



ETAT DE FRIBOURG
STAAT FREIBURG

**Autorité cantonale de la transparence, de la
protection des données et de la médiation APrDM**
**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 (première partie) – examen préalable des risques pour les droits fondamentaux des personnes concernées

1.1 Fondement de l'analyse d'impact sur la protection des données

Lorsqu'un nouveau traitement de données est susceptible d'engendrer un risque élevé pour les droits fondamentaux de la personne concernée, le responsable du traitement procède préalablement à une analyse d'impact relative à la protection des données personnelles (AIPD ; art. 41 al. 1 LPrD).

Pour rappel, une AIPD est nécessaire uniquement lorsque le projet vise à traiter des données personnelles au sens de l'article 4 alinéa 1 lettre a LPrD. Ainsi, des activités de traitement de données publiques ou anonymes ne sont pas soumises à l'obligation de réaliser une AIPD.

Notions importantes

Les données personnelles sont toutes les informations qui se rapportent à une personne identifiée ou identifiable. Ne sont pas considérées comme des données personnelles le budget de l'État, des mesures météorologiques ou des données qui ne sont pas ou qui ne peuvent pas être liées à une personne identifiable.

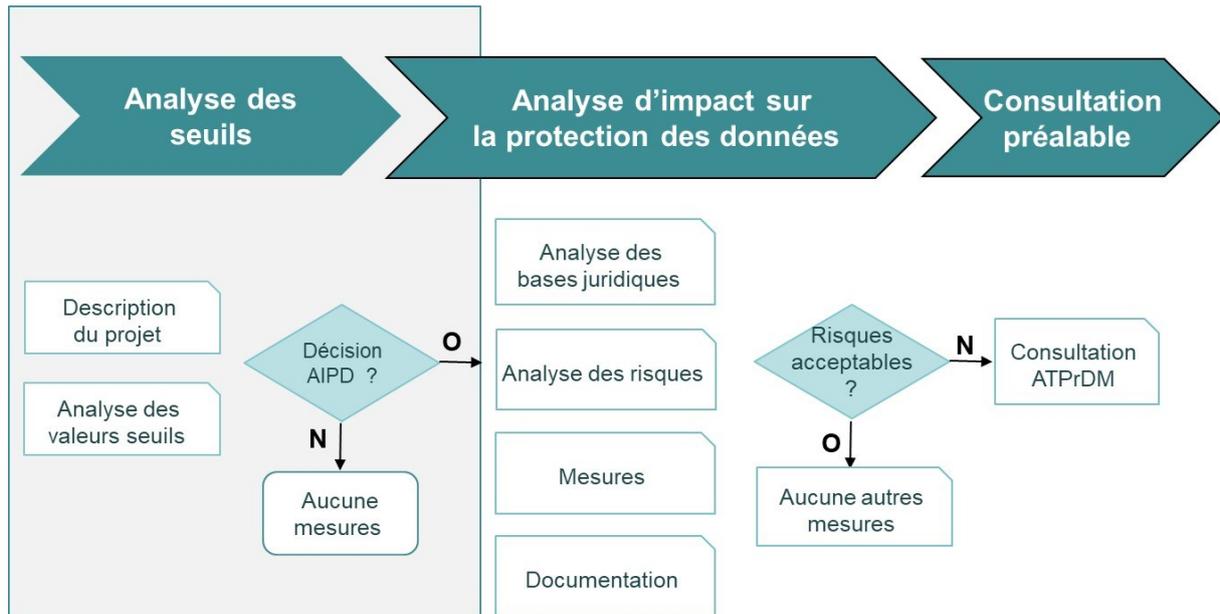
1.2 Objectif du document

Pour déterminer si le traitement de données envisagé présente un risque élevé ou non, le présent document fournit un modèle de mesure du risque. L'utilisation de ce document est facultative. Le responsable de traitement peut documenter son AIPD avec d'autres outils, notamment le concept SIPD.

Ce présent modèle est à remplir une fois le concept SIPD établi. Il est complémentaire au concept SIPD et peut s'y référer.

1.3 Procédure décisionnelle

Le schéma ci-dessous résume les différentes étapes relatives à une AIPD. En cas de risque élevé, le responsable du traitement doit consulter l'Autorité de surveillance (art. 42 al. 1 LPrD).



Dans la première phase d'une AIPD dite « analyse des seuils », il est conseillé de rédiger au préalable une description du traitement de données envisagé dans le cadre du projet. Le chapitre 2 du présent document fournit un modèle à cette fin.

Une fois le projet décrit, le responsable de traitement pourra effectuer l'analyse des valeurs seuils à proprement dite. Au terme de cette analyse, le risque pour les droits fondamentaux des personnes concernées sera qualifié d'élevé ou de faible.

En cas de risque élevé, le traitement de données envisagé doit faire l'objet d'une AIPD.

2 Organisation et description du traitement de données

Ce chapitre vise à donner une description générale du projet. Il concerne toutes les activités de traitement, y compris tous les projets informatiques impliquant un traitement de données personnelles.

2.1 Organisation

Mandataire du traitement de données	
Responsable du traitement de données	
Responsable de la protection des données	
Notions importantes	
<ul style="list-style-type: none"> ▪ <i>Le mandataire du traitement de données</i> est l'entité responsable des résultats du projet et de l'atteinte des objectifs dans le respect des coûts et des délais fixés. Il est chargé de conduire le projet de traitement de données et de le mener à bien. Il s'agit de spécifier une seule entité. ▪ <i>Le responsable du traitement de données</i> est l'entité qui détermine les finalités et les moyens du traitement de données personnelles (art. 4 al. 1 let. h LPrD). Concrètement, il s'agit de l'organe public qui décide du but du traitement des données personnelles et des moyens mis en place pour le faire. Il est possible d'avoir des responsables du traitement de données conjoints (art. 36 al. 2 LPrD). Cas échéant, il convient de préciser et de documenter la 	

responsabilité de chaque organe public concerné (quel organe public est responsable de l'exactitude des données, quel organe est responsable de la mise en œuvre technique de la solution logicielle, etc.). Il s'agit de spécifier une ou plusieurs entités.

- *Le responsable de la protection des données* est la personne physique chargée des questions de protection des données qui travaille pour le compte du responsable du traitement de données. Il est la personne de référence au sein de l'entité responsable du traitement de données. Il s'agit de spécifier une ou plusieurs personnes physiques.

2.2 Description du traitement de données

Mission	
Buts du traitement des données	
Liste des données personnelles traitées	
Cercle des utilisateurs	
Technologies utilisées	
Exploitation (sur site / cloud)	
Sous-traitance et externalisation	
Notions importantes	
<ul style="list-style-type: none"> ▪ <i>La mission</i> consiste à préciser l'objectif général du projet. Exemples : mettre en place un registre des propriétaires de citernes susceptibles de polluer les eaux, déployer une solution de facturation pour toutes les entités de l'administration. ▪ <i>Le but du traitement de données</i> vise à définir la ou les finalités des données traitées. ▪ <i>Les technologies utilisées</i> désignent la mise en œuvre technique du traitement des données. Plusieurs technologies peuvent être utilisées pour une activité de traitement. Exemples : Utilisation des services « cloud » comme par exemple Software as a Service (SaaS¹), utilisation de l'intelligence artificielle, informatique mobile à travers une application pour smartphone, etc. ▪ <i>L'exploitation</i> consiste à définir par quels moyens les données sont exploitées. Il s'agit en particulier de préciser si les données sont traitées en interne ou par le biais de prestataires de services tiers. Exemples : exploitation des données dans les centres de calcul propre, exploitation dans des infrastructures mises en place par le SITel (en interne), exploitation 	

¹ SaaS: le modèle SaaS repose sur le principe que le logiciel et l'infrastructure informatique sont exploités par un prestataire de services informatiques externe et utilisés par le client en tant que service.

externalisée auprès d'un prestataire de services, mise à disposition des données via le cloud, etc.

3 Analyse des valeurs seuils

		Non	Oui
1	Des données sensibles sont-elles traitées à grande échelle ?	<input type="checkbox"/>	<input type="checkbox"/>
2	Un grand nombre de personnes sont-elles concernées ?	<input type="checkbox"/>	<input type="checkbox"/>
3	Les données personnelles sont-elles utilisées/complétées/exploitées par différentes unités organisationnelles ?	<input type="checkbox"/>	<input type="checkbox"/>
4	Le traitement des données a-t-il lieu hors de Suisse dans des États qui ne sont pas soumis au règlement général sur la protection des données (RGPD) ?	<input type="checkbox"/>	<input type="checkbox"/>
5	Les données sont-elles traitées dans un cloud ?	<input type="checkbox"/>	<input type="checkbox"/>
6	Les données ou une partie d'entre elles sont-elles utilisées à des fins de profilage ou peuvent-elles être utilisées à cette fin dans des étapes ultérieures du traitement ?	<input type="checkbox"/>	<input type="checkbox"/>
7	De nouvelles technologies, de nouveaux mécanismes ou de nouvelles procédures sont-ils utilisés ?	<input type="checkbox"/>	<input type="checkbox"/>
8	Des espaces publics étendus sont-ils systématiquement surveillés ?	<input type="checkbox"/>	<input type="checkbox"/>
9	Des données personnelles sont-elles transférées dans un pays tiers où la législation étrangère n'assure pas une protection adéquate ?	<input type="checkbox"/>	<input type="checkbox"/>
10	Un nombre important ou illimité de personnes peuvent-elles accéder aux données ?	<input type="checkbox"/>	<input type="checkbox"/>
11	Existe-t-il un risque lié au traitement de données qui pourrait empêcher un traitement conforme à la protection des données ? (Développement, exploitation, support, etc...)	<input type="checkbox"/>	<input type="checkbox"/>

Remarques importantes relatives aux questions ci-dessus

Question 1	<p><i>Les données personnelles sensibles</i> sont celles définies à l'article 4 alinéa 1 lettre c LPrD. Exemples : données sur la santé, sur des mesures d'aide sociale ou sur les activités religieuses.</p> <p><i>Un traitement à grande échelle</i> signifie un traitement vaste. Sont à prendre en compte, notamment le nombre des personnes concernées, le volume de données traitées, la durée ou la permanence de l'activité de traitement, l'étendue géographique de l'activité de traitement. Il y a également un traitement à grande échelle lorsque les données sont traitées d'une manière systématique. Exemples : les données personnelles d'un service entier, d'un hôpital, de l'ensemble de données des bénéficiaires d'aide sociale, ou si des données personnelles sont collectées de différentes sources ou interconnectées.</p>
------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Question 2	<p><i>Un grand nombre de personnes</i> est une notion indéterminée laissée à l'appréciation du responsable du traitement. Il peut s'agir d'un nombre absolu de personnes ou d'un nombre relatif en proportion du cercle de personnes saisies. Exemples : les données des élèves d'une école primaire.</p> <p><i>Une personne concernée</i> vise une personne dont les données sont traitées. Il ne s'agit donc pas des personnes qui peuvent accéder aux données traitées pour l'accomplissement de leurs tâches (cf. Question 10).</p>
Question 4	<p>Le <i>RGPD</i> (règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données) est un règlement de l'Union européenne. Il s'applique aux 27 États membres de l'Union européenne.</p>
Question 5	<p>Par <i>cloud</i> (informatique en nuage), il faut comprendre des traitements des données effectués hors site par des serveurs gérés par des tiers (art. 4 al. 1 let. g LPrD).</p>
Question 6	<p><i>Le profilage</i> se définit comme toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne (art. 4 al. 1 let. f LPrD).</p> <p>En d'autres termes, il s'agit de déduire des informations sur des personnes à partir des données traitées.</p>
Question 7	<p>Par nouvelles technologies, nouveaux mécanismes et nouvelles procédures, il faut comprendre l'utilisation de nouvelles technologies innovantes, de nouveau type de traitement ou de changements significatifs d'une technologie déjà utilisée. L'utilisation de nouveaux matériels et logiciels sont également inclus dans les nouvelles technologies.</p> <p>Exemples : l'introduction d'un portail, l'utilisation de bodycams, l'utilisation de plateformes d'évaluation pour l'administration publique, les procédures biométriques, l'utilisation d'algorithmes pour la prise de décision automatisée, l'utilisation de l'intelligence artificielle, l'évaluation automatisée d'enregistrements vidéo, smart health, etc.</p>
Question 8	<p><i>La surveillance systématique</i> est définie comme la surveillance convenue, organisée ou méthodique ou ayant lieu dans le cadre d'une stratégie ou d'un plan général de collecte de données. Elle ne comprend pas seulement la vidéosurveillance, mais également la saisie automatique des numéros d'immatriculation des véhicules dans des parkings publics ou places de stationnement, la surveillance dans un hôpital, dans des stations de bus, etc.</p>
Question 10	<p><i>Un nombre important de personnes</i> est une notion indéterminée laissée à l'appréciation du responsable du traitement. Il peut s'agir d'un nombre absolu de personnes ou d'un nombre relatif en proportion du cercle de personnes saisies. Sont également inclus les accès en ligne ou les procédures d'appel. Exemples : l'ensemble des collaborateurs et collaboratrices de l'État.</p>

4. Décision

Si vous avez répondu « OUI » à au moins une des questions du chapitre 3, l'activité de traitement envisagée est soumise à la réalisation obligatoire d'une analyse d'impact sur la protection des données.

Une analyse d'impact sur la protection des données est-elle nécessaire ?	NON <input type="checkbox"/>	OUI <input type="checkbox"/>
--------------------------------------------------------------------------	---------------------------------	---------------------------------

Date :

Signature :

Pour la réalisation de l'analyse d'impact sur la protection des données, vous pouvez utiliser le document « Analyse d'impact sur la protection des données (deuxième partie) – évaluation des risques du point de vue de la protection des données ».