Fiche 6.

L'analyse d'impact relative à la protection des données à caractère personnel (AIPD)

Check-list des bonnes pratiques à respecter :

- → Lorsque je réalise un traitement de données, j'évalue les risques potentiels d'atteinte à la protection des données de mes patients et j'essaye d'y répondre en adoptant des mesures adéquates ;
- → S'il existe un risque **élevé** pour la protection des données de mes patients (ex : participation à des recherches scientifiques, recours à des nouvelles technologies et à la télémédecine), je suis tenu de réaliser une « AIPD » ;
- → Dans l'hypothèse où je suis tenu de réaliser une AIPD, je veille à la réaliser avant que le traitement des données commence, à suivre une certaine méthodologie et à évaluer régulièrement les résultats de l'AIPD.
- → Si les mesures de protection prises pour limiter les risques d'atteinte à la vie privée de mes patients ne suffisent pas, j'en informe l'Autorité de Protection des Données (APD).

Qu'est-ce qu'une « AIPD » ?

L'analyse d'impact relative à la protection des données (AIPD ou DPIA pour *Data Privacy Impact Assessment*) désigne la **procédure qui a pour objet de décrire et d'évaluer les différents risques afférents aux traitements des données à caractère personnel**. L'enjeu étant **d'identifier les risques potentiels** d'atteinte à la protection des données et **d'essayer d'y répondre** en adoptant des mesures de protection adéquates.

L'AIPD est un **outil important** du RGPD qui permet de responsabiliser tout acteur qui traite des données à caractère personnel. L'AIPD vous aidera dans la **mise en place des traitements de données plus respectueux de la vie privée** et vous permettra en outre de **démontrer que vous avez pris toutes les mesures appropriées**, conformément au respect du principe « *accountability* »[1].

La réalisation d'une AIPD est-elle obligatoire ?

NON.

L'article 35 du RGPD prévoit l'obligation de réaliser une AIPD uniquement lorsqu'un type de traitement de données personnelles, en particulier par le **recours à de nouvelles technologies**, est susceptible d'engendrer un ***risque élevé*** **pour les droits et libertés des personnes concernées** (*à savoir, le patient*), compte tenu de la nature, de la portée, du contexte et des finalités du traitement de données.

Une analyse d'impact est notamment obligatoire en cas de [2] :

- **Evaluation systématique et approfondie d'aspects personnels** fondée sur un **traitement automatisé** (*en ce compris le profilage*), et sur la base de laquelle sont prises des décisions produisant des effets juridiques ou des effets à l'impact similaire pour la personne concernée (*ex : le traitement de big data*);
- **Traitement de données sensibles**[3] **à grande échelle** (*ex : les données de santé des patients/occupants d'un établissement de soins*) ;
- Surveillance systématique **à grande échelle** des **locaux accessibles au public** » (*ex : la surveillance par caméras*).

L'Autorité de Protection des Données (APD) a établi une **liste officielle des types de traitement pour lesquels une AIPD est également obligatoire**[4]**.**

[1] Pour rappel le principe « *accountability* » signifie que le responsable du traitement des données doit garantir le respect des exigences du RGPD et être à même de démontrer que son traitement est en conformité avec ces exigences (article 5 du RGPD).
[2] Article 35, § 3 du RGPD.
[3] « Données sensibles » : « 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 ».

Dans le cadre de votre pratique professionnelle, **trois critères** vont vous permettre de déterminer si vous devez réaliser une AIPD ou non.

- **1er critère : la notion de « risque probablement élevé »**

Bien que la notion de risque soit omniprésente dans le RGPD, la définition de la notion de « risque élevé » est relativement floue. L'Autorité de Protection des Données(APD) estime que la notion de « risque élevé » renvoie aux traitements de données qui sont ou pourront être **susceptibles**[5] d'avoir des **incidences négatives sensibles**[6] pour les libertés et droits fondamentaux des personnes physiques[7].

Par conséquent, dès que vous recourrez à une **nouvelle technologie** qui expose, compte tenu de la nature, de la portée et du contexte et des finalités du traitement, le patient à un ***risque élevé*** pour ses droits et libertés, vous devez **réaliser une AIPD**. Le recours à une nouvelle technologie implique presque toujours un risque d'atteinte au respect des droits et libertés individuelles du patient.

Lorsque vous réalisez ou participez à une **recherche scientifique**, vous êtes également tenu, en votre qualité de chercheur/investigateur, de **réaliser une AIPD** si le traitement de données présente un ***risque élevé*** pour les droits et libertés des sujets étudiés.

☝ *A contrario*, lorsque vous réalisez des **analyses internes de suivi de vos patients**, bien que le nombre de données collectées puisse paraître important, vous n'exposez **pas** ces derniers à un risque élevé d'atteinte à la protection de leurs données personnelles. Vous ne devez donc pas réaliser préalablement une AIPD.

- **2ème critère : le traitement de données sensibles « à grande échelle »**

En vertu de ce 2ème critère, seuls les traitements de données de santé « ***à grande échelle*** » nécessitent la réalisation d'une AIPD.

Afin d'évaluer si un traitement de données est « à grande échelle », vous devez tenir compte du nombre de patients concernés, du volume de données traitées, de la diversité des données, du nombre de personnes qui traitent les données, de la durée de conservation des données et de la portée géographique du traitement.

---

[4] https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Liste_des_traitements_AIPD.pdf

[5] L'expression "susceptible de" ne signifie pas qu'il existe une lointaine possibilité d'incidence sensible. L'incidence sensible doit être plus probable qu'improbable. En revanche, cela signifie également qu'il n'est pas nécessaire que les personnes soient réellement affectées : la probabilité qu'elles soient sensiblement affectées suffit pour répondre à ce critère.

[6] Une "conséquence négative sensible" signifie que, dans le cas où le risque se produirait, la personne concernée serait sensiblement affectée dans l'exercice ou la jouissance de ses libertés et droits fondamentaux.

[7] https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2018.pdf

Compte tenu de ces éléments, **que vous exerciez votre activité professionnelle « en solo » ou « en groupe », vous ne réalisez pas de traitements de données sensibles à grande échelle**, à l'inverse d'un hôpital qui brasse lui d'énormes volumes de données. Par conséquent, vous n'êtes pas soumis à l'obligation de réaliser une AIPD[8].

- **3ème critère : la liste officielle de l'Autorité de Protection des Données (APD)**

En vertu de cette liste, vous devez obligatoirement réaliser une AIPD lorsque :

- des données de santé sont collectées par voie automatisée à l'aide d'un dispositif médical implantable actif ;
- des données sont collectées à grande échelle auprès de tiers afin d'analyser ou de prédire la santé ;
- des données sensibles sont échangées systématiquement entre plusieurs responsables de traitement ;
- des données sont générées, à grande échelle, au moyen d'appareils dotés de capteurs qui « télémonitorent » les patients, comme les objets connectés.

Que devez-vous retenir ?

OBLIGATION DE RÉALISER UNE AIPD	PAS OBLIGATION DE RÉALISER UNE AIPD
1. Recherches scientifiques 2. Recours à une nouvelle technologie (*ex : objets connectés*) 3. Télémédecine	1. Tenue d'un dossier patient 2. Analyses internes de suivi des patients 3. Autres
⇨ **Risque élevé**	⇨ **Pas de risque élevé**

L'obligation de réaliser une AIPD (dans certaines situations) est indépendante de votre obligation d'assurer la confidentialité et la sécurité des données de vos patients.

A quel moment faut-il réaliser une AIPD ?

L'AIPD doit être menée **avant** la mise en œuvre du traitement des données. Elle doit être démarrée le plus en amont possible et doit être mise à jour tout au long du cycle de vie du traitement.

[8] Considérant 91 du RGPD : « *Le traitement de données à caractère personnel ne devrait pas être considéré comme étant à grande échelle si le traitement concerne les données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel. Dans de tels cas, une analyse d'impact relative à la protection des données ne devrait pas être obligatoire* ».

Qui est chargé de la réalisation d'une AIPD ?

Vous assumez, en tant responsable de traitement, toujours la responsabilité finale afférente à la réalisation de l'AIPD en ce qui concerne les traitements de données qui relèvent de votre responsabilité.

Nonobstant, si vous avez désigné **un référent à la protection des données**, son avis peut être sollicité notamment sur la question de savoir si une AIPD est obligatoire, sur la méthodologie devant être suivie et sur les mesures nécessaires à prendre pour limiter les risques identifiés.

Lorsque le traitement des données a nécessité **l'intervention d'un sous-traitant**, ce dernier devra également aider à la réalisation de l'AIPD.

Remarque : lorsque vous n'êtes pas reconnu légalement comme « responsable de traitement » (dans le cadre d'une étude menée par Sciensano ou d'un projet e-santé mené par la région wallonne par exemple), ce n'est pas à vous de réaliser l'AIPD. Cette dernière sera initiée par celui qui est désigné comme légalement « responsable de traitement » (dans l'exemple donné, Sciensano ou la région wallonne)

Quelle méthodologie suivre pour réaliser une AIPD ?

Le RGPD ne précise pas de méthode pour évaluer, de manière objective, les risques liés à la protection des données personnelles.

Si vous êtes en principe libre de décider de la méthodologie à suivre pour réaliser une AIPD, cette dernière doit **contenir au minimum les éléments suivants**[9] :

- Une **description des traitements** visés comprenant les aspects techniques et opérationnels ainsi que les finalités du traitement;
- Une **évaluation, de nature plus juridique, des principes et droits fondamentaux des personnes concernées** (transparence et loyauté, nécessité et proportionnalité, limitation de la durée de conservation des données, droits des personnes concernées…) ;
- Une **analyse, des risques sur les droits et libertés des personnes concernées** (y compris l'identification des risques, l'attribution de valeurs de risques et la détermination de valeurs de risques acceptables) ;
- Une **description, de nature plus technique, des mesures de protection envisagées** afin d'appréhender les risques (mécanismes de sécurité et garanties de protection des données manipulées).

Remarque : une seule AIPD peut suffire si les traitements de données sont similaires et présentent les mêmes risques pour les patients concernés.

[9] Article 35, § 7 du RGPD.

La CNIL, autorité de protection des données française, a développé un logiciel gratuit vous permettant de réaliser une AIPD selon cette méthodologie.

Vous pouvez télécharger cet outil à l'adresse suivante : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

Que faire des conclusions de l'AIPD ?

L'analyse d'impact pour la protection des données personnelles doit pouvoir déboucher sur **la définition et l'adoption de mesures adéquates pour faire face aux risques identifiés**.

Dans l'hypothèse où **les mesures de protection prises pour minimiser les risques** d'atteinte à la protection de la vie privée de vos patients ne suffisent pas, vous devez **en avertir préalablement l'APD**[10]. **L'APD remettra alors un avis** endéans un délai de huit semaines[11], l'objectif étant pour l'APD de vérifier que les traitements de données soient bien conformes au RGPD.

Il est également nécessaire de **réévaluer** les conclusions de l'AIPD de manière régulière pour s'assurer que le niveau de risque reste acceptable tout au long de la vie du « traitement » des données, dans la mesure où l'environnement, technique notamment, sera amené à évoluer, ce qui nécessitera d'adapter les mesures mises en œuvre.

Pouvez-vous être sanctionné ?

Si, au regard des trois critères analysés ci-dessus, vous n'êtes pas tenus de réaliser une AIPD, vous ne serez soumis à aucune sanction du RGPD.

Pour e-santéwallonie,
Emeraude Camberlin, Juriste.

[10] Article 36, §1 du RGPD.
[11] Article 36, §2 du RGPD.