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

Fribourg, le 26 octobre 2023

Aide-mémoire mandat externalisation de traitement
—

Aide-mémoire concernant l'externalisation de traitement sur mandat (outsourcing) lorsque l'organe public sous-traite le traitement de données personnelles à un tiers privé

1. Objectif

Le présent aide-mémoire se fonde sur le pouvoir de conseil de la Préposée (art. 54 al. 1 let. b de la Loi fribourgeoise du 12 octobre 2023 sur la protection des données, LPrD ; RSF 17.1). A considérer comme ligne de conduite, il a pour but de guider les organes publics cantonaux ou communaux compétents lorsqu'ils font appel à la collaboration de personnes ou d'entreprises privées pour traiter leurs données. Cette collaboration peut porter sur la partie technique du traitement ; elle peut aussi concerner tout ou partie du traitement matériel des données personnelles, comme par ex. la collecte de celles-ci, l'hébergement ou encore le traitement à proprement parler. Le contenu du mandat est défini par le responsable de traitement / evtl. par les parties et doit être adapté au cas d'espèce. Nous vous rendons également attentif aux dispositions du Règlement du 29 juin 1999 sur la sécurité des données personnes (RSD ; RSF 17.15).
L'aide-mémoire est complété par des documents « check-liste pour établir un contrat » et « charte » (voir annexes).

2. Généralités

2.1. Les services de l'administration cantonale et communale font souvent appel à des entreprises ou de personnes privées pour traiter leurs données. Ce type d'externalisation du traitement de données personnelles sur mandat, appelé aussi outsourcing ou traitement sur mandat, est admissible selon la législation.

2.2. L'organe public qui conclut un mandat avec un tiers, demeure responsable de la protection des données (art. 19 ainsi que l'art. 37 al. 1 LPrD). Il garde la compétence de décision concernant les données, sur lui repose la légitimité du traitement et il est responsable que le traitement soit compatible avec les principes généraux de la protection des données. Il doit choisir avec soin le tiers auquel il veut confier les données et veiller à ce que le mandataire respecte les impératifs de la protection des données, plus encore s'il s'agit de données sensibles.

2.3. Le mandataire privé est en principe soumis à la Loi fédérale sur la protection des données du 25 septembre 2020 (LPD ; RS 235.1) et ainsi à la surveillance du Préposé fédéral. Pour que

l'organe public cantonal et communal, soumis à la loi cantonale de protection des données, puisse procéder à une telle externalisation, il doit respecter les principes et exigences prévus à l'article 18 et suivants LPrD.
C'est pourquoi, un contrat doit être conclu contenant les informations minimales citées dans l'article 19 alinéa 1 lettre b LPrD. Cela peut être réalisé sous la forme d'un contrat complémentaire au mandat principal ou faire partie intégrante du mandat.

3. Questions préliminaires à la conclusion et fixation du contenu du mandat

Du point de vue de la protection des données, il semble notamment important de traiter ces questions de manière préalable :

- Des données personnelles au sens de la LPrD (art. 4 al. 1 let. a et d LPrD), qu'elles soient sensibles ou non (art. 4 al. 1 let. c LPrD) seront-elles sous-traitées ?
- Le responsable du traitement est-il défini? Responsable du traitement voire coresponsable (art. 19 et 4 LPrD) ?
- Le responsable du traitement est-il en droit de traiter les données personnelles qui vont faire l'objet de l'externalisation de traitement (art. 19 al. 1 let. c LPrD) ?
- Existe-t-il un contrat écrit avec le sous-traitant qui doit être précisé ? Les clauses de protection des données sont-elles suffisantes ?
- S'agit-il de données personnelles soumises au secret de fonction ? si oui, une clause contractuelle spécifique est-elle prévue ?
- Les données soumises au secret de fonction sont-elles traitées/hébergées par le sous-traitant en Suisse ? Y a-t-il une sous-traitance en cascade à l'étranger ?
- Dans le cas où il y a une sous-traitance ou une sous-traitance en cascade à l'étranger, l'Etat étranger fait-il partie de la liste des Etats assurant un niveau de protection adéquat (Annexe 1 OPDo = Ordonnance sur la protection des données du 31 août 2022, RS 235.11) ?
- Le responsable du traitement a-t-il passé en revue les points essentiels de la sous-traitance ? Voir notamment l'aide-mémoire de Privatim concernant la technologie du cloud.
- Le responsable du traitement est-il en possession de l'analyse des risques (concept SIPD = de sécurité de l'information et protection des données) ?
- Le responsable du traitement a-t-il identifié une personne de contact / in conseiller à la protection des données (« data protection officer », DPO/DPD) ?

4. Obligations principales du mandant / du responsable de traitement

Pour l'exécution du mandat, le mandant devrait notamment, s'assurer des points suivants :

- L'objet et le but du mandat devrait être clairement défini. Cela en le délimitant à un projet, à une affaire ou à une tâche spécifique ;
- Les prestations attendues, les données traitées par le mandataire et toutes autres conditions du mandat (par ex. les délais, l'échéance, le prix, etc.) devraient être clairement fixées ;
- La bonne mise en œuvre par le sous-traitant de mesures techniques et organisationnelles appropriées pour répondre aux exigences imposées par la LPrD et le RSD.

5. Obligations principales du sous-traitant

Dans le cadre de l'exécution du mandat, le sous-traitant devra notamment :

- Respecter toutes les exigences de la protection des données dans la même mesure que le mandant ;
- Choisir son personnel avec soin ;
- Ne faire effectuer des tâches que par des personnes qui se sont préalablement engagées à respecter les obligations liées à la protection des données (voir le document « Charte ») ;
- Donner à son personnel les instructions nécessaires concernant la protection des données ;
- Présenter des garanties suffisantes quant aux ressources nécessaires (techniques, organisationnelles, humaines, etc.) pour exécuter le respect des différentes obligations (telles que la restitution des données découlant de l'art. 19 al.1 let. d LPrD par exemple) ;
- Veiller à ce que son personnel respecte les impératifs de la protection des données.

Ces obligations du sous-traitant doivent être définies et précisées dans le contrat avec le sous-traitant.

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 19 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.

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. 19 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») ;
- 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.

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.

Annexe 2

***

Charte

***

Modèle de déclaration d'« engagement pour le personnel » concernant la protection des données qui, sur la base de son activité, a accès aux données personnelles traitées dans le cadre du présent mandat.

1. La personne soussignée a, sur la base de son activité, accès aux données personnelles.

2. La personne soussignée s'engage à se conformer aux exigences de la protection des données et à garder le secret sur les informations dont elle aura connaissance dans l'exercice du présent mandat. Elle s'engage à traiter les données uniquement pour les fins prévues dans le mandat, à ne pas les réutiliser et à ne les transmettre ou à n'en faire un quelconque autre usage qu'avec l'accord du (mandant).

3. La personne soussignée s'engage à prendre – selon les instructions du (mandataire) – toutes les mesures nécessaires pour que les personnes non autorisées n'aient pas accès aux données personnelles dans le cadre du mandat susmentionné et qu'aucune donnée ne soit perdue.

4. La personne soussignée doit communiquer spontanément au (mandataire) tous problèmes, lacunes ou faiblesses en matière de protection des données qu'elle observera durant l'exercice du mandat.

Par la présente, je confirme avoir pris connaissance des obligations susmentionnées et je m'engage à les respecter.

Nom _____

Fonction _____

Signature _____

Lieu et date _____