



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/atprd

## Annexe 1

\*\*\*

### Check-liste pour l'externalisation de traitement de données personnelles

\*\*\*

Modèle de contenu non exhaustif des dispositions contractuelles concernant la protection des données personnelles qui peuvent figurer dans un mandat d'externalisation de traitement de données personnelles entre l'organe public responsable du traitement (mandant) et le tiers privé (mandataire) (article 19b alinéa 1 lettre b de la Loi du 12 octobre 2023 sur la protection des données (LPrD ; RSF 17.1)).

#### 1. Description du mandat / détermination des parties / autres éléments du contrat :

- 1.1. le responsable du traitement est-il défini ? Il faut également définir qui est le sous-traitant ; c'est ce dernier qui est effectivement responsable envers la Direction ou le responsable de traitement en cas de mauvaise exécution du contrat ;
- 1.2. il faut déterminer les prestations attendues dans le cadre du mandat, le but (par ex. recouvrement des impôts impayés). Il faut fixer également les délais, l'échéance, le prix, ainsi que toutes autres conditions du mandat.

#### 2. Objet et but de l'externalisation de traitement / nature, finalité et la durée de l'externalisation (art. 19 al. 1 let. b ch. 1 LPrD) :

- 2.1. le but permet de fixer le cadre dans lequel les données vont être transmises au sous-traitant. Ce dernier ne pourra traiter les données que dans ce cadre ;
- 2.2. il convient de prévoir les finalités permises et celles qui sont exclues.

#### 3. Traitement de données et les catégories de données concernées (art. 19 al. 1 let. b ch. 2 LPrD) :

- 3.1. il convient de définir les catégories des données personnelles concernées par l'externalisation ;
- 3.2. la liste des catégories de données sous-traitées, leur degré de sensibilité et leur cycle de vie en détail peuvent faire l'objet d'une annexe.



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/atprd

#### 4. Obligations des parties (art. 19 al. 1 let. b ch. 3 LPrD) :

- 4.1. il convient de s'assurer que le sous-traitant (mandataire) s'engage à traiter les données selon les principes généraux de protection des données tels que prévus par la LPrD et selon les instructions du responsable de traitement (mandant) ;
- 4.2. le sous-traitant (mandataire) doit notamment s'engager à ne pas utiliser les données dans un autre but que celui communiqué par le responsable de traitement (mandant), cela même pour des données pseudonymisées et/ou anonymisées ;
- 4.3. il est notamment conseillé de préciser le devoir d'informer en cas de communication (ou risque y relatif) à une autorité étrangère (l'art. 19 al. 1 let. b ch. 6 LPrD), le devoir d'hébergement en suisse ou dans un Etat garantissant un niveau de protection des données équivalent (art. 18 al. 2 LPrD) ou encore l'obligation de la fourniture des garanties suffisantes (mise en œuvre de mesures techniques et organisationnelles appropriées pour répondre aux exigences imposées par les législations pertinentes, ressources suffisantes pour garantir le respect des différentes obligations telles que la portabilité des données découlant de l'art. 19 al. 1 let. d LPrD, etc.) ;
- 4.4. il est conseillé de donner des instructions en matière de la conservation, destruction et archivage des données aussi bien informatiques que sur papier.

#### 5. Sous-traitance en cascade (art. 19 al. 1 let. b ch. 5 LPrD)

Les questions touchant une éventuelle sous-traitance ultérieure devraient également être réglées. Il est conseillé de définir l'admissibilité ou non de la sous-traitance ultérieure, qui sont les sous-traitants et les mesures de sécurité mises en place pour ceux-ci. A noter : une sous-traitance ultérieure est interdite sans autorisation préalable par le responsable de traitement.

#### 6. Mesures de sécurité des données (art. 20 LPrD et le Règlement du 29 juin 1999 sur la sécurité des données personnes, RSD ; RSF 17.15)

- 6.1. Le sous-traitant (mandataire) est tenu d'engager toutes les mesures de sécurité techniques et organisationnelles pour s'assurer de l'intégrité, de la disponibilité et de la confidentialité des données et d'informer dans les plus brefs délais le (mandant) de tout manquement dans la sécurité des données, de tout accès indu et de toute perte de données ;
- 6.2. ces mesures peuvent être détaillées dans un document en annexe (voire concept SIPD si nécessaire). Les mesures de sécurité des données traitent notamment les questions suivantes :
  - > description des mécanismes cryptographiques s'agissant des données concernées ? (aussi bien au repos qu'en transit) ;
  - > description des mécanismes de gestion des clés (indications quant au stockage ? la détention de la clé. Il est recommandé que le chiffrement soit réalisé par l'organe public et que celui-ci conserve la clé de chiffrement (« Hold Your Own Key ») ;



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/atprd

- > description des risques, risques résiduels, mesures, back-up concept, résilience, etc. (à présenter en annexe, sous la forme d'un document SIPD par exemple) ;
- > preuves des éventuelles certifications et autres standards internationalement reconnus.

## 7. Droits des personnes concernées

Le sous-traitant (mandataire) doit s'engager à permettre au responsable de traitement (mandant) de répondre aux demandes formulées par les personnes dont les données sont sous-traitées et à fournir, dans les plus brefs délais, au responsable de traitement (mandant) toutes les informations et données nécessaires pour répondre à leurs demandes. Il s'agit notamment du droit d'accès à ses propres données (art. 27 ss LPrD), du droit de destruction de données illicites, du droit de modification des données, etc.

## 8. Contrôle, sanctions et surveillance (art. 19 al. 1 let. b ch. 4 LPrD)

- 8.1. le responsable de traitement (mandant) doit s'assurer que le sous-traitant (mandataire) et ses éventuels sous-traitants (avec accord du responsable de traitement), respectent bien le contrat et les obligations de protection des données. Le responsable de traitement doit notamment pouvoir accéder à tous les documents permettant de vérifier le respect des obligations (journal d'événements, rapports d'audits, etc.) ;
- 8.2. le droit d'audit du responsable de traitement auprès du sous-traitant (mandataire) et de ses éventuels sous-traitants en cascade doit exister ;
- 8.3. mentionner que l'Autorité cantonale de la transparence, de la protection des données et de la médiation a la possibilité d'effectuer des contrôles.

## 9. Personnel du mandataire et confidentialité

- 9.1. le sous-traitant (mandataire) s'engage à employer dans le cadre du mandat susmentionné uniquement du personnel ayant préalablement signé un « engagement pour le personnel » qui oblige les signataires à se conformer aux exigences de la protection des données et à garder le secret sur les informations dont ils auront connaissance dans l'exercice du présent mandat ;
- 9.2. le sous-traitant (mandataire) s'engage à veiller au respect effectif des exigences liées à la protection des données ainsi que du secret par ses employés et par ses sous-traitants en cascade (à l'aide des mesures comme sélection, instruction et surveillance adéquates du personnel), et ceci même après l'expiration du mandat.



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/atprd

## **10. Responsabilité et indemnisation**

- 10.1.** Le responsable de traitement s'assure contractuellement que le sous-traitant (mandataire) mette en place les mesures adéquates en lien avec la LPrD pour le traitement des données transmises dans le cadre de la sous-traitance ;
- 10.2.** Le sous-traitant (le mandataire) est responsable pour les faits des sous-traitants en cascade qu'ils soient autorisés ou non. Une indemnisation pleine et entière pour l'ensemble des dommages directs et indirects subis par le responsable de traitement (mandant) et causés par le sous-traitant (mandataire) ou un sous-traitant en cascade est due.

## **11. Durée et résiliation du contrat**

- 11.1.** il convient de prévoir un droit de résilier le contrat par le (mandant), moyennant le respect d'un préavis resp. un délai de résiliation, sauf dans les cas où de justes motifs (à prévoir dans le contrat ; problèmes graves de sécurité par exemple) permettent de résilier immédiatement le contrat ;
- 11.2.** les conséquences de la résiliation du contrat devraient être prévues. Il s'agit notamment de l'obligation de restituer dans les plus brefs délais toutes les données au responsable de traitement (mandant) et de détruire l'ensemble des copies de ces données ;
- 11.3.** il est aussi utile de prévoir la transition vers un autre sous-traitant (rappel de la portabilité des données au sens de l'article 19 LPrD).

## **12. For et droit applicable**

Le droit suisse est-il applicable et un for en Suisse est-il prévu ? il est fortement conseillé d'avoir un for en Suisse.