

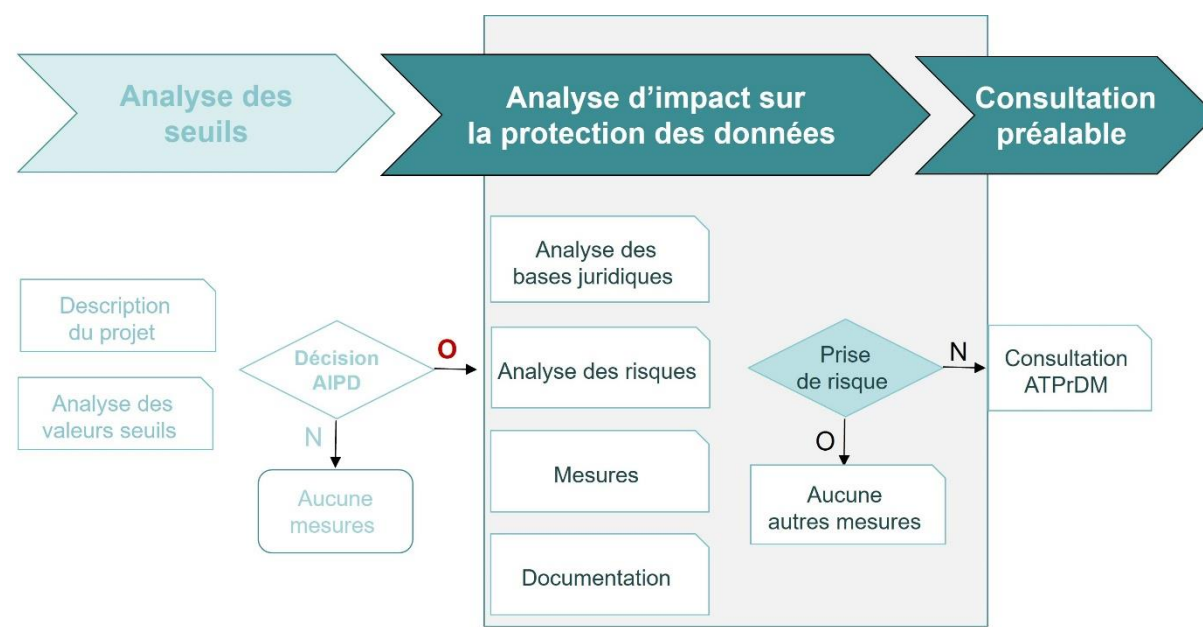


V2.1 du 27 août 2024

# 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 (première partie de l'analyse d'impact sur la protection des données). L'analyse d'impact relative à la protection des données (AIPD) à proprement dite est alors nécessaire. La suite de la procédure est schématisée ci-dessous.



L'AIPD proprement dite se fonde sur l'analyse des bases juridiques et des fondements du traitement des données, l'analyse des risques, le catalogue des mesures et la documentation de l'analyse.

Ce présent document a pour objectif de fournir un guide général pour réaliser les trois premières exigences 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. 2 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

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

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 chiffrement, l'anonymisation, la pseudonymisation, la transmission du mot de passe, les pare-feux, les antivirus, 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, de formation et de 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 d'accord contractuel avec les prestataires de services ou accords contractuels insuffisants ou défallants.	<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 ( <i>précisez</i> ) : ..... ..... .....	<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 ( <i>précisez</i> ) : ..... ..... .....	<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

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 ISMS (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 et formation).	<input type="checkbox"/>	<input type="checkbox"/>
Les données sont classifiées (art. 9 du Règlement sur la sécurité des données personnelles) et les propriétaires des données personnelles sont déterminés.	<input type="checkbox"/>	<input type="checkbox"/>
L'application est exploitée dans un environnement certifié (p. 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"/>

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 ( <i>précisez</i> ) :	<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 chiffrement, l'anonymisation, la pseudonymisation, la transmission du mot de passe, les pare-feux, les antivirus, 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, de formation et de 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 d'accord contractuel avec les prestataires de services ou accords contractuels insuffisants ou défallants.	<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 ( <i>précisez</i> ) : ..... ..... .....	<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 ( <i>précisez</i> ) : ..... ..... .....	<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 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), 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 LPrD).

Cas échéant, il remettra à l’autorité toute documentation utile (chapitre 7) ainsi que la présente AIPD (la première et la deuxième partie).

Une consultation de l’Autorité de surveillance est nécessaire.	NON <input type="checkbox"/>	OUI <input type="checkbox"/>
--	---------------------------------	---------------------------------

Date :

Signature :

## 7 Preuves et documentations

Il convient de remettre à l’Autorité de surveillance toute documentation décrivant les mesures organisationnelles, juridiques et techniques 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