**Informations de l’AIPD**

Nom de l’AIPD

**XXXXXX**

Nom de l'auteur

XXXXXXX

Nom de l'évaluateur

XXXXXXXXX

Nom du validateur

XXXXXXXXXX

Date de création

JJ/MM/AAAA

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Modifié par** | **Brève Description du changement** |
| 1 | JJ/MM/AAAA | XXXXX | Livraison de l’AIPD |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Sommaire

[Sommaire 1](#_Toc2081735275)

[Glossaire 2](#_Toc28092762)

[Validation de l’AIPD 3](#_Toc589679091)

[I. Contexte 4](#_Toc316857573)

[1. Vue d'ensemble 5](#_Toc1716437681)

[2. Données, processus et supports 6](#_Toc610960024)

[II. Principes fondamentaux 8](#_Toc34040700)

[1. Proportionnalité et nécessité 9](#_Toc1139545505)

[2. Mesures protectrices des droits 13](#_Toc560555058)

[III. Risques 20](#_Toc2020500279)

[1. Mesures existantes ou prévues 21](#_Toc1474926497)

[2. Accès illégitime à des données 28](#_Toc1088338226)

[3. Modification non désirée de données 30](#_Toc683610823)

[4. Disparition de données 32](#_Toc1149647115)

[IV. Plan d'action 34](#_Toc604992039)

[V. Annexes 35](#_Toc1515826849)

# Glossaire

# Validation de l’AIPD

Etapes de de validation de l’AIPD :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Avis du RSSI : |  |  | | |
| Avis du DPD : |  |  | | |
| Avis des personnes concernées : |  | L’avis des personnes concernées a été demandé | | |
|  | L’avis des personnes concernées n’a pas été demandé | | |
| Responsable de la validation de l’AIPD ([Préciser]) : | Après lecture intégrale de l’AIPD concernant le traitement des données liées à l’activité de : XXXXXX | | | |
|  | Je confirme que la description du contexte de mon traitement est conforme à la réalité\* | | |
|  | Je confirme avoir pris connaissance des risques existants en fonction des mesures actuellement mises en œuvre ou prévues. \* | | |
|  | Je valide les mesures correctives indiquées\* | | |
|  | Je m’engage à mettre en œuvre dans les plus brefs délais les mesures correctives indiquées. \* | | |
| **Refuser la validation** | | **Validation** | **Signature du responsable** |
|  | |  |  |

\*tous les champs doivent être cochés.

# Contexte

## Vue d'ensemble

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | **Réponse** | **Evaluation** | **Commentaire d’évaluation** | **Plan d’action** |
| Quel est le traitement qui fait l’objet de l’étude ? | Nom / Description du traitement |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Nom de l’application |  |
| Finalités du traitement |  |
| Enjeux du traitement |  |
| Contexte d’utilisation |  |
| Quelles sont les responsabilités liées au traitement ? | Responsable de traitement |  |
| Sous-traitant |  |
| Co-responsables |  |
| Quels sont les référentiels applicables ? | Textes applicables au traitement  (Textes législatifs et réglementaires, …) |  |
| Modalité de prise en compte |  |
| Quelle est la fiche de registre associée ? | |  |

## Données, processus et supports

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | | **Réponse** | **Evaluation** | **Commentaire d’évaluation** | **Plan d’action** |
| Quelles sont les données traitées ? | Données collectées et traitées | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Acceptable** | |  | **Améliorable** | |  |  |
| Collecte de données sensibles | |  |
| Destinataires | |  |
| Personnes pouvant y accéder | |  |
| Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?  Par exemple à l'aide d'un schéma de flux de données et d'une description de chaque processus mis en œuvre  Les éléments fonctionnels à définir sont notamment :  - le stockage  - les différentes étapes de traitement  - le processus d'archivage. | Autorisation d’utilisation / de collecte | Description détaillée |  |
| Support des données |
| Collecte / Enregistrement | Description détaillée |
| Support des données |
| Transfert des données | Description détaillée |
| Support des données |
| Consultation des données | Description détaillée |
| Support des données |
| Extraction des données | Description détaillée |
| Support des données |
|  | Autres |  |  |  |  |

# Principes fondamentaux

## Proportionnalité et nécessité

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **Réponse** | **Evaluation** | **Commentaire d’évaluation** | **Plan d’action** |
| Les finalités du traitement sont-elles déterminées, explicites et légitimes ? | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Quel(s) est(sont) le(s) fondement(s) qui rend(ent) votre traitement licite ? | - le consentement au traitement de ses données est fourni  par la personne concernée pour une ou plusieurs finalités spécifiques |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| - le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci |  |
| - le traitement est nécessaire au respect d'une obligation légale, définie par le droit de l'Union ou le droit de l'Etat membre auquel le responsable de traitement est soumis |  |
| - le traitement est nécessaire à la sauvegarde des intérêts vitaux  de la personne concernée ou d'une autre personne physique. |  |
| - le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement |  |
| - le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable de traitement ou par un tiers,  à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. |  |
| Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ? | Détail des données traitées |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Catégories  (sensibles / non sensibles) |
| Justification du besoin et de la pertinence des données |
| Mesures de minimisation |
| Les données sont-elles exactes et tenues à jour ? | Chiffrement des données |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Intégrité des données |  |
| Séparation des profils |  |
| Autres |  |
| Quelle est la durée de conservation des données ? | Types de données  (données courantes, archivées, fonctionnelles, logs techniques, papier, …) |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Durée de conservation |
| Justification de la durée de conservation |
| Un système de purge à l’issue de la durée de conservation existe-t-il ? | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Un système d’anonymisation à l’issue de la durée de conservation existe-t-il ? | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |

## Mesures protectrices des droits

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | **Réponse** | | | | **Evaluation** | **Commentaire d’évaluation** | **Plan d’action** |
| Comment les personnes concernées sont-elles informées à propos du traitement ? | Mesures pour le droit à l’information | |  | | | | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Présentation des conditions d’utilisation/ confidentialité | |  | | | |
| Possibilité d’accéder aux conditions d’utilisation/ confidentialité | |  | | | |
| Conditions lisibles et compréhensibles | |  | | | |
| Existence de clauses spécifiques au dispositif | |  | | | |
| Présentation détaillée des finalités des traitements de données (objectifs précis, croisements de données s’il y a lieu, etc.) | |  | | | |
| Présentation détaillée des données personnelles collectées | |  | | | |
| Présentation des éventuels destinataires | |  | | | |
| Présentation des droits de la personne concernée (retrait du consentement, suppression de données, etc.) | |  | | | |
| Information sur le mode de stockage sécurisé des données, notamment en cas d’externalisation | |  | | | |
| Modalités de contact de l'entreprise (identité et coordonnées) pour les questions de confidentialité | |  | | | |
| Le cas échéant, information de la personne concernée de tout changement concernant les données collectées, les finalités, les clauses de confidentialité | |  | | | |
| Si applicable, comment le consentement des personnes concernées est-il obtenu ? | Libre  Ni contraint ni influencé, sans conséquences négatives en cas de refus. | |  | | | | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Spécifique  Doit correspondre à un seul traitement, pour une finalité déterminée | |  | | | |
| Eclairé  Contient avant recueil du consentement :  . L’identité du responsable de traitement  . Les finalités poursuivies  . Les catégories de données collectées  . L’existence d’un droit de retrait du consentement  . Selon les cas, contient l’information que les données seront utilisées dans le cadre de décisions automatisées ou qu’elles feront l’objet d’un transfert vers un pays hors UE. | |  | | | |
| Univoque  Être donné par une déclaration ou tout autre acte positif clairs. | |  | | | |
| Conservation de la preuve du consentement | |  | | | |
| Comment les personnes concernées peuvent-elles exercer leurs droits : | Accès | |  | | | | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Portabilité | |  | | | |
| Rectification | |  | | | |
| Effacement | |  | | | |
| Limitation | |  | | | |
| Opposition | |  | | | |
| Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?  (Spécificités complémentaires :  - le périmètre de ses responsabilités est formalisé  - les contrats, codes de conduite et certifications fixent ses obligations) | Nom du sous-traitant | | Sous-traitant 1 : | Sous-traitant 2 : | Sous-traitant 3 : | Sous-traitant 4 : | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Finalité | |  |  |  |  |
| Périmètre | |  |  |  |  |
| Référence du contrat | |  |  |  |  |
| En cas de transfert de données en dehors de l’Union Européenne, les données sont-elles protégées de manière équivalente ? | | - Les pays hors UE où sont stockées ou traitées des données sont identifiés  Le lieu géographique de stockage des différentes données du traitement doit être connu par le responsable de traitement |  | | | | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| - Ces pays ont été reconnus comme adéquats ou bien disposent de clauses qui encadrent le transfert. |  | | | |

# Risques

## Mesures existantes ou prévues

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | **Réponse** | **Evaluation** | **Commentaire d’évaluation** | **Plan d’action** |
| Sécurisation de l’exploitation et sécurisation physique | - Les procédures d'exploitation, inventaire et mise à jour des logiciels et matériels, correction des vulnérabilités, duplication des données, limiter l'accès physique au matériel, etc. sont documentées | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| - Des mesures de contrôle des accès physiques aux locaux hébergeant le traitement ont été mises en place (zonage, accompagnement des visiteurs, port de badge, portes verrouillées, etc.) | |  |
| - Des moyens d’alerte en cas d’effraction ont été définis | |  |
| Sécurisation des matériels | Sécuriser les postes de travail | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Sécuriser l’informatique mobile | |  |
| Sécuriser les serveurs | |  |
| Sécurisation des canaux informatiques | Protéger le réseau informatique interne | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Archivage | Encadrer la maintenance et la destruction des données | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Archiver de manière sécurisée | |  |
| Sauvegarde des données | - Une politique de sauvegarde est formalisée, permettant d'assurer la disponibilité et/ou l’intégrité des données à caractère personnel. | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| - Une politique de continuité d'activité est formalisée. | |  |
| - La confidentialité des données est protégée :  . Régularité des sauvegardes  . Chiffrement du canal de transmission des données  . Test d'intégrité  etc. | |  |
| Chiffrement : Chiffrer, garantir l'intégrité | - Mise en place de chiffrement symétrique | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| - Mise en place de chiffrement asymétrique | |
| Contrôle des accès logiques | Gérer les habilitations | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Authentifier les utilisateurs | |  |
| Mots de passe | |  |
| Autres | |  |
| Protection des sites Web | Sécuriser les sites WEB *(WAF, …)* | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Anonymisation | Anonymiser | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Encadrer les développements informatiques | |  |
| Statistiques | |  |
| Gestion des tiers accédant aux données | Sécuriser les échanges avec d'autres organismes | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Minimisation des données | | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Lutte contre les logiciels malveillants | | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Protection contre les sources de risques non humains | - Existence de mesures pour éviter que des sources de risques, humaines ou non humaines portent atteinte aux données à caractère personnel  (produits dangereux, zones géographiques dangereuses, transfert des données en dehors de l'UE, etc.). | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| - Existence de mesures pour réduire ou éviter les risques liés à des sources non humaines (phénomènes climatiques, incendie, dégât des eaux, accidents internes ou externes, animaux, etc.) qui pourraient affecter la sécurité des données à caractère personnel (mesures de prévention, détection, protection, etc.). | |  |
| Maintenance | | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Journalisation et traçabilité | - Existence d'un dispositif de gestion des traces et des incidents | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| - Existence de mesures mises en place pour être capable de détecter les incidents concernant des données à caractère personnel de façon précoce et de disposer d’éléments exploitables pour les étudier ou pour fournir des preuves dans le cadre d’enquêtes | |  |
| Cloisonnement des données (par rapport au reste du système d’information) | | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Sécurisation des documents papier | | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
| Organisation (Gouvernance) | | Gérer la politique de protection de la vie privée, Gestion des règles |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |
|  | | Gestion des risques |  |  |  |  |
|  | | Gestion des projets |  |  |  |  |
|  | | Gestion des incidents et des violations de données |  |  |  |  |
|  | | Relations avec les tiers |  |  |  |  |
|  | | Gestion des personnels |  |  |  |  |
|  | | Supervision |  |  |  |  |
| Audits | | |  | |  |  | | --- | --- | |  | **A corriger** | |  | **Améliorable** | |  | **Acceptable** | |  |  |

## Accès illégitime à des données

Quels pourraient être les principaux **impacts sur les personnes concernées** si le risque se produisait ?

|  |  |
| --- | --- |
| CORPOREL |  |
| MATERIEL |  |
| MORAL |  |

Quelles sont les principales **menaces** qui pourraient permettre la réalisation du risque ?

|  |  |
| --- | --- |
| MATERIELS |  |
| LOGICIELS |  |
| CANAUX INFORMATIQUES |  |
| AUTRES |  |

|  |  |
| --- | --- |
| Quelles **sources** de risques pourraient-elles en être à l'origine ?   * XXXXXXXXX * XXXXXXXXX | Quelles sont les **mesures**, parmi celles identifiées, qui contribuent à traiter le risque ?   * XXXXXX * XXXXXX * XXXXXX |

Comment estimez-vous la **gravité du risque d’accès illégitime à des données**, notamment en fonction des impacts potentiels et des mesures prévues ? *(Cocher la case correspondante)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Négligeable** | **Limitée** | **Importante** | **Maximale** |  |
|  |  |  |  |
|  | | | |

Comment estimez-vous la **vraisemblance du risque d’accès illégitime à des données**, notamment au regard des menaces, des sources de risques et des mesures prévues ?

|  |  |  |  |
| --- | --- | --- | --- |
| **Négligeable** | **Limitée** | **Importante** | **Maximale** |
|  |  |  |  |
|  | | | |

## Modification non désirée de données

Quels pourraient être les principaux **impacts sur les personnes concernées** si le risque se produisait ?

|  |  |
| --- | --- |
| CORPOREL |  |
| MATERIEL |  |
| MORAL |  |

Quelles sont les principales **menaces** qui pourraient permettre la réalisation du risque ?

|  |  |
| --- | --- |
| LOGICIELS |  |
| CANAUX INFORMATIQUES |  |
| PERSONNES |  |
| DOCUMENTS PAPIER |  |

|  |  |
| --- | --- |
| Quelles **sources** de risques pourraient-elles en être à l'origine ?   * XXXXXXXX * XXXXXXXXX | Quelles sont les **mesures**, parmi celles identifiées, qui contribuent à traiter le risque ?   * XXXXXXXXXX * XXXXXXXXXX * XXXXXXXXX |

Comment estimez-vous la **gravité du risque de modification non désirée de données**, notamment en fonction des impacts potentiels et des mesures prévues ? *(Cocher la case correspondante)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Négligeable** | **Limitée** | **Importante** | **Maximale** |  |
|  |  |  |  |
|  | | | |

Comment estimez-vous la **vraisemblance du risque de modification non désirée de données**, notamment au regard des menaces, des sources de risques et des mesures prévues ?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Négligeable** | **Limitée** | **Importante** | **Maximale** |  |
|  |  |  |  |
|  | | | |

## Disparition de données

Quels pourraient être les principaux **impacts sur les personnes concernées** si le risque se produisait ?

|  |  |
| --- | --- |
| CORPOREL |  |
| MATERIEL |  |
| MORAL |  |

Quelles sont les principales **menaces** qui pourraient permettre la réalisation du risque ?

|  |  |
| --- | --- |
| MATERIELS |  |
| LOGICIELS |  |
| CANAUX INFORMATIQUES |  |
| PERSONNES |  |
| DOCUMENTS PAPIER |  |
| CANAUX PAPIER |  |

|  |  |
| --- | --- |
| Quelles **sources** de risques pourraient-elles en être à l'origine ?   * XXXXXXXXX * XXXXXXXXX | Quelles sont les **mesures**, parmi celles identifiées, qui contribuent à traiter le risque ?   * XXXXXXXXXX * XXXXXXXXX * XXXXXXXX |

Comment estimez-vous la **gravité du risque de disparition de données**, notamment en fonction des impacts potentiels et des mesures prévues ? *(Cocher la case correspondante)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Négligeable** | **Limitée** | **Importante** | **Maximale** |  |
|  |  |  |  |
|  | | | |

Comment estimez-vous la **vraisemblance du risque de disparition de données**, notamment au regard des menaces, des sources de risques et des mesures prévues ?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Négligeable** | **Limitée** | **Importante** | **Maximale** |  |
|  |  |  |  |
|  | | | |

# Plan d'action

|  |  |  |  |
| --- | --- | --- | --- |
| Partie | Mesure | Porteur | Echéance |
|  |  |  |  |
|  |  |  |  |

# Annexes