



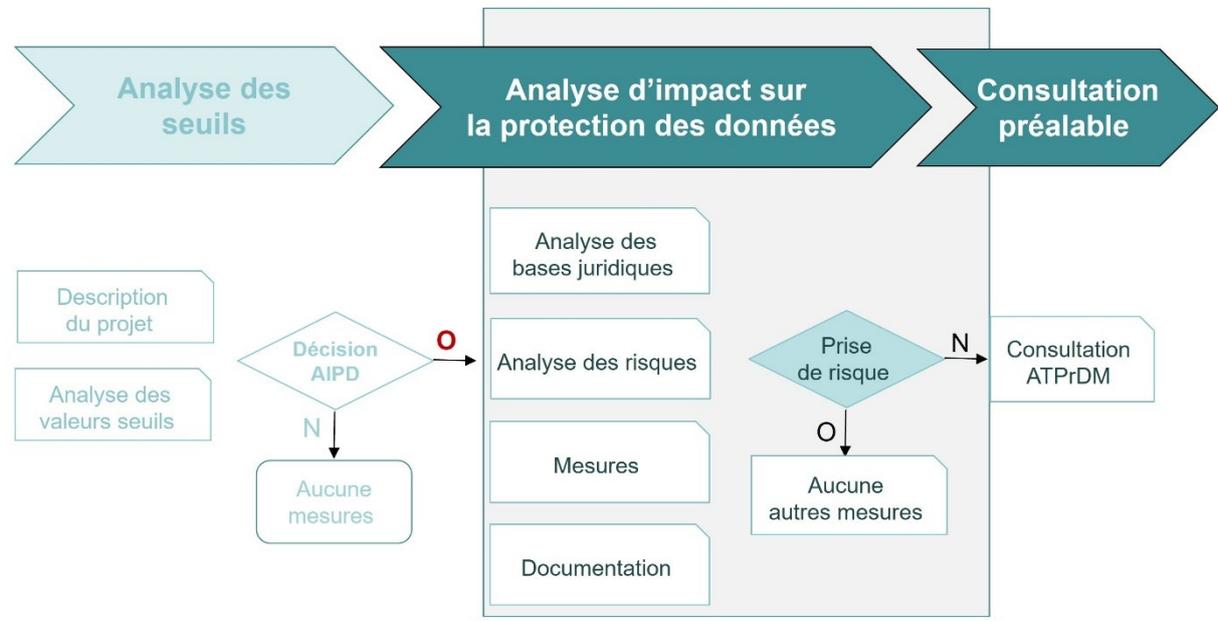
V2 du 26 janvier 2024

## 1 Analyse d'impact sur la protection des données AIPD

### 1.1 Situation initiale

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 :

### 1.2 Procédure-AIPD



Comme il ressort de la procédure, il faut pour cela :

- Analyse des bases juridiques
- Analyse des risques
- Catalogue des mesures
- Documentation

Utilisez pour cela les modèles des chapitres suivants.

## 2 Analyse des bases juridiques

### 2.1 Bases juridiques

Sur quelles bases juridiques 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

- Utilisation : indiquez le cercle des utilisateurs-trices et le type d'utilisation

- Stockage : indiquez le stockage et les lieux de stockage

- Conservation : indiquez les exigences légales pour la conservation des données

- Archivage : Indiquez la base juridique pour / contre l'archivage

- Suppression : Indiquez les exigences légales pour la suppression des données

### 2.3 Proportionnalité

Établissez la proportionnalité de l'utilisation prévue en tenant compte du principe de l'économicité et de la minimisation des données

### 3 Évaluation des risques du point de vue de la protection des données

#### 3.1 Évaluation des risques principaux (sans les mesures)

Accès non autorisé à des données personnelles (confidentialité)	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Manipulation non autorisée de données personnelles (intégrité)	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Perte des données / aucun accès aux données (disponibilité)	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Communication/transmission non autorisée de données personnelles en Suisse et/ou à l'étranger	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mise en péril des mesures de protection (ex : le cryptage, l'anonymisation / la pseudonymisation, la transmission du mot de passe, les logiciels malveillants, etc...)	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Insuffisance ou absence de directives pour les utilisateurs. Manque de sensibilisation / formation / contrôle	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Absence/insuffisance d'accords contractuels avec les prestataires de services	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Autres risques	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Autres risques	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 4 Mesures visant à minimiser les risques

Parmi les mesures suivantes<sup>1</sup>, lesquelles sont les plus propices à réduire les risques et seront mises en œuvre avant le début de l'exploitation.

### 4.1 Mesures générales pour la protection de base

	Non	Oui
Il existe un SMSI (Information Security Management System). Le traitement de données est lié à celui-ci.	<input type="checkbox"/>	<input type="checkbox"/>
Une organisation de la sécurité est établie : les responsabilités, les tâches et les compétences pour la protection des données sont définies et attribuées.	<input type="checkbox"/>	<input type="checkbox"/>
La sensibilisation des utilisateurs-trices au traitement des données personnelles est en place dans l'organisation (introduction, formation).	<input type="checkbox"/>	<input type="checkbox"/>
Les données sont classifiées (art. 9, Règlement sur la sécurité des données personnelles RSD) et les propriétaires des données personnelles sont déterminés.	<input type="checkbox"/>	<input type="checkbox"/>
L'application est exploitée dans un environnement certifié (ex : ISO 27001/2).	<input type="checkbox"/>	<input type="checkbox"/>

### 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.	<input type="checkbox"/>	<input type="checkbox"/>
Tous les destinataires de données personnelles externes/internes sont désignés et il est assuré qu'ils sont autorisés à traiter des données.	<input type="checkbox"/>	<input type="checkbox"/>
L'intégrité des données personnelles est assurée (aucune manipulation intentionnelle ou involontaire des données personnelles n'est possible).	<input type="checkbox"/>	<input type="checkbox"/>
Les mesures de cryptage/chiffrement nécessaires permettant la protection des données personnelles sont appliquées avec précision.	<input type="checkbox"/>	<input type="checkbox"/>
La gestion des clés cryptographiques est du ressort exclusif de l'institution responsable.	<input type="checkbox"/>	<input type="checkbox"/>
Les mesures pour une protection physique adéquate des données et des systèmes sont prises et leur efficacité est vérifiée.	<input type="checkbox"/>	<input type="checkbox"/>
Les processus d'exploitation pour la gestion du changement et de la mise en production sont établis.	<input type="checkbox"/>	<input type="checkbox"/>
Les données sont régulièrement sauvegardées (sauvegarde & restauration).	<input type="checkbox"/>	<input type="checkbox"/>
Il y a une protection appropriée contre les logiciels malveillants.	<input type="checkbox"/>	<input type="checkbox"/>
Les accès aux données sont répertoriés et vérifiés.	<input type="checkbox"/>	<input type="checkbox"/>
Les mises à jour de sécurité sont installées rapidement selon des procédures testées.	<input type="checkbox"/>	<input type="checkbox"/>

<sup>1</sup> Inspiré de la norme ISO 27002

La sécurité du réseau est assurée.	<input type="checkbox"/>	<input type="checkbox"/>
Les canaux de communication sont définis et répondent aux exigences en matière de protection des données.	<input type="checkbox"/>	<input type="checkbox"/>
Les fournisseurs sont tenus de respecter les exigences en matière de protection des données (contrat, SLA).	<input type="checkbox"/>	<input type="checkbox"/>
Les mesures de sécurité sont contrôlées et adaptées périodiquement.	<input type="checkbox"/>	<input type="checkbox"/>
Il existe un manuel d'utilisation pour les utilisateurs et/ou une formation des utilisateurs	<input type="checkbox"/>	<input type="checkbox"/>
Autres mesures :	<input type="checkbox"/>	<input type="checkbox"/>

## 5 Évaluation des risques après la mise en œuvre des mesures

### 5.1 Évaluations des risques principaux (avec les mesures)

Accès non autorisé à des données personnelles (confidentialité)	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Manipulation non autorisée de données personnelles (intégrité)	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Perte des données / aucun accès aux données (disponibilité)	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Communication/transmission non autorisée de données personnelles en Suisse et/ou à l'étranger	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mise en péril des mesures de protection (ex : le cryptage, l'anonymisation / la pseudonymisation, la transmission du mot de passe, les logiciels malveillants, etc...)	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Insuffisance ou absence de directives pour les utilisateurs. Manque de sensibilisation / formation / contrôle	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Absence/insuffisance d'accords contractuels avec les prestataires de services	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Autres risques	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Autres risques	<b>Probabilité d'occurrence</b>	<b>Impact :</b>		
		faible	moyen	élevé
	élevé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	moyen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	faible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 5.2 Risques résiduels

Indiquez les risques qui sont encore « jaunes » ou « rouges » dans l'évaluation après la mise en œuvre des mesures :

..
..

## 6 Décision de consultation préalable

Si des risques sont mentionnés au chapitre 5.2, une consultation préalable de l’Autorité cantonale de la transparence, de la protection des données et de la médiation du canton de Fribourg est nécessaire.

Une consultation préalable est nécessaire	NON <input type="checkbox"/>	OUI <input type="checkbox"/>
---	---------------------------------	---------------------------------

Date:

Signature:

## 7 Preuves et documentations

Il convient de mentionner ici les justifications et la documentation qui décrivent les mesures organisationnelles, juridiques et techniques assurant une exploitation conforme à la protection des données :

- 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