Agence fédérale des médicaments et des produits de santé

Analyse d'impact relative à la protection des données (AIPD)

Numéro de SOP : DPO/002/SOP/F (1)

Nombre total de pages : 24

Annexe(s) : 1

Cette procédure est destinée à guider les responsables internes de traitement de données (que ce soit un traitement informatisé ou manuel) à conduire une analyse d'impact relative à la protection des données à caractère personnel, conformément aux exigences du Règlement Général de Protection des Données (RGPD).

	Nom	Fonction	Signature
Vérifié par	Nicolas Vervaeck	Data Protection Officer – Soutien transversal	
Approuvé par	Xavier De Cuyper	Administrateur général	
	Greet Musch	Directeur général – DG PRE	
	Hugues Malonne	Directeur général – DG POST	
	Ethel Mertens	Directeur général – DG INSP	

Date d'application : voir « Application Date » dans DMS Quality

TABLE DES MATIERES

Annexes

Annexe 1 Evaluation de risques

Analyse d'impact relative à la protection des données (AIPD)

1. Champ d'application et responsabilités

1.1. Champ d'application

Cette procédure est destinée à guider les responsables internes de traitement de données (que ce soit un traitement informatisé ou manuel) à conduire une analyse d'impact relative à la protection des données à caractère personnel, conformément aux exigences du Règlement Général de Protection des Données (RGPD).

- Cette procédure décrit la méthodologie, l'outil et les étapes pratiques pour l'exécution d'une **analyse d'impact** relative à la protection des données (AIPD) à caractère personnel, que ces données fassent l'objet d'un **traitement automatisé ou non**, de façon à pouvoir démontrer la conformité du traitement aux exigences du Règlement Général de la Protection des Données (RGPD).
- Le traitement concerné peut être un **traitement futur** (non encore mis en place, mais envisagé dans le cadre d'un projet), ou un **traitement déjà en place**.

Cette procédure est applicable tant pour effectuer la toute **première analyse** d'impact d'un traitement que pour réviser et mettre à jour les résultats d'une **analyse précédente**

- en réaction à de nouveaux événements immédiats
- ou dans le cadre d'une révision biannuelle des risques effectuée dans un esprit d'amélioration continue ou pour identifier les changements depuis la dernière analyse

1.2. Responsabilités

Cette procédure est **principalement** destinée aux responsables internes des traitements de données (= "Responsables Internes de Traitement", RIT), qui endossent la responsabilité directe de l'analyse.

Cette procédure est **également** destinée à guider les autres intervenants qui apportent leur aide au RIT:

- les experts « sécurité » qui contribuent à l'analyse
    - tout particulièrement le Data Protection Officer (DPO) de l'agence, qui a pour rôle de vérifier que la procédure est bien suivie, que les résultats sont correctement documentés et plausibles, de garder ces informations pour répondre aux demandes d'audit, et de guider vers des ressources utiles comme des Bases de Connaissance (*Knowledge Bases*) et des directives particulières (*guidelines*).
    - le Conseiller en Sécurité de l'Information (CSI) de l'agence, qui a pour rôle de donner des conseils pour ce qui concerne la sécurité de l'information, et de veiller à ce que la politique de l'agence concernant la sécurité de l'information soit correctement appliquée.

- les experts de la Division Qualité, qui peuvent apporter une aide pour comprendre et appliquer les « analyses de risque » du AIPD.
- les experts de la Division Juridique, qui peuvent clarifier des textes du RGPD, ainsi que les bases légales du traitement concerné.
- les experts du « business » concerné, qui ont une connaissance approfondie des données traitées, des flots de données et des raisons « business » du traitement, comme des représentants des personnes concernées à l'AFMPS qui traitent les données.
- les experts ICT concernés **lorsque le traitement est automatisé**, qui ont une connaissance des technologies utilisées et peuvent donc indiquer les risques d'origine technique et les contre-mesures mises en place ou à mettre en place.
- Si possible, un représentant des personnes concernées dont on traite des données à caractère personnelle.

2. But de la procédure

Cette procédure décrit comment effectuer une analyse d'impact pour tous les traitements (automatiques ou non) de données à caractère personnel pour lesquels on estime qu'il y aurait un risque élevé pour les droits et libertés des personnes physiques concernées.

Dans tous les cas, l'AIPD est un outil qui permet de s'assurer que des mesures adéquates sont (ou seront) mises en place pour couvrir le niveau de risque associé au traitement présent (ou futur), et de justifier ces mesures en démontrant que l'analyse a été bien faite. L'AFMPS doit pouvoir démontrer cela au DPA (Autorité de protection des données) en gardant le rapport de l'AIPD à disposition.

Si l'existence de mesures adéquates ne sont pas démontrées par l'analyse AIPD correspondant au traitement, le traitement futur ne peut pas avoir lieu, et le traitement en cours doit être arrêté.

3. Définitions et abréviations

AIPD: Analyse d'Impact relative à la Protection des Données

CNIL: Commission Nationale de l'Informatique et des Libertés

CSI: *Conseiller en sécurité de l'information*

DPA: *Data Protection Authority*, l'Autorité de protection des données

DPIA: *Data Protection Impact Assessment*, Analyse d'impact relative à la protection des données

Voir AIPD

DPO: *Data Protection Officer*, Délégué à la Protection des Données (DPD)

DS: *Data Subject*, personne concernée

EBIOS: Expression des Besoins et Identification des Objectifs de Sécurité

Nom d'une méthode française de gestion des risques.

GDPR: *General Data Protection Regulation*, Règlement Général sur la Protection des Données (RGPD) Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Personne concernée: La personne dont on traite les données à caractère personnel

PIA: *Privacy Impact Assessment*, évaluation des facteurs relatifs à la vie privée

Considéré ici comme synonyme à DPIA.

PID: *Project Initiation Documentation*, Document de lancement du projet

Un document qui décrit la direction et le périmètre d'un projet, considéré comme le « contrat » entre le Chef de Projet et son client.

RGPD: Règlement Général sur la Protection des Données

Voir GDPR

RIT: Responsable **Interne** du Traitement

Collaborateur de l'AFMPS responsable d'un traitement structurel ou régulier de données à caractère personnel. C'est la personne qui participe activement à l'analyse AIPD et qui en est responsable à l'intérieur de l'agence, pour le compte du **Responsable du Traitement** (= AFMPS). C'est la personne mentionnée comme **Process Owner** dans le registre RGPD.

ROI: *Return On Investment*, Retour d'investissement

SOP: *Standard Operating Procedure*, procédure de travail standard

SQERT: *Scope Quality Effort Risks Time*, Périmètre Qualité Effort Risques Temps

Rapport mensuel de projet par un Chef de Projet

TBC: *To Be Confirmed*, à confirmer

4. Généralités

Le **Règlement Général sur la Protection des Données** (RGPD) nous oblige à évaluer tous nos traitements de données à caractère personnel, tant ceux sujets à un traitement automatisé qu'à un traitement manuel, et d'exécuter une **analyse d'impact relative à la protection des données** (AIPD) complète pour tous les traitements qui ont été identifiés avec un risque élevé (voir champ **DPIA Required?** dans le registre GDPR de l'AFMPS).

La procédure qui suit explique comment procéder, pas à pas, en 4 étapes. Elle est dérivée de la méthodologie du CNIL (Commission Nationale de l'Informatique et des Libertés), elle-même basée sur la méthode française EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), avec quelques adaptations ou conventions spécifiques au contexte de travail de l'AFMPS (intervenants de l'agence, outils de travail standards) expliquées dans cette procédure.

Cette méthodologie est largement supportée et **facilitée** par l'outil software « **PIA** » du CNIL. L'installation de cet outil PIA peut être demandé auprès du Service Desk ICT.

L'outil PIA fournit des explications courtes sur les réponses attendues, ainsi qu'une **base de connaissances** contextuelle avec des explications plus détaillées. On s'aidera également de l' « exemple de PIA » (à la page « Accueil »).

Par convention, nous indiquons par [+] dans cette procédure quelques conventions particulières ou astuces qui ne sont pas imposées par l'outil.

[+] Pour des raisons pratiques, lorsque l'outil PIA parle du « Responsable du Traitement », on se référera en fait au « **Responsable Interne du Traitement** (RIT) » :

- Le « **Responsable du Traitement** » (terminologie RGPD) est l'AFMPS, représenté par son Administrateur Général, responsable vis-à-vis de l'extérieur.
- Le « **Responsable Interne du Traitement** » (terminologie non RGPD) est une personne plus spécifique intérieure à l'agence qui, pour des raisons pratiques (la connaissance plus approfondie du traitement qu'il supervise), participe très activement à l'analyse AIPD, et est responsable vis-à-vis de l'Administrateur Général.

5. Procédure

5.1. Déclenchement: dépistage de base (Basic Screening)

Pour tous les traitements de données à caractère personnel qui se font de façon régulière et/ou structurée (par ex. application informatique, mailing lists, Service Desk, traitement de formulaires « papier » de notifications, etc.), le Responsable Interne du Traitement est responsable pour la documentation du traitement dans le **registre de traitements RGPD**, comme décrit dans DPO/001/SOP/F "Registre GDPR des traitements". Cette procédure contient aussi une étape de dépistage de base (**Basic Screening**) qui détermine si une analyse AIPD complète est nécessaire. Si c'est le cas, cela déclenche l'exécution de la présente procédure, qui tombe également sous la responsabilité du Responsable Interne du Traitement.

Cet exercice doit ensuite être **ré-exécuté tous les 2 ans**, ainsi qu'en cas de **changements importants** au traitement.

C'est donc au Responsable Interne du Traitement de prendre l'initiative pour commencer une nouvelle procédure AIPD (en particulier de **mise à jour bisannuelle**), en notifiant le DPO de son intention d'entamer cette procédure (par ex. en envoyant un email à DPO@fagg-afmps.be).

5.2. Préparation de l'exercice AIPD

5.2.0. Création ou réexécution d'une analyse AIPD

Le Responsable Interne du Traitement (ou l'expert business ou le membre d'équipe projet à qui il délègue cette tâche), utilise l'**outil PIA** pour **créer** une nouvelle analyse AIPD, en suivant les conventions suivantes pour le remplissage des propriétés de l'AIPD [+]:

- Intitulé du PIA = valeur du champ "**Process**" dans le registre RGPD
- Saisie = le nom du Responsable Interne du Traitement, et éventuellement le nom de l'auteur principal, par ex. un Business Analyst ou un expert business
- Evaluation = les noms des personnes participant à l'évaluation de l'AIPD
- Validation = le nom de l'Administrateur Général

Si par contre il s'agit d'une **réexécution** d'une analyse AIPD: l'outil PIA permet d'importer l'analyse précédente et de le dupliquer pour éviter de devoir tout créer à partir de zéro. Les valeurs énumérées ci-dessus peuvent ensuite être mises à jour dans l'écran d'accueil de l'outil PIA.

L'outil fournit des explications sur les informations demandées, ainsi qu'un exemple de PIA (à la page « Accueil »), et une base de connaissances.

Les informations demandées sont couvertes en 3 sections, parcourues plus en détail dans les paragraphes suivants:

- Contexte
- Principes Fondamentaux
- Risques

5.2.1. Section "Contexte"

Le contexte comprend 2 parties avec les questions suivantes:

- Partie 1 - Vue d'ensemble
    - Quel est le traitement qui fait l'objet de l'étude ?
    - Quelles sont les responsabilités liées au traitement ?
    - Quels sont les référentiels applicables ?
- Partie 2 - Données, processus et supports
    - Quelles sont les données traitées ?
    - Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?
    - Quels sont les supports des données ?

La majorité de l'information demandée devrait pouvoir être recopiée du registre RGPD.

A la fin de chaque partie, on peut indiquer que le contenu est prêt pour être évalué en cliquant sur le bouton "Demander l'évaluation".

5.2.1.1. [+] Partie 1 - Quel est le traitement qui fait l'objet de l'étude ?

- Bien identifier le traitement qui fait l'objet de l'analyse en répétant sans déformer l'information reprise dans le **registre de traitement RGPD** :
    - nom officiel = champ **Process** du registre RGPD
    - finalités du traitement = **Process Goals** et/ou **Processing Purposes**
- Fournir un bref aperçu du traitement (informatique ou manuel) analysé, en précisant la **nature** du produit / système faisant ce traitement, son **périmètre** d'application, son **contexte d'utilisation**, les **enjeux**. Pour expliquer les **enjeux**, répondre à la question « quels sont les bénéfices du traitement pour l'AFMPS ou pour les personnes concernées par le traitement comme les professionnels de la santé, les patients ou la société en général ? » :
    - A cette fin, les sources additionnelles suivantes peuvent être utiles :
        - Project Idea (spreadsheet)
        - Project Flyer (Word)
        - Outline Business Case d'un Project Brief
        - Project Information Documentation (PID)
        - Rapport SQERT
- Fournir en pièce jointe (optionnellement) :
    - un diagramme de vue d'ensemble ou **Overview Diagram** (de l'application informatique ou du traitement manuel) décrivant le **contexte d'utilisation**, exposant les **flots de données** et les entités (personnel et/ou systèmes) qui manipulent ces données.
    - une illustration « grand public » du système faisant l'objet de l'analyse AIPD, sous forme de graphique, de copie d'écran principal, de photographie, etc.

5.2.1.2. [+] Partie 1 - Quelles sont les responsabilités liées au traitement ?

- **Data Controller** - Responsable du traitement
    - C'est l'AFMPS, (on ne va pas analyser un traitement dont on n'est pas responsable).
    - [+] Préciser en plus une personne en particulier: le **Responsable Interne du Traitement (RIT)**, indiqué aussi dans le registre RGPD sous le champ **Process Owner**.
- **Data Processor(s)** – Les sous-traitants
    - Ce sont les sous-traitants de l'AFMPS, typiquement: Smals, Cegeka, etc.
    - De façon générale, identifier qui fournit les services suivants :
        - hébergement de site web
        - Service Desk
        - calculs spéciaux (par ex. encryption par eHealth)

5.2.1.3. [+] Partie 1 - Quels sont les référentiels applicables ?

- Identifier les **textes de loi** qui justifient le traitement par l'AFMPS: champ **Legal Context** du registre RGPD
- Identifier les **certifications** pertinentes en protection de données évoquées par les sous-traitants.
    - A cette fin, les sources suivantes peuvent être utiles:
        - Offre technique du sous-traitant
    - Illustrations:
        - Le fournisseur XYZ est en cours de certification ISO 27001 « Information Security Management System »
        - Le fournisseur ABC a déjà obtenu les certifications ISO 27001, 27002 et ISAE 3000
- Fournir ces textes en pièce jointe.

5.2.1.4. [+] Partie 2 - Quelles sont les données traitées ?

Voir champs **Persons Data Categories**, **Persons Data Details**, **Incidence of Personal Data** et **Data Retention Period** dans le registre RGPD.

Utiliser la check-list suivante pour vérifier que les informations sont bien suffisamment complètes:

- Données fournies par les **différents types d'utilisateur** (collaborateur AFMPS, professionnel de la santé, patient, volontaire sain, etc. avec attention particulière si des enfants sont potentiellement concernés)
    - Données
    - Destinataires
    - Durée de conservation
- Données fournies par des **applications ou bases de données tierces** (par ex. Source Authentiques, Personal Health Viewer, réseaux sociaux, etc.)
    - Données
    - Destinataires
    - Durée de conservation
- Données fournies pas des **sondes** (par ex. température)
    - Données
    - Destinataires
    - Durée de conservation
- Données calculées (par ex. **statistiques**)
    - Données
    - Destinataires
    - Durée de conservation

- Données déduites (information sensible, comme information relative à la **santé**, **vie sexuelle**, etc.)
    - Données
    - Destinataires
    - Durée de conservation

5.2.1.5. [+] Partie 2 - Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

Voir champ **Process Activities** dans le registre RGPD.

Il faut identifier chaque étape du traitement, en utilisant comme fil conducteur une progression naturelle (par ex. création d'un compte, collecte des données, envoi vers des systèmes extérieurs, création de statistiques). Eventuellement, identifier ces traitements par type d'utilisateur.

Les sources additionnelles suivantes peuvent aussi être utiles :

- Le diagramme de vue d'ensemble (**Overview Diagram, Fiche de processus**) peut servir de fil conducteur pour illustrer le flot depuis la création des données (par ex. création d'une compte utilisateur) jusqu'à la destruction, en passant par les traitements intermédiaires, comme l'utilisation à des fins de **statistiques** dans un Data Warehouse.
- Les Use Cases ou scénarios d'utilisation dans les documents de collecte des besoins (**Requirements**) produits par un Business Analyst dans le cadre d'un projet informatique.

5.2.1.6. [+] Partie 2 - Quels sont les supports des données ?

Voir champ **Application(s)** du registre RGPD.

Pour vérifier que les informations sont suffisamment complètes, on peut parcourir le fil conducteur du chapitre précédent et identifier le support des données correspondant pour chaque étape du traitement.

Pour un système complexe, la check-list suivante peut aider à identifier chaque support de données:

- Ressources informatiques
    - composants **hardware** (ou médias de données électroniques)
        - par ex. ordinateurs fixes ou mobiles, serveurs
    - composants **software**
        - par ex. navigateur web, application mobile
    - canaux de **communication**
        - par ex. Bluetooth, Wi-Fi, Internet
- Autres ressources
    - **personnel**
        - par ex. utilisateurs principaux, utilisateur administratifs, personnel d'entreprises de service
    - **installations**
        - par ex. domicile, bureaux d'une compagnie, locaux occupés par le personnel
    - **documents papier**
    - **canaux de transmission de papier**

Dans le diagramme de vue d'ensemble :

- les ressources informatiques doivent apparaître (obligatoire)
- le personnel devrait apparaître (désirable)

5.2.2. Section "Principes fondamentaux"

5.2.2.0. Introduction

Cette section a pour but de vérifier et démontrer la **conformité** du traitement avec les **exigences légales** (donc non négociables) de protection de la vie privée.

C'est le 1er pilier de la conformité RGPD:

Les principes fondamentaux comprennent 2 parties expliquées ci-après.

La majorité de l'information demandée devrait pouvoir être recopiée du registre RGPD.

A la fin de chaque partie, on peut indiquer que le contenu est prêt pour être évalué en cliquant sur le bouton "Demander l'évaluation".

5.2.2.1. Partie 1 - Proportionnalité et nécessité du traitement

- Les finalités du traitement sont-elles déterminées, explicites et légitimes ?
    - Voir champs **Process Goals** et **Processing Purposes** du registre RGPD.
    - [+] Distinguer les finalités primaires, secondaires (par ex. statistiques) et tertiaires (par ex. amélioration du service, partage)
- Quel(s) est(sont) les fondement(s) qui rend(ent) votre traitement licite ?
    - Voir champ **Lawfulness** du registre RGPD.
- Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?
    - Voir champs **Persons Data Details** et **Persons Data Categories** du registre RGPD.
- Les données sont-elles exactes et tenues à jour ?
    - Expliquer comment.
- Quelle est la durée de conservation des données ?
    - Voir champ **Lawfulness** du registre RGPD. En effet, la durée de conservation pourrait déjà être indiquée dans un texte de loi.
    - Voir champ **Data Retention Period**.
    - Quelle est la motivation pour cette durée ?
    - [+] Voir aussi : « Destruction des données » dans le cycle de vie identifiée dans la « Section 'Contexte' ».

5.2.2.2. Partie 2 - Mesures protectrices des droits

- Comment les personnes concernées sont-elles informées à propos du traitement ?
    - Voir champ **Right to be Informed** du registre RGPD
- Si applicable, comment le consentement des personnes concernées est-il obtenu ?
    - Voir champ **Lawfulness** du registre RGPD qui pourrait indiquer qu'on obtient le consentement.
- Comment les personnes concernées peuvent-elles exercer leurs droit d'accès et droit à la portabilité ?
    - Voir champs **Right of Access** et **Right to Data Portability** du registre RGPD
- Comment les personnes concernées peuvent-elles exercer leur droit de rectification et droit à l'effacement (droit à l'oubli) ?
    - Voir champs **Right to Rectification** et **Right to Erasure** du registre RGPD
- Comment les personnes concernées peuvent-elles exercer leur droit de limitation et droit d'opposition ?
    - Voir champs **Right to Non-automated Decisions** et **Right to Object** du registre RGPD
- Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?
    - Voir champs **Data Processors** et **Contract with Data Processors** dans le registre RGPD.
    - Eventuellement charger les contrats comme annexe à l'AIPD dans l'outil PIA.
- En cas de transfert de données en dehors de l'Union européenne, les données sont-elles protégées de manière équivalente ?
    - Le DPO peut donner conseil sur ce qui doit être vérifié à ce sujet dans ce cas.

5.2.3. Section "Risques"

5.2.3.0. Introduction

Cette étape est une analyse de risques permettant de s'assurer que le **risque résiduel** après application des mesures (existantes ou prévues) de protection est **acceptable**. C'est le 2e pilier de la conformité RGPD:

Pour une familiarisation rapide avec l'évaluation des risques, voir Annexe 1.

5.2.3.1. Partie 1 – Mesures existantes ou prévues

L'outil PIA prévoit une première partie à remplir: "Mesures existantes ou prévues".

- Cette partie sert à énumérer toutes les mesures qui sont prévues ou appliquées pour répondre au risques analysés dans les autres parties.
- On peut utiliser le catalogue de la base de connaissance de l'outil **PIA** pour identifier les mesures existantes ou prévues:
    - Chiffrement (Encryption)
    - Anonymisation (Anonymization)
    - Cloisonnement (Data partitioning)
    - Contrôle des accès logiques (Logical access control)
    - Journalisation (Traceability / Logging)
    - Sécurisation des documents papier (Paper document security)
    - Minimisation des données
    - etc.
- Il existe aussi la possibilité de créer de nouvelles mesures qui n'avaient pas été prévues dans le catalogue de la base de connaissance de l'outil PIA.
- Dans tous les cas, quelques mots d'**explication ou justification** doivent être fournis pour appuyer la déclaration.

5.2.3.2. Parties 2, 3 et 4 – Analyse de 3 risques standards (A, M, D)

L'outil **PIA** propose 3 **événements craints** standards, qui correspondent aux 3 prochaines parties à remplir:

- (A) Accès illégitime à des données
- (M) Modifications non désirées de données
- (D) Disparition de données

Pour chacun de ces 3 risques, l'outil **PIA** pose les questions suivantes, qui permettent de révéler toutes les composantes du risque:

- Quelles **sources** de risques pourraient-elles en être à l'origine ?
    - [+] Voir check-list de [RD01]
      "Privacy Impact Assessment (PIA) – Application to IoT Devices"
- Quelles sont les principales **menaces** qui pourraient permettre la réalisation du risque ? (= **événements craints**)
- Quels pourraient être les principaux **impacts** sur les personnes concernées si le risque se produisait ?
- Quelles sont les **mesures**, parmi celles identifiées, qui contribuent à traiter le risque ?

Chaque réponse fournie doit être expliquée en commentaire.

L'outil **PIA** caractérise le niveau de risque (risk level) par 2 paramètres classiques: (1) la **gravité** (severity) et (2) la **vraisemblance** du risque (likelihood) :

- Comment estimez-vous la **gravité** du risque, notamment en fonction des impacts potentiels et des mesures prévues ?
- Comment estimez-vous la **vraisemblance** du risque, notamment au regard des menaces, des sources de risques et des mesures prévues?

Pour ces 2 paramètres, des échelles sont proposées par l'outil PIA, avec 4 valeurs + (Non définie). Une explication décrivant chaque valeur est disponible dans la base de connaissances.

Pour chaque partie qui est finalisé, on peut indiquer cela en cliquant sur le bouton "Demander l'évaluation".

5.2.3.3. Partie 5 - Vue d'ensemble des risques

La partie "Vue d'ensemble des risques" permet de visualiser tous les impacts potentiels, toutes les menaces, les sources et les mesures en relation avec les 3 événements craints, avec le score de gravité et de vraisemblance.

5.3. Evaluation des 3 sections

5.3.1. Constitution et organisation du comité d'évaluation

Le Responsable Interne du Traitement désigne les membres de l'équipe qui vont participer à l'évaluation de l'AIPD. Cette équipe est constitué d'experts divers: voir section 1.2 « Responsabilités ».

Le Responsable Interne du Traitement organise ensuite une ou plusieurs réunions pour faire l'évaluation.

5.3.2. Vérification du registre de traitement RGPD

Lors de l'évaluation de toutes les parties, un des aspects à vérifier est que le traitement est bien documenté dans le registre de traitement RGPD, et qu'il y a une parfaite correspondance entre les informations dans le registre et l'AIPD. En cas d'informations manquantes ou incorrectes, le responsable interne fait le nécessaire pour corriger la situation.

5.3.3. Evaluation de la section « Contexte »

La description du contexte doit être revue de façon à s'assurer que cette description soit bien compréhensible, complète et conforme à la réalité. Cette validation est d'autant plus importante que le contexte fournit les fondations aux étapes suivantes.

Le résultat de l'évaluation doit ensuite être enregistré dans l'outil PIA :

- Si évaluation = « A corriger »
    - On apporte une explication des changements à apporter, et puis la partie redevient éditable après « Valider l'évaluation ».
- Si évaluation = « Acceptable »
    - Il faut motiver ce résultat, puis « Valider l'évaluation ». Cette partie n'est plus éditable et est proposée à la validation finale : « Partie évaluée, en attente de la validation finale ».
- Il est cependant possible d'annuler une demande de validation et ainsi revenir en mode édition.

5.3.4. Evaluation de la section « Principes fondamentaux »

- Si ceci est une **mise à jour** d'une analyse précédente :
    - Parcourir le contenu précédent, l'évaluation précédente, ainsi que le plan d'actions concernant cette partie, et vérifier si ces points d'action ont bien été exécutés.
- Pour chaque mesure (= point de la Partie 1 ou 2) :
    - évaluer si la mesure est (1) « A corriger », (2) « Améliorable » ou (3) « Acceptable »
    - expliquer (1) ce qui manque pour pouvoir juger, (2) les mesures additionnelles nécessaires pour devenir acceptable (3) pourquoi les mesures apparaissent suffisantes.
- « Valider l'évaluation » avec des mesures qui ne sont pas encore acceptables permet de retourner en mode édition.

5.3.5. Evaluation de la section « Risques »

Pour chacun des 3 risques (A, M, D):

- Revoir les réponses aux questions et les valeurs de **gravité** et **vraisemblances** pour le risque, ainsi que les explications fournies en commentaire.
- Juger si les réponses et explications fournies sont de qualité suffisante, et choisir entre (1) « A corriger », (2) « Améliorable » ou (3) « Acceptable ».
    - Dans le cas (1), expliquer ce qui manque pour obtenir la qualité suffisante, en indiquant :
        - Commentaire d'évaluation
    - Dans le cas (2), expliquer les **mesures additionnelles** à prévoir pour contrer le risque, en indiquant :
        - **Plan d'action** / mesures correctives
        - Commentaire d'évaluation
        - Les nouvelles valeurs pour **gravité** et **vraisemblance** si le plan d'action est implémenté
    - Dans le cas (3), il suffit de fournir :
        - Commentaire d'évaluation
- Ensuite « Valider l'évaluation ».

5.4. Validation finale

5.4.0. Vue générale

- Objectif : Cette 4ème étape a pour objectif de fournir des résumés afin de communiquer les résultat de l'analyse AIPD, et de prendre une décision
- Auteurs :
    - Responsable Interne du Traitement (RIT)
    - DPO (avis)
    - un représentant des personnes concernée (avis)
- Outils : Cette étape est supportée par l'outil **PIA**
- Etapes:
    - Cartographie des risques
    - Plan d'action
    - Avis du DPO et des personnes concernées

5.4.1. Cartographie des risques (Communicate)

- L'outil **PIA** résume les 3 risques (A, M, D), avant et après des **mesures complémentaires** éventuelles, sous forme de grille gravité / vraisemblance.

5.4.2. Plan d'action (Plan & Implement)

- L'outil **PIA** fournit une vue synthétique de la validation et recommandations effectuée par le DPO pour chaque mesure, et en particulier les **mesures améliorables** des sections
    - principes fondamentaux
    - risques → mesures existantes ou prévues
    - risques → (A), (M), (D)
- Pour chaque mesure améliorable (= Plan), le responsable interne du traitement définit un responsable de mise en œuvre et une date-butoir (= Implement).

5.4.3. Avis du DPO et des personnes concernées

- Cette partie n'est accessible qu'une fois toutes les parties précédentes validées par le Responsable Interne du Traitement.
- Le **DPO** exprime son avis, non contraignant, quant à la conformité du traitement (qui pourrait ou, au contraire, ne devrait pas être mis en œuvre) ainsi que les raisons.
- Un **représentant** des personnes concernées fait de même. Si le responsable du traitement ne fait pas cette démarche (personne n'a été consulté) ou passe outre cet avis, il faut aussi l'indiquer et le justifier.

5.4.4. Validation formelle par le Responsable Interne du Traitement

5.4.4.1. Approche générale

- [Valider le PIA] pour atteindre cette étape.
- Le **Responsable Interne du Traitement (RIT)** relit l'analyse APID et décide de l'acceptabilité ou non des mesures existantes ou prévues, des risques résiduels et des mesures complémentaires (plan d'action), en tenant compte aussi des avis.
- Ensuite trois possibilités :
    - [Refuser la validation]
    - [Valider et signer le DPIA]
    - [Validation simple]
- [+] Dans tous les cas, demander au DPO de mettre à jour le Registre RGPD avec la décision (voir champs **Last DPIA Date** et **Review Status**).

5.4.4.2. Cas [Refuser la validation]

- Le Responsable Interne du Traitement motive son refus.
- Ensuite deux possibilités (la première est le cas normal):
    - **Refuser le PIA** → retour à l'évaluation de chaque partie de l'AIPD
    - Abandonner le traitement → archivage de l'analyse (plus modifiable !)

5.4.4.3. Cas [Validation simple]

- Si le résultat du DPIA est positif, avec un risque résiduel négligeable, sans avis négatif du DPO ou du représentant des personnes concernées, le Responsable Interne du Traitement peut simplement clôturer le DPIA.
- Cela signifie que le traitement peut effectivement avoir lieu.
- Le RIT fait un export de l'analyse, et fournit le fichier PIA au DPO pour contrôle de versions.

5.4.4.4. Cas [Faire signer le PIA par le responsable]

- Si par contre il y a un avis négatif du DPO ou du représentant des personnes concernées, ou si le risque résiduel n'est pas négligeable et que le DPO indique qu'il faudrait demander l'avis de l'Autorité de protection des données, le rapport doit être validé par l'Administrateur Général de l'AFMPS, qui décidera ensuite de soumettre ou non le rapport DPIA pour approbation à l'Autorité de protection des données.

- Il faut donc d'abord imprimer le rapport, et le soumettre pour signature à l'Administrateur Général, ensemble avec l'avis du DPO et du représentant des personnes concernées, et demandant aussi l'accord pour soumettre le rapport DPIA à l'Autorité de protection des données.
- Scanner le rapport signé et « Ajouter le rapport PIA signé » (sélectionner le fichier scanné) en fichier joint dans l'outil PIA.
- Exporter l'analyse et fournir le fichier ainsi que le scan du rapport signé au DPO pour contrôle des versions.
- Le DPO documente aussi la décision de l'Administrateur Général dans son registre des incidents.

5.4.5. Soumission du DPIA à l'Autorité de protection des données

Si les risques résiduels sont trop élevés, ou si il y a un avis négatif du DPO ou du représentant des personnes concernées, le rapport DPIA (signé par l'Administrateur Général) est censé être soumis à l'Autorité de protection des données. Si effectivement l'Administrateur Général a donné son accord pour cela, le DPO se charge de cette soumission.

Le DPO documente ensuite l'avis reçu dans son registre des incidents, et communique cet avis à toutes les personnes concernées. Le Responsable Interne du Traitement fait ensuite le nécessaire pour suivre ou implémenter les recommandations de l'Autorité de protection des données.

6. Références et documents connexes

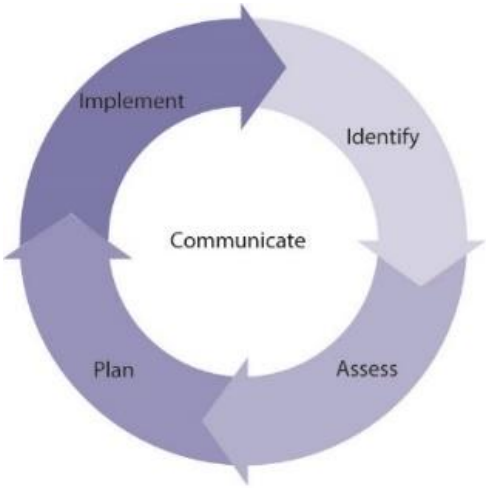
- DPO/001/SOP/F: Registre GDPR des activités de traitement
- FAMHP/078/SOP/F : Procédure de maîtrise des risques liés à l'objectif de processus
- [RGPD] https://www.cnil.fr/reglement-europeen-protection-donnees ou https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR
- [RD01] Privacy Impact Assessment (PIA) – Application to IoT Devices https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-en.pdf

7. Historique

Analyse d'impact relative à la protection des données (AIPD)		
Rédigé par: Bernard Fontaine (FR)	Traduit par: Elke Dinneweth	
Numéro de procédure	Date d'application	Raison des modifications
DPO/002/SOP/F (1)	Voir "Application Date" dans DMS Quality	Première édition

Annexe 1 – Evaluation de risques

Toute évaluation de risques comporte typiquement les étapes suivantes :



- **Identify** (Identifier):
  - Une bonne formulation du **risque résiduel** peut se faire à l'aide de la phrase-canevas suivante:

à cause de	<**source** avec la **motivation** sur un **support** de données>
il y a une	menace
que	<**événement craint** sur les données personnelles>
ce qui résulterait en	<**impact**>
malgré	<les **mesures** envisagées>

Par exemple :

à cause de	un employé malveillant animé d'un désir de vengeance ayant la possibilité d'accéder au disque
il y a une	menace
que	les données soient détruites
ce qui résulterait en	une détérioration de la qualité du service (interruption avec perte de temps pour restaurer les données)
malgré	l'existence de backups

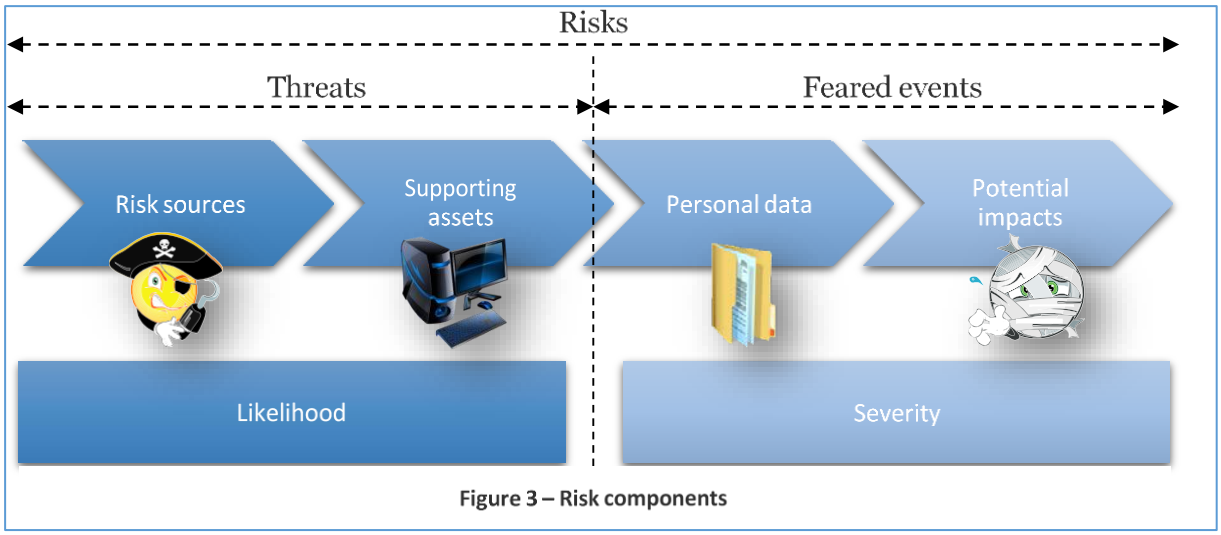


Figure 3 – Risk components

Source: [RD01]

Assess (Evaluer): Il faut estimer le niveau de risque, ce qui peut se faire de plusieurs façons. Une façon classique est d'utiliser 2 paramètres:

(1) l'**impact** (severity)

(2) la **probabilité** du risque (likelihood)

On détermine généralement un score pour chacun de ces paramètres sur base d'une échelle prédéterminée.

- **Plan:** Planifier des mesures pour contrer ces risques.
- **Implement:** Implémenter les mesures planifiées.
- **Communicate:** Faire connaître les résultats de chaque étape.