ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence, de la protection des données et de la médiation ATPrDM
Kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation ÖDSMB

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08
www.fr.ch/atprdm

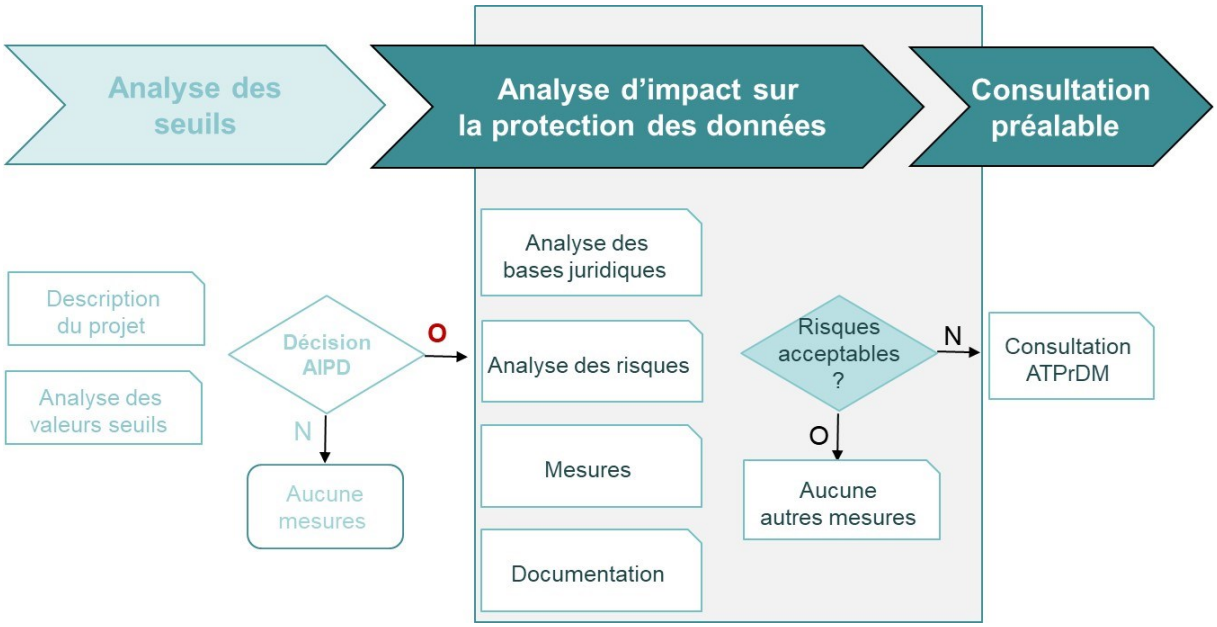
2024-PrD-301

V2.2 du 09. Janvier 2025

1 Analyse d'impact sur la protection des données (deuxième partie) – évaluation des risques du point de vue de la protection des données

1.1 Procédure décisionnelle

L'analyse des valeurs seuils de votre traitement de données a montré qu'une analyse d'impact sur la protection des données est nécessaire. La suite de la procédure est schématisée ci-dessous.



L'AIPD proprement dite se fonde sur :

1. L'analyse des bases juridiques et des fondements du traitement des données
2. L'analyse des risques
3. Le catalogue des mesures
4. La documentation de l'analyse

Ce présent document a pour objectif de fournir un guide général pour réaliser les trois premiers themes d'une AIPD. La documentation est à préparer par le responsable de traitement concerné.

1.2 Marche à suivre

Ce guide est à compléter dans l'ordre des chapitres.

Au chapitre 3, il convient d'évaluer les risques dans une situation où aucune mesure de sécurité n'est prise. Dans la pratique, certaines mesures sont déjà implémentées. Il convient dès lors de partir d'une situation hypothétique où aucune mesure n'est prise.

Au chapitre 5, il sied d'évaluer les risques dans un contexte où toutes les mesures de sécurité sont mises en œuvre ou sont à mettre en œuvre.

Ce n'est que dans le cas où l'activité de traitement présente en dépit des mesures des risques élevés que le responsable de traitement doit consulter l'Autorité de surveillance (art. 42 al. 1 LPrD).

Une liste exemplative de documents attendus se trouve au chapitre 7 du présent guide.

L'Autorité de surveillance communique ses éventuelles objections et recommandations concernant le traitement envisagé dans un délai de deux mois. Exceptionnellement, ce délai peut être prolongé d'un mois, lorsqu'il s'agit d'un traitement de données complexe.

2 Analyse des fondements du traitement des données

2.1 Bases légales

Énumérez les bases légales sur lesquelles se fondent le traitement des données.

…

2.2 Cycle de vie des données

Décrivez le cycle de vie des données.

- **Collecte de données** : indiquez les sources et les formes de collecte des données

  …

- **Utilisation** : indiquez le cercle des utilisateurs (y compris les procédures d'appel) et le type d'utilisation des données (collecte, consultation, copie, modification, sous-traitant, etc.)

  …

- **Stockage** : indiquez le stockage (support, moyens techniques, sous-traitance à des tiers, etc.) et les lieux de stockage des données

  …

- **Conservation** : indiquez les exigences légales relatives à la conservation des données (en particulier la durée de conservation)

  …

- **Archivage** : indiquez les bases légales obligeant ou interdisant l'archivage des données

  …

- **Suppression** : indiquez les exigences légales en matière de suppression des données (procédure à mettre en place pour la suppression des données, anonymisation des données, etc.)

2.3 Proportionnalité

Indiquez les mesures prises pour respecter le principe de la proportionnalité en matière de traitement des données. Seules des données aptes et nécessaires à atteindre les finalités du traitement peuvent être traitées. Il découle du principe de la proportionnalité que le but du traitement doit être réalisé dans la mesure du possible sans collecte de données nouvelles et que seules les données absolument nécessaires au but poursuivi soient traitées.

…

3 Évaluation des risques du point de vue de la protection des données (voir annexe 1)

3.1 Évaluation des risques principaux (sans les mesures de sécurité)

Accès non autorisé à des données personnelles (confidentialité).	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☒	☐
	faible	☐	☐	☐
Manipulation non autorisée de données personnelles (intégrité).	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☒
	faible	☐	☐	☐
Perte des données / aucun accès aux données (disponibilité).	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐
Communication / transmission non autorisée de données personnelles en Suisse et / ou à l'étranger.	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☒	☐	☐

	faible	☐	☐	☐

Mise en péril des mesures de protection (ex : le chiffrement, l'anonymisation, la pseudonymisation, la transmission du mot de passe, les pares-feux, les antivirus, etc.).	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐

Insuffisance ou absence de directives pour les utilisateurs. Manque de sensibilisation, de formation et de contrôle.	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐

Absence d'accord contractuel avec les prestataires de services ou accords contractuels insuffisants ou défaillants.	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐

Autres risques *(précisez)* : …… …… ……	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐

Autres risques *(précisez)* : …… …… ……	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐

4 Mesures visant à minimiser les risques

Le responsable de traitement doit adopter des mesures propres à réduire les risques ayant un impact moyen ou élevé. Ces mesures doivent être mises en œuvre avant le début du traitement des données envisagé.

Le présent guide propose ci-dessous une liste exemplative de mesures inspirées de la norme ISO 27002.

4.1 Mesures générales pour la protection de base

	Non	Oui
Il existe un SMSI (Système de management de la sécurité de l'information). Le traitement de données est lié à celui-ci.	☒	☐
Une organisation de la sécurité est établie : les responsabilités, les tâches et les compétences pour la protection des données sont définies et attribuées.	☐	☐
La sensibilisation des utilisateurs-trices au traitement des données personnelles est en place dans l'organisation (introduction et formation).	☐	☐
Les données sont classifiées (art. 9 du Règlement sur la sécurité des données personnelles) et les propriétaires des données personnelles sont déterminés.	☐	☐
L'application est exploitée dans un environnement certifié (p. ex : ISO 27001).	☐	☒

4.2 Mesures spécifiques à l'application

Le concept d'autorisation est établi et les principes de l'approche « need-to-know » sont pris en compte.	☐	☐
Tous les destinataires de données personnelles externes/internes sont désignés et il est assuré qu'ils sont autorisés à traiter des données.	☐	☐
L'intégrité des données personnelles est assurée (aucune manipulation intentionnelle ou involontaire des données personnelles n'est possible).	☐	☐
Les mesures de chiffrement nécessaires permettant la protection des données personnelles sont appliquées avec précision.	☐	☐
La gestion des clés cryptographiques est du ressort exclusif de l'institution responsable.	☐	☐
Les mesures pour une protection physique adéquate des données et des systèmes sont prises et leur efficacité est vérifiée.	☐	☐
Les processus d'exploitation pour la gestion du changement et de la mise en production sont établis.	☐	☐
Les données sont régulièrement sauvegardées (sauvegarde & restauration).	☐	☐
Il y a une protection appropriée contre les logiciels malveillants.	☐	☐
Les accès aux données sont répertoriés et vérifiés.	☐	☐
Les mises à jour de sécurité sont installées rapidement selon des procédures testées.	☐	☐
La sécurité du réseau est assurée.	☐	☐
Les canaux de communication sont définis et répondent aux exigences en matière de protection des données.	☐	☐
Les fournisseurs sont tenus de respecter les exigences en matière de protection des données (contrat, SLA).	☐	☐
Les mesures de sécurité sont contrôlées et adaptées périodiquement.	☐	☐

Il existe un manuel d'utilisation pour les utilisateurs et/ou une formation des utilisateurs.	☐	☐
Autres mesures *(précisez)* :	☐	☐

5 Évaluation des risques après la mise en œuvre des mesures

5.1 Évaluations des risques principaux (avec les mesures)

	Probabilité d'occurrence	**Impact :** faible	moyen	élevé
Accès non autorisé à des données personnelles (confidentialité).	élevé	☐	☐	☐
	moyen	☐	☒	☐
	faible	☐	☐	☐
	Probabilité d'occurrence	**Impact :** faible	moyen	élevé
Manipulation non autorisée de données personnelles (intégrité).	élevé	☐	☐	☐
	moyen	☐	☐	☒
	faible	☐	☐	☐
	Probabilité d'occurrence	**Impact :** faible	moyen	élevé
Perte des données / aucun accès aux données (disponibilité).	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐
	Probabilité d'occurrence	**Impact :** faible	moyen	élevé
Communication / transmission non autorisée de données personnelles en Suisse et / ou à l'étranger.	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐
	Probabilité d'occurrence	**Impact :** faible	moyen	élevé
Mise en péril des mesures de protection (ex : le chiffrement, l'anonymisation, la pseudonymisation, la transmission du mot de passe, les pares-feux, les antivirus, etc.).	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐
	Probabilité d'occurrence	**Impact :** faible	moyen	élevé
Insuffisance ou absence de directives pour les utilisateurs. Manque de sensibilisation, de formation et de contrôle.	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐

Absence d'accord contractuel avec les prestataires de services ou accords contractuels insuffisants ou défaillants.	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐
Autres risques *(précisez)* : …… …… ……	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐
Autres risques *(précisez)* : …… …… ……	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐

5.2 Risques résiduels

Indiquez les risques moyens (jaunes) ou élevés (rouges) qui subsistent après la mise en œuvre des mesures.

..
..
..
..

6 Nécessité de consultation de l'Autorité de surveillance

S'il existe encore des risques résiduels (chapitre 5.2) qui comportent des risques élevés pour les droits fondamentaux de la personne concernée (risques en rouge ou en jaune), le responsable de traitement doit consulter l'Autorité de la transparence, de la protection des données et de la médiation du canton de Fribourg (art. 42 al. 1 LPrD).

Cas échéant, il remettra à l'autorité toute documentation utile (chapitre 7) ainsi que la présente AIPD

Une consultation de l'Autorité de surveillance est nécessaire.	NON ☐	OUI ☐

Date : Signature :

7 Preuves et documentations

Il convient de remettre à l'Autorité de surveillance toute documentation décrivant les mesures organisationnelles, techniques et juridiques propres à garantir une exploitation conforme à la protection des données.

Les documents nécessaires sont les suivants :

- Concept SIPD
- Concept de droit d'accès
- Plan architectural
- Cycle de vie des données, y compris le concept de suppression
- Règlement du personnel concernant le traitement des données personnelles
- Contrats des fournisseurs (contrats de services)
- Bases légales du traitement des données
- Autres documents

Annexe 1 : Exemple d'évaluation des risques

Un risque est calculé à partir du produit de la probabilité d'occurrence et de l'impact. **Cette évaluation peut varier fortement en fonction du type et de l'ampleur du traitement des données. C'est pourquoi il est important de vérifier cette évaluation en fonction du traitement des données/du projet en question et de l'adapter si nécessaire.**

La probabilité d'occurrence peut être classé en trois niveaux : élevé, moyen ou faible. Ceux-ci peuvent varier en fonction de la situation et doivent être précisés au cas par cas. Exemple d'évaluation des trois niveaux :

- faible : moins d'une fois tous les 10 ans.
- Moyen : tous les 2 à 5 ans ;
- Élevé : plusieurs fois par an ;

L'impact peut être classé en trois niveaux : faible, moyen ou élevé. Cela peut varier en fonction de la situation et doit être précisé au cas par cas. Ces niveaux peuvent être décrits comme suit :

- Faible : impact négligeable sur la sécurité et la protection des données; préjudices moraux ou sociaux à peine perceptibles ; éventuel dommage financier minimal ;
- Moyen : impact sur la sécurité et la protection des données faible sur le long terme ou grave à court terme ; faibles préjudices psychiques, moraux ou sociaux ; éventuel dommage financier ;
- Elevé : impact sur la sécurité et la protection des données grave sur le long terme ; préjudices physiques, psychiques, moraux et sociaux de gravité moyenne ; dommage financier substantiel.

Les risques en vert dans la matrice ci-dessous peuvent être considérés comme acceptables, c'est-à-dire que les risques résiduels sont admissibles sans que des mesures ne doivent être prises. Les risques en jaune ou en rouge doivent être considérés comme élevés et des mesures s'imposent afin de la ramener si possible dans la zone verte.

Evaluation des risques	Impact		
Probabilité d'occurrence	faible	moyen	elevé
elevé			
moyen			
faible			