CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Privacy Impact Assessment (AIPD)

INSA-Lyon/Nantes – 15 février 2025

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

ANALYSE D'IMPACT SUR LA PROTECTION DES DONNÉES (AIPD)

Que dit le règlement général sur la protection des données ?
(et les *Guidelines* du G29)

L'AIPD
dans le RGPD

RGPD

Article 35 RGPD

•*Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est* ***susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques****, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.*

Un cadre européen

- **Belgique :**
- https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/analyse-d-impact-relative-a-la-protection-des-donnees

- **Espagne :** *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
- https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/evaluaciones-de-impacto

- **France** : *Étude d'impacts sur la vie privée (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd

- **Angleterre** : *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
  https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/accountability-and-governance/data-protection-impact-assessments/

- **Allemagne :** Standard Data Protection Model, V.1.0 – Trial version, 201631.
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf

Le cadre européen

Annexe 2 — Critères d'acceptabilité d'une AIPD

Les critères suivants proposés par le GT29 peuvent être utilisés par les responsables du traitement pour déterminer si une AIPD ou une méthodologie d'AIPD considérée est suffisamment complète aux fins du respect des exigences du RGPD:

- ☐ une description systématique du traitement est fournie [article 35, paragraphe 7, point a)]:
  - ☐ la nature, la portée, le contexte et les finalités du traitement sont pris en compte (considérant 90);
  - ☐ les données à caractère personnel concernées, les destinataires et la durée pendant laquelle les données à caractère personnel seront conservées sont précisés;
  - ☐ une description fonctionnelle de l'opération de traitement est fournie;
  - ☐ les actifs sur lesquels reposent les données à caractère personnel (matériels, logiciels, réseaux, personnes, documents papier ou canaux de transmission papier) sont identifiés;
  - ☐ le respect de codes de conduite approuvés est pris en compte (article 35, paragraphe 8);
- ☐ la nécessité et la proportionnalité sont évaluées [article 35, paragraphe 7, point b)]:
  - ☐ les mesures envisagées pour assurer la conformité au règlement sont déterminées [article 35, paragraphe 7, point d), et considérant 90], avec prise en compte:
    - ☐ de mesures contribuant au respect des principes de proportionnalité et de nécessité du traitement, fondées sur les exigences suivantes:
      - ☐ finalités déterminées, explicites et légitimes (article 5, paragraphe 1, point b)];
      - ☐ licéité du traitement (article 6);
      - ☐ données adéquates, pertinentes et limitées à ce qui est nécessaire [article 5, paragraphe 1, point c)];
      - ☐ durée de conservation limitée [article 5, paragraphe 1, point e)];
    - ☐ de mesures contribuant aux droits des personnes concernées:
      - ☐ informations fournies à la personne concernée (articles 12, 13 et 14);
      - ☐ droit d'accès et droit à la portabilité des données (articles 15 et 20);
      - ☐ droit de rectification et droit à l'effacement (articles 16, 17 et 19);
      - ☐ droit d'opposition et droit à la limitation du traitement (articles 18, 19 et 21);
      - ☐ relations avec les sous-traitants (article 28);
      - ☐ garanties entourant le ou les transferts internationaux (chapitre V);
      - ☐ consultation préalable (article 36);
- ☐ les risques pour les droits et libertés des personnes concernées sont gérés [article 35, paragraphe 7, point c)]:
  - ☐ l'origine, la nature, la particularité et la gravité des risques sont évalués (considérant 84) ou, plus spécifiquement, pour chaque risque (accès illégitime aux données, modification non désirée des données, disparition des données) du point de vue des personnes concernées:
    - ☐ les sources de risques sont prises en compte (considérant 90);
    - ☐ les impacts potentiels sur les droits et libertés des personnes concernées sont identifiés en cas d'événements tels qu'un accès illégitime aux données, une modification non désirée de celles-ci ou leur disparition.
    - ☐ les menaces qui pourraient conduire à un accès illégitime aux données, à une modification non désirée de celles-ci ou à leur disparition sont identifiées;
    - ☐ la probabilité et la gravité sont évaluées (considérant 90);
  - ☐ les mesures envisagées pour faire face à ces risques sont déterminées [article 35, paragraphe 7, point d), et considérant 90];
- ☐ les parties intéressées sont impliquées:
  - ☐ l'avis du DPD est recueilli (article 35, paragraphe 2);

L'utilité de l'AIPD pour un RT

- Qu'est-ce qu'un DPIA ?
  - Un processus permettant de :
    - évaluer la nécessité et la proportionnalité
    - gérer les risques sur les droits et libertés
  - Un outil pour bâtir sa conformité et la démontrer
  - DPIA (RGPD) = PIA

L'objet de l'AIPD

❖ Sur quoi une AIPD porte-t-elle ?

- Un traitement
- Des traitements similaires
  - Traitements identiques mis en œuvre par plusieurs responsables de traitements (RT)
  - Traitements partagés par plusieurs RT
  - Traitements similaires en termes de finalités, fonctionnalités, risques, technologies, etc.
- Un produit (utilisé par plusieurs RT)

Les traitements concernés

❖ Quels traitements font l'objet d'une AIPD ?

- Créés avant mai 2018, en cas de modification substantielle
  - contexte
  - finalité, fonctionnalités, etc.
  - comportant des risques : données, supports des données, sources de risques, impacts potentiels, menaces

- Créés après mai 2018 et soumis à AIPD

Point commun = des risques élevés

Les critères du CEPD

Lignes directrices AIPD

https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

Obligatoire

•Risques élevés = 9 critères à considérer

- *Évaluation/scoring*
- *Décision automatique avec effet légal*
- *Surveillance systématique*
- *Données sensibles/hautement personnel*
- *Large échelle*
- *Croisement de données*
- *Personnes vulnérables*
- *Usage innovant*
- *Blocage d'un droit/contrat*

- Liste AIPD obligatoire

Pas obligatoire

- Pas susceptible d'engendrer des risques élevés
- DPIA existant sur traitement similaire
- Base légale UE/nationale + AIPD
- Liste de traitements dispensés
- Démonstration que les risques ne sont pas élevés

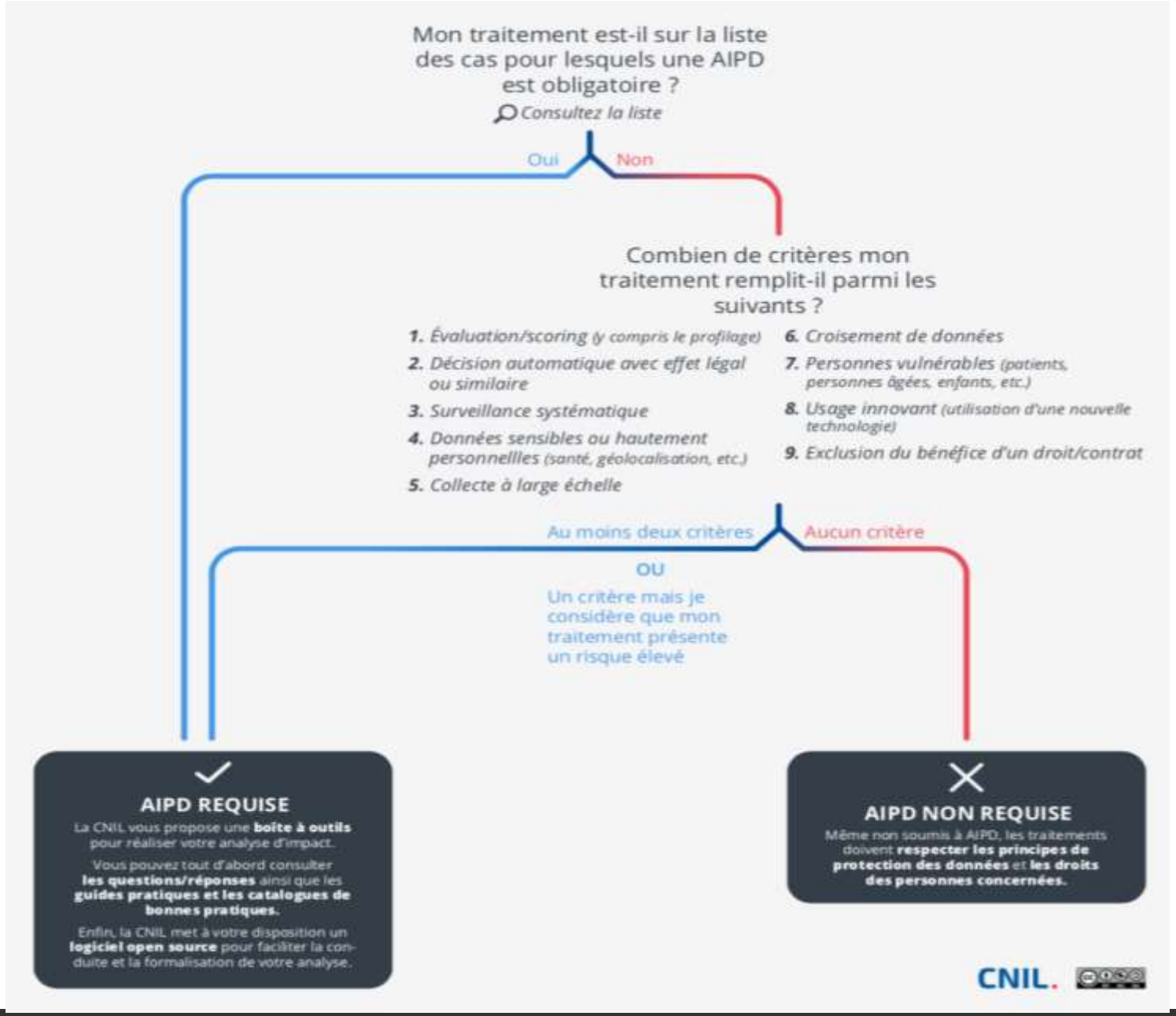
- Liste AIPD non obligatoires

Les listes publiées par les autorités

- Application du mécanisme de cohérence par le CEPD
  - 26 listes AIPD obligatoire publiées depuis octobre 2018
  - Un point commun = les 3 critères listés à l'article 35.3 RGPD

  https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en?f%5B0%5D=register_decisions_topic%3A138

- 3 listes AIPD non obligatoires
  - France/ République Tchèque/Lituanie


Mon traitement est-il sur la liste des cas pour lesquels une AIPD est obligatoire ?
Consultez la liste
Oui
Non
Combien de critères mon traitement remplit-il parmi les suivants ?
1. Évaluation/scoring (y compris le profilage)
2. Décision automatique avec effet légal ou similaire
3. Surveillance systématique
4. Données sensibles ou hautement personnellles (santé, géolocalisation, etc.)
5. Collecte à large échelle
6. Croisement de données
7. Personnes vulnérables (patients, personnes âgées, enfants, etc.)
8. Usage innovant (utilisation d'une nouvelle technologie)
9. Exclusion du bénéfice d'un droit/contrat
Au moins deux critères
OU
Un critère mais je considère que mon traitement présente un risque élevé
Aucun critère
AIPD REQUISE
La CNIL vous propose une boîte à outils pour réaliser votre analyse d'impact.
Vous pouvez tout d'abord consulter les questions/réponses ainsi que les guides pratiques et les catalogues de bonnes pratiques.
Enfin, la CNIL met à votre disposition un logiciel open source pour faciliter la conduite et la formalisation de votre analyse.
AIPD NON REQUISE
Même non soumis à AIPD, les traitements doivent respecter les principes de protection des données et les droits des personnes concernées.
CNIL.

Les parties prenantes de l'AIPD

- Le responsable de traitement
  - L'AIPD peut être menée par autrui, mais le RT est responsable
- Le DPO, s'il est désigné
  - Conseil et vérification d'exécution, évaluation des mesures et risques résiduels, développement de bases de connaissances personnalisées
- Les personnes concernées (ou leurs représentants), le cas échéant
  - Leur avis devrait être pris, si possible avant mise en œuvre, directement ou indirectement, et documenté
- Les sous-traitants, s'il y en a
  - Assistance et fourniture d'informations (règles à contractualiser)
- Le métier, si possible
  - Proposition de mener une AIPD, participation à sa rédaction
- Le responsable de la sécurité des systèmes d'information (chargé sécurité SI…)
  - Évaluation des mesures, proposition de mener une AIPD, assistance
- La direction informatique, si possible
  - Assistance

La consultation préalable de la CNIL

- La consultation est **obligatoire quand les risques résiduels demeurent élevés**

- *Article 36.1 RGPD : lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque* »

- **Consultation de la CNIL par le RT** via un téléservice dédié

Autres cas de communication de l'AIPD

❖ Une AIPD peut être communiquée

- À la CNIL
  - Communication potentiellement requise en cas de contrôle

- Aux personnes intéressées (public, partenaires, personnes concernées)
  - Publication ou communication conseillée afin d'apporter de la confiance
  - Tout ou partie de l'AIPD (on peut exclure des parties compromettantes : risques de sécurité, secrets industriels ou commerciaux, etc.)

Les sanctions

❖ Que risque-t-on ?

- «Interdiction du traitement, effacement des données, limitation (art.58 RGPD)
- « Amendes *administratives pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu* » [art. 83(4)(a)

❖ Dans quels cas ?

- Quand une AIPD n'a pas été menée alors qu'elle aurait dû l'être
- Quand la CNIL n'a pas été consultée alors qu'elle aurait dû l'être
- Quand une AIPD n'a pas été correctement menée et documentée

Panorama du DPIA

Objectif & enjeux

Évaluer la nécessité et la proportionnalité
Gérer les risques sur les droits et libertés

Sanction

10M€ ou 2% du chiffre d'affaires mondial

Processus

Description, analyse juridique, technique, évaluation des risques, mesures correctrices

DPIA

Communication

Consultation de la CNIL
Communiquer à autrui (vecteur de confiance)

Acteurs

RT, DPO, sous-traitants, métier, RSSI/DSI, personnes concernées

Temporalité

Avant la mise en œuvre du traitement

Traitement

Sauf exception, traitements impliquant des risques élevés ➡ 9 critères

METHODOLOGIE

Une AIPD repose sur deux piliers

Que signifie être conforme au Règlement ?

- Les principes et droits fondamentaux (finalité, information…), « non négociables », fixés par la loi, devant être respectés et ne pouvant faire l'objet d'aucune modulation

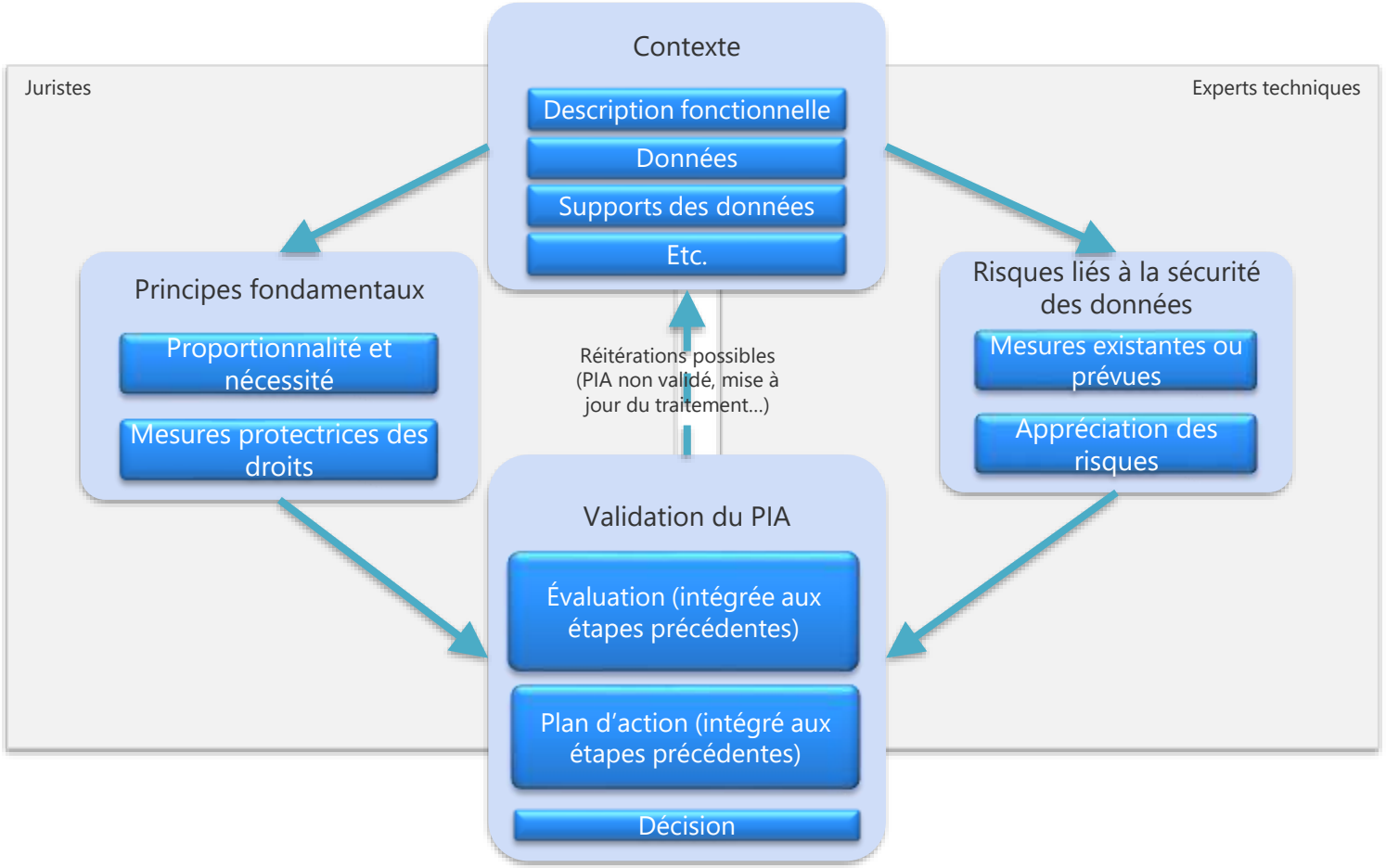
- La gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données

- Le *Privacy Impact Assessment* (PIA) est un moyen de se mettre en conformité et de le démontrer (notion d'accountability)

15/01/2019

Quelle méthodologie ?

Adaptation des guides AIPD



Le contexte

De quoi parle-t-on ? (étape 1)

- Le traitement de données à caractère personnel
  - Quelle est sa finalité ?
  - Quels sont ses apports ? (pour l'organisme, pour les personnes concernées, pour la société…)

- Le plus important : comprendre le cycle de vie des données
  - Quelles sont les données ?
  - Qui sont les destinataires ?
  - Qui peut y accéder ?
  - Quelle est leur durée de conservation ?
  - Sur quoi reposent-elles ?
  - Quelles sont les étapes du traitement ?

Les principes fondamentaux

(étape 2)

❖ Les mesures garantissant la proportionnalité et la nécessité du traitement

- Finalité(s) (déterminée, explicite et légitime – interdiction du détournement de finalité) [art. 5.1 (b)]
- Fondement/licéité du traitement [art. 6]
- Données adéquates, pertinentes, non excessives (minimisation), exactes et tenues à jour [art. 5 (c)]
- Durée de conservation limitée [art. 5 (e)]

Les principes fondamentaux

(étape 2)

❖ Les mesures protectrices des droits des personnes

- Information des personnes (traitement loyal et transparent) [art. 12, art. 13, art. 14]
- Droit d'accès et droit à la portabilité
- Droits de rectification, d'effacement, d'opposition et de limitation du traitement
- Sous-traitance [art. 28]
- Transferts [art. 44 et suivants]

Les mesures de sécurité
initialement prévues
(étape 3)

- Mesures sur les données du traitement
  - Chiffrer
  - Anonymiser
  - Cloisonner
  - Contrôler les accès logiques
  - Journaliser
  - Contrôler l'intégrité
  - Archiver
  - Sécuriser les documents papier

- Mesures générales de sécurité
  - Sécuriser l'exploitation
  - Lutter contre les logiciels malveillants
  - Gérer les postes clients
  - Sécuriser les sites web
  - Sauvegarder
  - Maintenance
  - Sécuriser les canaux informatiques
  - Tracer l'activité du système
  - Contrôler l'accès physique
  - Réduire les vulnérabilités des matériels
  - S'éloigner des sources de risques
  - Se protéger des sources de risques non humaines

- Mesures organisationnelles
  - Gérer l'organisation de la protection de la vie privée
  - Gérer la politique de protection de la vie privée
  - Gérer les risques
  - Intégrer la protection de la vie privée dans les projets
  - Gérer les incidents de sécurité et les violations de données
  - Réduire les vulnérabilités du personnel
  - Relations avec les tiers
  - Superviser la protection de la vie privée

Identification risques initiaux et impacts

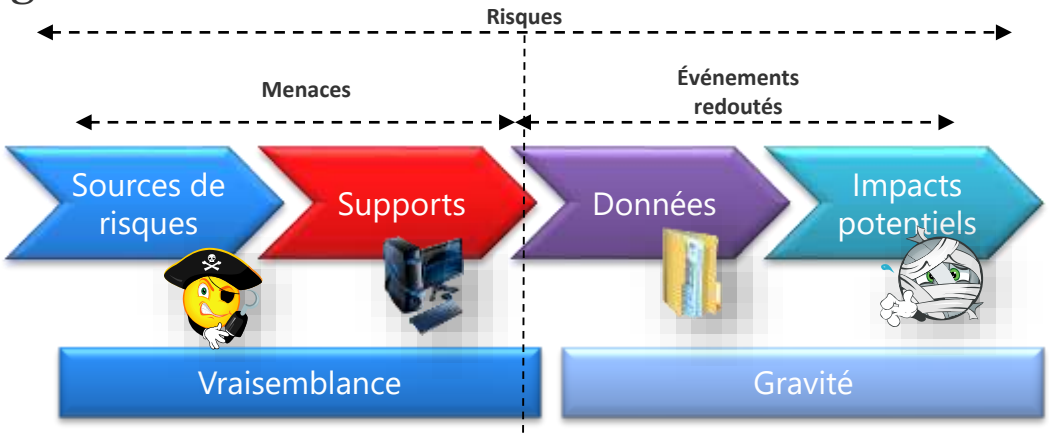
(étape 4)

- Il existe un « risque sur la vie privée » dans le cas suivant :
  - menaces + évènement redouté + atteinte potentielle à la confidentialité, intégrité ou à la disponibilité (accès, modification, disparition)
  - Fait peser un risque sur la vie privée car il peut avoir des impacts potentiels sur les droits et libertés des personnes

L'identification des risques initiaux et des impacts

(étape 4)

- Un risque sur la « vie privée » est un scénario décrivant un événement redouté et toutes les menaces qui le rendent possible. Il est estimé en termes de gravité et de vraisemblance



- Sources de risques
  - Personnes externes
  - Personnes internes
  - Sources non humaines
- Supports
  - Matériels
  - Logiciels
  - Réseaux
  - Personnes
  - Supports papier
  - Canaux papier
- Données
  - Données du traitement
  - Données liées aux mesures
- Impacts potentiels
  - Vie privée
  - Identité humaine
  - Droits de l'homme
  - Libertés publiques

L'identification des risques initiaux et impacts

(étape 4)

❖ Ce risque est estimé en termes de **gravité** et de **vraisemblance**

- Mesure de la gravité: quelles conséquences réelles pour les personnes concernées (et non pour l'organisme !)

- Mesure de la vraisemblance : quel est le niveau de probabilité que l'évènement redouté se réalise ? Toutes les menaces qui permettraient que l'événement redouté se réalise

Voir nombreux exemples de menaces, d'évènements et d'impacts à partir de la page 9 :
https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf

L'évaluation

(étape 5)

- Analyser la conformité de ce premier « état des lieux »
  - Utiliser la documentation disponible (RGPD, méthodologie de référence, référentiel, recommandations CNIL, documentation de outil AIPD…)

- Analyser chacun des risques identifiés et les impacts correspondants
  - Scénario : un ancien employé conserve ses accès et les utilise pour accéder à des informations confidentielles
  - Exemple de risque : accès illégitime avec fort niveau de vraisemblance
  - Impact potentiel : risque de chantage…

- Identifier tous les points d'amélioration qui vont permettre de traiter ces risques
  - Exemple de mesure correctrice : révision de la procédure de gestion des habilitations

Le risque résiduel

(Étape 6)

❖ Ré-évaluer les risques en tenant compte des mesures correctrices

Obtenir le risque résiduel

❖ Un risque résiduel élevé est « inacceptable » (lignes directrices du G29)

- **Gravité :** *« dès lors qu'il exposerait les personnes à des conséquences importantes, voire irréversibles, qu'elles seraient susceptibles de ne pas pouvoir surmonter (par ex:. un accès illégitime à leurs données qui pourrait menacer leur vie, entraîner une mise à pied, mettre en péril leur situation financière) »*

et/ou

- ***Vraisemblance** : « lorsqu'il semble évident que le risque se concrétisera (par ex.: dans la mesure où il n'est pas possible de réduire le nombre de personnes accédant aux données en raison de leurs modes de partage, d'utilisation ou de distribution, ou en présence d'une vulnérabilité bien connue non corrigée). »*

Le risque résiduel

5.2 Appréciation des risques

Echelles d'évaluation du risque

- ***Echelle de vraisemblance***

1	Exceptionnelle	Théoriquement possible, pas de cas rencontré par ailleurs, ou réalisable dans des conditions particulières, très difficiles à obtenir, nécessitant des moyens et compétences très importants. Evènement très rare s'il s'agit d'un accident. Cela ne devrait pas se produire.
2	Peu probable	Cas déjà rencontré une ou plusieurs fois, rarement pour un incident d'origine involontaire, ou réalisable dans des conditions difficiles pour une malveillance, avec nécessité de personnes organisées, très compétentes et disposant de moyens importants, ou malveillance présente peu d'intérêt pour son auteur. Cela pourrait se produire.
3	Plausible	Cas rencontré assez fréquemment par ailleurs, pouvant se produire avec probabilité pour un incident d'origine involontaire, ou réalisable dans des conditions occasionnelles pour une malveillance, par des personnes ou organisations dotées de moyens limités. Cela devrait se produire un jour ou l'autre.
4	Quasi certaine	Cas auquel le système est de toute façon confronté, fréquent s'il s'agit d'un incident d'origine involontaire, ou réalisable facilement et avec un intérêt évident s'il s'agit d'une malveillance. Cela va certainement se produire.

5.2.1 Echelle de vraisemblance basée en partie sur l'analyse de risque de l'outil.

- ***Echelle de gravité***

Axes de gravité	Gravité			
	1 - Mineur	2 – Faible	3 – Significatif	4 - Critique
Impact sur la santé d'un patient	**Sans aggravation** de l'état de santé	Aggravation **limitée** de l'état de santé d'un patient (l'état du patient reste stable)	Aggravation **significative** de l'état de santé d'un patient mais le pronostic vital **n'est pas engagé** (l'état du patient devient instable)	Aggravation significative de l'état de santé d'un patient et son **pronostic vital est engagé.**
			Mise en danger de la vie **d'un patient**	Mise en danger de la vie de **plusieurs patients**

Synthèse de la démarche

❖ Action I :

- Rédiger l'AIPD (contexte, juridique, sécurité - étapes 1,2,3)
- Identifier les risques initiaux (accès, modification, disparition – étape 4) et leurs impacts

❖ Action II

- Evaluer + identifier les mesures correctrices = recommandations qui faites lors de l'évaluation (juridique/technique/organisationnelles – étape 5)

❖ Action III

- Réévaluer les risques initiaux en tenant compte des mesures correctrices identifiées (étape 6)

Les étapes 5 et 6 peuvent être renouvelées plusieurs fois

démarche itérative

\ /

diminution niveaux vraisemblance et gravité

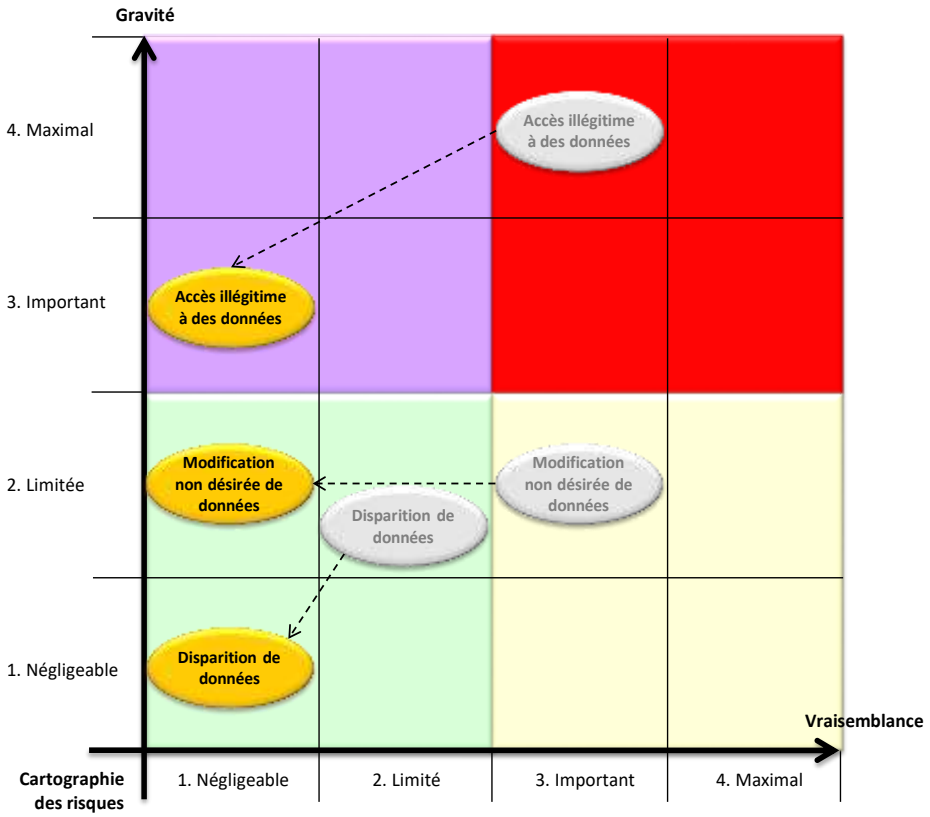
\ /

réduction des impacts

↓

risque résiduel faible

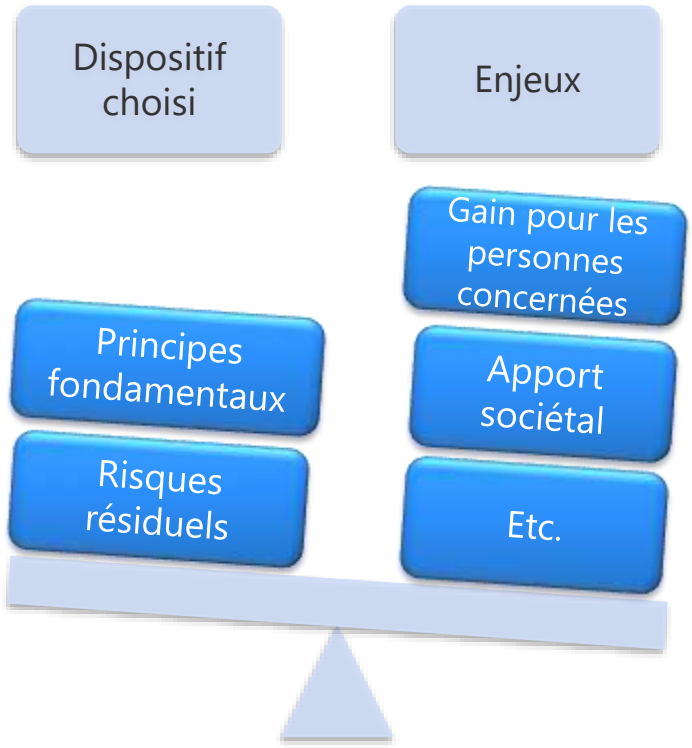
Cartographie du traitement des risques



- Une cartographie des risques permet de comparer visuellement les risques les uns par rapport aux autres
- Elle permet également de faciliter la détermination des objectifs pour les traiter (par « zones »)

La décision

Les risques résiduels sont-ils acceptables ?



- Si les mesures prévues (pour respecter les principes fondamentaux et traiter les risques) sont jugées suffisantes et les risques résiduels acceptables, alors l'AIPD peut être validée par le responsable de traitement
- Sinon, alors il convient d'identifier les objectifs pour y parvenir et de refaire une itération de la démarche

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

MERCI DE VOTRE ATTENTION