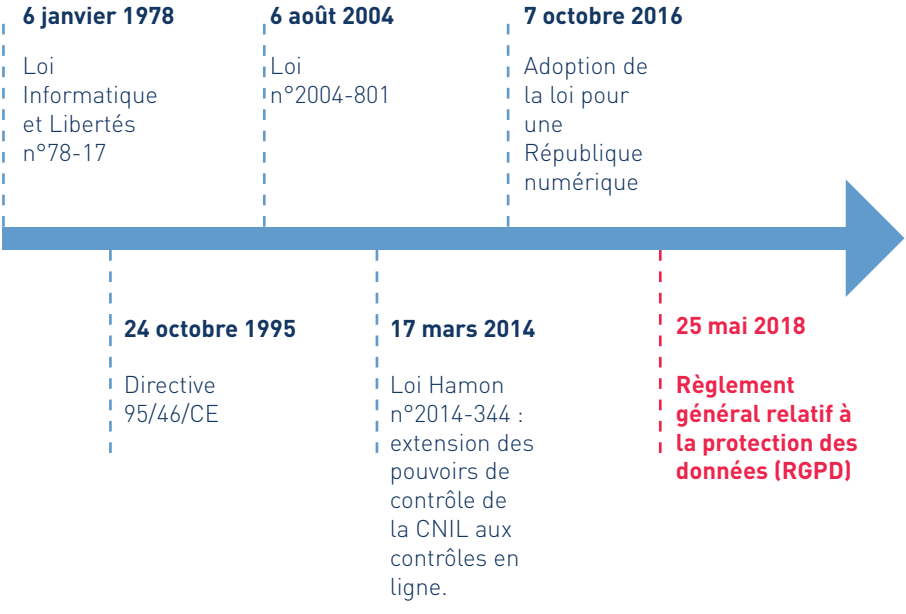
Le responsable de traitement est tenu de prouver le respect de tous les principes relatifs à la protection des données énumérés ci-dessus. Il en est le responsable principal.

V. LE CALENDRIER

Le **RGPD**, adopté le 27 avril 2016, a été le fruit de nombreuses législations et réglementations à la fois nationales et européennes.

Il harmonise le cadre juridique européen en matière de protection des données.

Son application est prévue **le 25 mai 2018**.



LES ACTEURS CONCERNÉS PAR L'APPLICATION DU RGPD DOIVENT SE PRÉPARER RAPIDEMENT ET SÉRIEUSEMENT AVANT LE 25 MAI 2018 ET PROUVER LEUR CONFORMITÉ AUX EXIGENCES NOUVELLES EN MATIÈRE DE PROTECTION DES DONNÉES.

VI. COMMENT SE CONFORMER AU RGPD ?

VII. NOS SOLUTIONS ET MISSIONS

AUDIT DE MISE EN CONFORMITÉ

ANALYSE D'IMPACT OBLIGATOIRE (PIA) : ARTICLE 35 du RGPD

RÉDACTION D'ANALYSE ET DE DOCUMENTS LÉGAUX

FORMATIONS

DPO EXTERNALISÉ - ARTICLE 37 du RGPD

AUDIT DE MISE EN CONFORMITÉ

CARTOGRAPHIE DES TRAITEMENTS DE DONNÉES A CARACTÈRE PERSONNEL

L'objectif est de déterminer avec précision :

- la nature des données concernées
- le type de traitement effectué
- les finalités du traitement
- les modalités et durée de conservation
- la typologie et les conditions d'accès et d'effacement des données
- le transfert ou échange des données.

Livrable : Un registre de traitement, article 30 – RGPD

AUDIT ORGANISATIONNEL

L'objectif de l'audit organisationnel est :

- d'analyser les procédures mises en œuvre en matière d'accès aux données par les personnes internes et externes
- d'analyser les flux de données opérés
- d'analyser la politique de protection des données (si existante)
- de vérifier le respect de la procédure de recueil du consentement de la personne concernée
- de mesurer les moyens de sécurité mis en œuvre en matière d'accès aux données
- de déterminer les ressources humaines, matérielles et financières disponibles pour la protection des données.

ANALYSE DU SYSTÈME DE SÉCURITÉ INFORMATIQUE

L'audit du système de sécurité de protection des données est nécessaire afin de vérifier si des mesures techniques sont mises en œuvre pour respecter les principes d'intégrité et de confidentialité des données.

PROGRAMME D'ACTIONS PRÉVENTIVES & CORRECTIVES

Un rapport d'audit listant toutes les failles de sécurité ou points d'amélioration recensés dans le cadre de l'audit sera délivré (élaboration et révision de process). Ce rapport sera accompagné d'un calendrier de mise en œuvre des actions correctives en fonction des risques et des priorités de mise en conformité.

ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

Article 35 - RGPD

L'analyse d'impact relative à la protection des données est obligatoire lorsque le traitement des données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. L'analyse doit être réalisée avant le traitement. Les acteurs traitant à grande échelle des données de santé sont concernés par cette obligation.

SCHÉMA DES OPÉRATIONS DE TRAITEMENT

L'analyse d'impact doit comporter une description systématique :

- des opérations de traitement
- des finalités du traitement
- et, le cas échéant, de l'intérêt légitime poursuivi par le responsable de traitement.

Nous nous engageons à vous accompagner dans toutes ces étapes de mise en conformité juridique et technique afin de déterminer les risques liés au traitement de données et d'assurer la conformité au RGPD.

RAPPORT D'ÉVALUATION

L'analyse d'impact comportera une évaluation :

- de la nécessité
- et de la proportionnalité des opérations de traitement au regard des finalités.

Elle comportera également une évaluation des risques pour les droits et libertés des personnes dont les données sont traitées.

Outil : La méthodologie de gestion des risques EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), Agence nationale de la sécurité des systèmes d'information.

PROGRAMME DES MESURES DE SECURITÉ

Un rapport des mesures, garanties et mécanismes de sécurité sera remis en fin de mission afin d'assurer la protection des données et de prouver la mise en conformité du traitement au RGPD.

RÉDACTION DE NOTES D'ANALYSE, DE CLAUSES ET DE DOCUMENTS LÉGAUX

Le RGPD impose à tout responsable de traitement et à tout sous-traitant de prouver sa conformité aux nouvelles exigences principalement par la documentation.

Le régime de responsabilité venant se substituer au régime de déclaration, les acteurs doivent davantage se protéger notamment dans leurs relations avec les personnes concernées par le traitement de données, mais également avec leurs partenaires.

La gestion des risques en matière de responsabilité impose une protection juridique spécifique à la protection des données.

Nos domaines d'expertise :

- notes juridiques relatives à l'application du RGPD et des enjeux en matière d'organisation
- politique de confidentialité
- mentions légales
- clauses « Protection des données à caractère personnel »
- accord de confidentialité (à destination des partenaires, des fournisseurs et des employés)
- conditions générales d'utilisation
- conditions générales de vente

FORMATIONS SUR MESURE

Catalogue général des formations :

- Enjeux et risques liés à la protection des données de santé
- RGPD et responsable de traitement
- RGPD et sous-traitant
- RGPD et DPO
- Comment réaliser une analyse d'impact ?

En cas de besoin spécifique, nous nous engageons à vous proposer un catalogue de formations adapté à vos attentes, à votre organisation, à votre secteur et à votre activité.

Nos formations peuvent être effectuées en Web-conférence, sur site ou bien au sein du cabinet.

DÉLÉGUÉ À LA PROTECTION DES DONNÉES
DATA PROTECTION OFFICER (DPO)

Article 37 - RGPD

Vous êtes un responsable de traitement ou un sous-traitant , vous avez l'obligation de nommer un DPO si :

- vous êtes une autorité publique ou un organisme public
- vous êtes une entité privée ou publique et vos activités de base consistent en 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
- vous êtes une entité privée ou publique et vos activités de base consistent en un traitement à grande échelle de catégories particulières de données

Catégories particulières de données :

- les données concernant la santé
- les données génétiques
- les données biométriques
- les données concernant la vie sexuelle ou l'orientation sexuelle
- les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale

Dès lors, tous les acteurs de la santé, publics ou privés, qui traitent des données énumérées ci-dessus à grande échelle sont tenus de nommer un DPO soit en interne, soit en faisant appel à un prestataire externe qualifié, l'acteur concerné demeurant l'unique responsable des opérations de traitement.

Le Cabinet Houdart et Associés propose d'être le DPO des acteurs de santé (établissements de santé, fédérations, industries, startup, associations etc.).

Conformément à l'article 39 du RGPD, nous nous engageons à :

- vous informer et vous conseiller sur les obligations qui vous incombent à vous et à vos employés
- contrôler le respect du RGPD au sein de votre organisation
- sensibiliser et former votre personnel participant aux opérations de traitement
- vous dispenser des conseils sur demande s'agissant de l'analyse d'impact relative à la protection des données
- coopérer avec la CNIL et être le point de contact officiel.

Le DPO est soumis au secret professionnel et à une obligation de confidentialité.

VIII. NOS ACTIONS ET OBJECTIFS

>> Pour un accompagnement compétent et complet :

- Mobilisation de toutes nos compétences juridiques internes spécialisées en droit des nouvelles technologies et en protection des données

- Partenariat avec des acteurs spécialisés dans le secteur de l'ingénierie technique des systèmes d'information

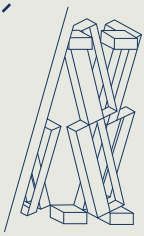
>> Pour un accompagnement sécurisé et vigilant :

Disponibilité

Efficacité

Rigueur

Réactivité



HOUDART ET ASSOCIÉS

SOCIÉTÉ D'AVOCATS

+33 (0)1 40 21 45 45
cabinet@houdart.org
www.houdart.org