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/atprdm

Fribourg, le 26 octobre 2023

Checklist
—

CHECKLIST pour l'externalisation du traitement de données personnelles

Selon les articles 19 ss de la Loi cantonale du 12 octobre 2023 sur la protection des données (LPrD, RSF 17.1), le traitement de données personnelles, y compris de données sensibles peut être externalisé aux conditions posées par la loi. Un contrat doit être conclu contenant les informations minimales citées dans l'article 19 al. 1 let. b LPrD. Il convient également de consulter le Règlement du 29 juin 1999 sur la sécurité des données personnes (RSD ; RSF 17.15) s'agissant des exigences en matière de sécurité des données.

Le présent document, non exhaustif, constitue une aide à la décision et permet de s'assurer que les points principaux ont été prévus dans le contrat. Il est néanmoins important de toujours prendre en compte les spécificités du cas d'espèce.

1. Questions préalables

Eléments à vérifier/prévoir dans le contrat	*Fait/oui*
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) sont-elles sous-traitées ?	☐
Le responsable du traitement est-il défini? S'agit-il du responsable du traitement voire co-responsable selon l'art. 19 al. 2 et 3 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 avec le sous-traitant ?	☐
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 parti de la liste des Etats assurant un niveau de protection adéquat (Annexe 1 OPDo) (art. 18 al. 2 LPrD) ?	☐
Le responsable du traitement a-t-il l'assurance que seuls les traitements confiés seront effectués par le sous-traitant ? Laquelle ?	☐
Est-ce que le contrat contient-il l'interdiction faite au sous-traitant de sous-traiter à son tour un traitement sans l'autorisation préalable du responsable de traitement (art. 19 al. 1 lit. b chiff. 5 LPrD) ?	
Le responsable du traitement a-t-il identifié éventuellement une personne de contact / conseiller à la protection des données (« data protection officer » / DPO/DPD) ?	☐
Le responsable du traitement a-t-il l'assurance que la sécurité des données personnelles sera garantie dans le cadre de cette externalisation de traitement (art. 19 al. 1 LPrD)? est-il en possession de l'analyse des risques (concept SIPD = sûreté/sécurité de l'information et protection des données) ?	☐
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).	☐
Les clauses de protection des données sont-elles suffisantes ?	☐

2. Description du mandat / détermination des parties / autres éléments du contrat

Description du mandat : il sied de déterminer les prestations attendues dans le cadre du mandat, le but du traitement (par ex. recouvrement des impôts impayés). Il faut fixer également les délais, l'échéance, le prix, ainsi que toutes autres conditions du mandat	☐
Détermination des parties : les parties au contrat sont-elles suffisamment définies ? Le responsable de traitement est-il défini ? Evtl. le co-responsable de traitement ?	☐
Détermination des parties : Le sous-traitant est-il clairement défini ? Cela est important notamment pour savoir à qui effectivement on sous-traite le traitement de données personnelles.	☐

3. 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)

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. Est-ce que l'objet et la nature de l'externalisation sont-ils définis d'une manière claire ?	☐
Il convient de prévoir les finalités permises et celles qui sont exclues. Les finalités du traitement sont-elles décrites ?	☐

4. Données personelles

Listing des catégories des données personnelles concernées par l'externalisation (art. 19 al. 1 let. b ch. 2 LPrD). *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.*	☐
Description du processus de migration des données (responsabilités, déroulement et contrôles, essais de réception, vérification de l'intégrité des données, etc.).	☐
S'agit-il de données personnelles sensibles (art. 4 al.1 let. c LPrD)?	☐
Dans le cas de données personnelles (sensibles ou non) soumises au secret de fonction, le sous-traitant, le(s) sous-traitant(s) ultérieur(s) ainsi que leurs employés devront être soumis au secret par le biais d'une clause de confidentialité.	☐
Dans le cas de sous-traitance à l'étranger (notamment sous la forme de redondance/sauvegarde) de données personnelles soumises au secret de fonction ou des données sensibles (art. 21 LPrD)	
Il convient de chiffrer les données soumises au secret en Suisse et de s'assurer que la clé de chiffrement (privée) soit détenue par le responsable du traitement.	☐
Si la clé est détenue par le sous-traitant ou par un tiers en Suisse, le contrat doit inclure des règles strictes sur l'interdiction de transmettre la clé à l'étranger de manière à ce que les données ne puissent être déchiffrées.	☐
Une interdiction stricte de transmettre la clé à l'étranger doit être prévue dans le contrat (cf. violation du secret de fonction, article 320 du Code pénal Suisse du 21 décembre 1937, respectivement du secret professionnel, article 321 CP (CP ; RS 311.0).	☐
Lieux de traitement des données par le sous-traitant.	
Hébergement exclusivement en suisse.	☐
Hébergement dans un Etat garantissant un niveau de protection des données adéquat en vertu de l'art. 18 al. 2 LPrD.	☐
Hébergement dans un Etat **ne garantissant pas** un niveau de protection des données équivalent. Dans ce cas, il faut prévoir des garanties contractuelles supplémentaires pour s'assurer que le sous-traitant et ses éventuels sous-traitants respectent les règles de la LPrD (contrat de communication transfrontière de données 15 al. 2 et 3 LPrD). Attention aux données soumises au secret de fonction.	☐

5. Obligations des parties (art. 19 al. 1 let. b ch. 3 LPrD)

Obligations et droits du responsable du traitement/responsable du fichier		
	Veiller à ce que les obligations et droits soient définis dans le contrat	☐
	S'assurer par quel biais les données sont obtenues et en respectant les principes de la LPrD (licéité, finalité, proportionnalité, exactitude, bonne foi, etc.) (art. 19 al. 1 ch. c LPrD).	☐
	S'assurer que les données seront traités conforment aux exigences légales et contractuelles (droit d'audit et de surveillance, art. 19 al. 1 let. b chiff. 4 LPrD).	☐
	S'assurer quant à la mise en œuvre par le sous-traitant de mesures techniques et organisationnelles appropriées pour répondre aux exigences imposées par la LPrD et le RSD.	☐
Obligations et droits du sous-traitant		
	Prévoir l'obligation de traitement conforme aux instructions et exigences légales (finalité, proportionnalité, exactitude, bonne foi, sécurité des données, etc.).	☐
	Prévoir l'interdiction d'utiliser les données dans un autre but que celui communiqué par le responsable de traitement, cela même pour des données pseudonymisées et/ou anonymisées.	☐
	Prévoir l'obligation de rectifier/effacer les données personnelles dès la réception d'instructions données par le responsable de traitement.	☐
	Prévoir l'obligation de rapatrier les données dans un format exploitable par le responsable de traitement, ce en vertu de l'art. 19 al. 1 let. d LPrD.	☐
	Prévoir le devoir d'informer en cas de toute modification dans la manière de traiter les données (lieu du traitement, sous-traitance, etc.).	☐
	Prévoir le devoir d'informer de failles de sécurité ou tout manquement dans la sécurité des données, de tout accès indu et/ou de toute perte de données.	☐
	Prévoir le devoir d'informer (l'art. 19 al. 1 let. b ch. 6 LPrD) de toute demande de transmission de données personnelles émanant d'une autorité étrangère ou judicaire.	☐
	Prévoir des indications claires quant au(x) lieu(x) de traitement des données personnelles (par exemple, le lieu d'hébergement des de la sauvegarde, de la redondance, de la maintenance, etc.).	☐
	Prévoir l'obligation de sensibiliser et instruire le personnel du sous-traitant concernant la protection des données personnelles et l'élaboration d'une charte destinée au personnel.	☐

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

Les questions touchant une éventuelle sous-traitance ultérieure doivent également être réglées.

Prévoir l'admissibilité ou l'inadmissibilité (et les modalités le cas échéant) d'un recours par le sous-traitant à un autre sous-traitant (sous-traitance en cascade). (Attention : Il y a l'interdiction faite au sous-traitant des sous-traiter à son tour sans l'autorisation préalable du responsable du fichier.)	☐
S'assurer de la clarté des informations s'agissant du destinataire de la sauvegarde et/ou de la redondance des données.	☐
Inclure la possibilité pour le responsable du traitement d'exiger la liste de tous les sous-traitants ultérieurs.	☐
S'assurer que les données personnelles demeurent en suisse.	☐
Dans le cas de sous-traitance en cascade à l'étranger, s'assurer que le sous-traitant ultérieur garantit un niveau de protection des données adéquat.	☐
Indiquer clairement que le sous-traitant reste responsable du respect des exigences légales et contractuelles par ses propres sous-traitants.	☐

7. Mesures de sécurité des données (art. 20 LPrD + RSD)

La précision des mesures techniques et organisationnelles en détail peut faire l'objet d'une annexe.

Description de l'architecture technique concrète.	☐
Description des mécanismes d'authentification et/ou d'autorisation.	☐
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 de la clé secrète/privée). En principe, le chiffrement devrait être réalisé par l'organe public et celui-ci devrait détenir la clé privée (« Hold Your Own Key»).	☐
Garanties quant aux ressources suffisantes 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).	☐
Indication des objectifs pour garantir la sûreté de l'information et protection des données et les mesures prévues pour les atteindre.	☐
Description des risques, risques résiduels, mesures, back-up concept, résilience, etc. (à présenter en annexe, sous la forme d'un document SIPD par exemple).	☐
S'assurer que les mesures soient adaptées à la nature des données personnelles concernées (art. 21 LPrD pour les données sensibles).	☐
Preuves des éventuelles certifications (ISO, BSI) et autres standards internationalement reconnus. Suivi de	☐

	recommandations/best practices (OWASP top 10, = Open Web Application Security Project, etc.).	

8. Droits des personnes concernées

Droits des personnes concernées.		
	Le sous-traitant doit s'engager à permettre au responsable du traitement de répondre aux demandes formulées par les personnes dont les données sont sous-traitées et à fournir, dans les plus brefs délais, au responsable du traitement 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.	☐

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

Droit de contrôle et d'audit.		
	Le responsable du traitement doit avoir la possibilité de s'assurer que le sous-traitant et ses éventuels sous-traitants, respectent bien le contrat et les obligations de protection des données. Il faut notamment pouvoir accéder à tous les documents permettant de vérifier le respect des obligations (journal d'événements, rapports d'audits, etc.).	☐
	Le sous-traitant doit s'engager à procéder à des contrôles et audits réguliers de son infrastructure, compte tenu des standards internationaux.	☐
	Un droit d'audit par le responsable du traitement et les modalités doivent être également prévues.	☐
	L' Autorité cantonale de la transparence, de la protection des données et de la médiation doit aussi avoir la possibilité d'effectuer des contrôles.	☐

10. Personnel du mandataire et confidentialité

Clause de confidentialité, chartes.		
	Il convient de prévoir contractuellement que le sous-traitant et ses employés soient soumis au secret de fonction. Le sous-traitant devra également s'assurer du respect effectif du secret par ses employés et par ses sous-traitants en cascade.	☐
	Le sous-traitant s'engage à employer dans le cadre du mandat susmentionné uniquement du personnel ayant préalablement signé une charte « 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

11. Responsabilité et indemnisation

Responsabilités et indemnisation.	
Le responsable du traitement demeure responsable de la protection des données personnelles (art. 19 al.1 et art. 37 al. 1 LPrD).	☐
Le sous-traitant est responsable pour les faits des sous-traitants en cascade qu'ils soient autorisés ou non.	☐
Il convient de s'assurer contractuellement que le sous-traitant mette en place les mesures adéquates en lien avec la LPrD pour le traitement des données transmises dans le cadre de la sous-traitance	☐
Une indemnisation pleine et entière pour l'ensemble des dommages directs et indirects subis par le responsable du traitement et causés par le sous-traitant, ses employés ou encore par ses sous-traitants en cascade devrait être prévue.	☐

12. Durée et résiliation du contrat

Durée et résiliation du contrat.	
Prévoir la possibilité de résilier le contrat moyennant le respect d'un préavis (sous réserve de justes motifs justifiant une résiliation avec effet immédiat, comme des problèmes graves de sécurité par exemple).	☐
Prévoir clairement les effets de la résiliation, notamment la restitution des données et leur suppression.	☐
Prévoir la transition vers un autre sous-traitant (rappel de la portabilité des données au sens de l'article 19 LPrD)	☐

13. For et droit applicable

Droit matériel suisse	☐
For exclusif en Suisse, de préférence en romande	☐

14. Annexe(s)

Documents (à joindre si nécessaire dans le cas précis).	Joint
Liste des catégories de données sous-traitées, leur cycle de vie et leur degré de sensibilité.	☐
Documents concernant la SIPD.	☐
Charte destinée au personnel du sous-traitant.	☐
Documents concernant la sous-traitance en cascade.	☐
Documents attestant des mesures techniques et organisationnelles nécessaires.	☐