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

Freiburg, 26. Oktober 2023

Merkblatt Mandat für die Auslagerung der Datenbearbeitung

—

Merkblatt zur Auslagerung der Datenbearbeitung auf Auftragsbasis (Outsourcing), wenn ein öffentliches Organ die Bearbeitung von Personendaten an einen privaten Dritten überträgt,

1. Ziel

Das vorliegende Merkblatt stützt sich auf die Beratungskompetenz der Beauftragten (Art. 54 Abs. 2 Bst. b des Gesetzes vom 12. Oktober 2023 über den Datenschutz des Kantons Freiburg, DSchG; SGF 17.1). Es ist als Leitfaden gedacht mit dem Ziel, die öffentlichen kantonalen oder kommunalen Behörden zu begleiten, wenn sie die Zusammenarbeit mit privaten Personen und Unternehmen für die Bearbeitung ihrer Daten suchen. Diese Zusammenarbeit kann sich auf die technische Seite der Bearbeitung beziehen; sie kann auch die materielle Bearbeitung von Personendaten betreffen, unabhängig davon, ob sie teilweise oder vollumfänglich erfolgt, wie beispielsweise die Sammlung von Daten, deren Beherbergung oder die Bearbeitung an sich. Der Inhalt des Mandats wird durch den Verantwortlichen der Datenbearbeitung definiert / evtl. durch die Parteien und ist auf den Einzelfall anzupassen. Wir weisen ebenfalls auf die Bestimmungen des Reglements vom 29. Juni 1999 über die Sicherheit der Personendaten (DSR; SGF 17.15) hin.

Dieses Merkblatt wird ergänzt durch eine Checkliste für die Vertragsgestaltung sowie eine Charta (siehe Beilagen).

2. Allgemeines

2.1 Die Dienststellen der kantonalen und kommunalen Verwaltung ziehen häufig private Unternehmen oder Personen zur Datenbearbeitung bei. Diese Art der Auslagerung der Bearbeitung von Personendaten im Rahmen eines Auftrags, häufig auch Outsourcing genannt, ist gemäss Gesetzgebung zulässig.

2.2 Das öffentliche Organ, das mit einem Dritten einen Vertrag schliesst, bleibt für den Datenschutz verantwortlich (Art. 19 Abs. 1 und Art. 37 Abs. 1 DSchG). Es behält die Entscheidungsbefugnis über die Daten; ihm obliegt die Rechtmässigkeit der Bearbeitung und es ist verantwortlich dafür, dass die Bearbeitung mit den allgemeinen Grundsätzen des Datenschutzes konform ist. Es muss die Drittperson, die es mit der Bearbeitung beauftragen will, sorgfältig auswählen und dafür sorgen, dass der/die Beauftragte die Anforderungen des Datenschutzes einhält, insbesondere bei besonders schützenswerten Personendaten trifft dies in verstärktem Mass zu.

2.3 Der/die private Beauftragte untersteht grundsätzlich dem Bundesgesetz über den Datenschutz vom 25. September 2020 (Datenschutzgesetz, DSG; SR 235.1) und damit der Aufsicht durch den Eidgenössischen Datenschutzbeauftragten. Damit das öffentliche kantonale oder kommunale Organ, das dem kantonalen Datenschutzgesetz untersteht, eine solche Auslagerung vornehmen kann, muss es die Grundsätze und Anforderungen der Artikel 18 und folgende des kantonalen DSchG beachten.

Aus diesem Grund muss der Vertrag den Mindestanforderungen genügen, wie sie in Artikel 19 Absatz 1 Bst. b DSchG vorgesehen sind. Dies kann in Form eines Zusatzvertrags zum Hauptmandat oder in den Vertrag integriert werden.

3. Vorfragen vor Vertragsschluss und vor Definition des Vertragsinhalts

Aus dem datenschutzrechtlichen Blickwinkel ist es wichtig, die nachfolgenden Fragen vorgängig zu klären:

- Werden Personendaten im Sinne des Datenschutzgesetzes (Art. 4 Abs. 1 Bst. a und e DSchG), unabhängig davon, ob es besonders schützenswerte Daten sind oder nicht (Art. 4 Abs. 1 Bst. c DSchG) durch einen Dritten bearbeitet?
- Ist der Verantwortliche der Bearbeitung bestimmt? Verantwortlicher oder Mitverantwortlicher (Art. 19 Abs. 2 und 4 DSchG)?
- Darf der Verantwortliche die Personendaten, die Gegenstand der Auslagerung der Bearbeitung sind, bearbeiten (Art. 19 Abs. 1 Bst. c DSchG)?
- Existiert bereits ein Vertrag mit dem Auftragnehmer, der präzisiert oder ergänzt werden muss? Sind die Datenschutzklauseln hinreichend?
- Handelt es sich um Daten, die dem Amtsgeheimnis unterstehen? Wenn ja, ist eine spezifische Vertragsklausel vorgesehen?
- Werden die dem Amtsgeheimnis unterliegenden Daten vom Auftragnehmer in der Schweiz bearbeitet/beherbergt? Gibt es eine kaskadenartige Weitervergabe an Subunternehmer/Unter-Auftragsbearbeiter im Ausland?
- Im Fall der Auftragsbearbeitung oder der Unter-Auftragsbearbeitung im Ausland, ist das entsprechende Land auf der Liste der Länder mit einem gleichwertigen Datenschutzniveau geführt (Anhang 1 der DSV = Verordnung über den Datenschutz, Datenschutzverordnung vom 31. August 2022, SR 235.11)?
- Hat der Verantwortliche der Bearbeitung alle wichtigen Aspekte der Auftragsbearbeitung beachtet? (vgl. insbesondere das Merkblatt von Privatim zur Cloud-Technologie)
- Verfügt der Verantwortliche der Datenbearbeitung über eine Risikoanalyse (Konzept ISDS = Informationssicherheit und Datenschutz)?
- Hat der Verantwortliche der Datenbearbeitung eine Kontaktperson Datenschutz/Datenschutzberater/-in («data protection officer», DPO/DPD) bestimmt?

4. Hauptverpflichtungen des Auftraggebers / des Verantwortlichen der Bearbeitung

Für die Durchführung des Mandats muss sich der Auftraggeber insbesondere der folgenden Punkte versichern:

- Gegenstand und Zweck des Auftrags müssen klar definiert sein; sei es, dass der Auftrag auf ein Projekt, eine Angelegenheit oder eine spezifische Aufgabe begrenzt wird;

- Die erwarteten Leistungen, die durch den Auftragnehmer bearbeiteten Daten und die anderen Bedingungen des Auftrags (z.B. Fristen, Fälligkeit, Preis usw.) sind klar zu fixieren;
- Die gute Umsetzung von geeigneten technischen und organisatorischen Massnahmen durch den Auftragnehmer ist sicherzustellen, um die Bedingungen des DSchG sowie des DSR zu erfüllen.

5. Hauptverpflichtungen des Auftragnehmers / Auftragsbearbeiters

Im Rahmen der Mandatsausführung muss der Auftragnehmer insbesondere

- Sämtliche Anforderungen an den Datenschutz gewährleisten, wie es auch der Verantwortliche der Datenbearbeitung tun müsste;
- Sein Personal mit Sorgfalt auswählen;
- Die Auftragserfüllung nur durch Personen ausführen lassen, die sich vorgängig auch verpflichtet haben, die datenschutzrechtlichen Verpflichtungen einzuhalten (siehe Dokument «Charta»);
- Seinem Personal die notwendigen Anweisungen im Hinblick auf die Einhaltung des Datenschutzes zu erteilen;
- Hinreichende Garantien für die notwendigen Ressourcen (technische, organisatorische Ressourcen, Personalressourcen usw.) präsentieren, um die verschiedenen Verpflichtungen einhalten zu können (wie z.B. die Rückgabe der Daten gemäss Art. 19 Abs. 1 Bst. d DSchG);
- Sicherstellen, dass das Personal die Anforderungen des Datenschutzes einhält.

Die genannten Verpflichtungen des Auftragnehmers sind im Vertrag mit diesem klar zu definieren.

Anhang 1

***

Checkliste für die Auslagerung der Bearbeitung von Personendaten

***

Muster zum nicht abschliessenden Inhalt der Bestimmungen zum Datenschutz, die in einen Vertrag über die Auslagerung der Bearbeitung von Personendaten zwischen dem für den Datenschutz verantwortlichen öffentlichen Organ (Auftraggeber) und dem privaten Dritten (Auftragnehmer/Auftragsbearbeiter) aufgenommen werden können (Art. 19 Abs. 1 des Gesetzes vom 12. Oktober 2023 über den Datenschutz [DSchG; SGF 17.1].

1. Beschreibung des Mandats / Bezeichnung der Parteien / andere Elemente des Vertrags

1.1. Ist der Verantwortliche der Datenbearbeitung bestimmt? Der Auftragnehmer ist ebenfalls zu bezeichnen; dieser ist schliesslich gegenüber der Direktion oder dem Verantwortlichen der Datenbearbeitung bei Schlechtausführung des Vertrags verantwortlich.

1.2. Die im Rahmen der Vertragserfüllung erwarteten Leistungen sind zu bezeichnen, wie der Zweck (z.B. Einforderung von ausstehenden Steuern), die Fristen, Fälligkeit, Preis sowie alle anderen Bedingungen des Vertrags.

2. Gegenstand und Zweck der Auslagerung der Bearbeitung / Natur, Finalität und Dauer der Auslagerung (Art. 19 Abs. 1 Bst. b Ziff. 1 DSchG)

2.1. Der Zweck der Bearbeitung erlaubt den Rahmen, zu welchem die Daten dem Auftragnehmer übermittelt werden, zu bestimmen. Der Auftragnehmer kann und darf die Daten nur in diesem Rahmen bearbeiten;

2.2. der erlaubte und der nicht erlaubten Zweck der Bearbeitung ist zu definieren.

3. Bearbeitung der Daten und die betroffenen Datenkategorien (Art. 19 Abs. 1 Bst. b Ziffer 2 DSchG)

3.1. die durch die Auslagerung betroffenen Kategorien von Personendaten sind zu definieren;

3.2. die Liste der im Auftrag bearbeiteten Datenkategorien, ihr Sensibilitätsgrad und der Lebenszyklus der Daten im Detail können Gegenstand eines Vertragsanhangs sein.

4. Pflichten der Parteien (Art. 19 Abs. 1 Bst. b Ziff. 3 DSchG):

4.1. Es ist sicherzustellen, dass der Auftragsbearbeiter (Auftragsnehmer) sich verpflichtet, die Daten gemäss den allgemeinen Datenschutzprinzipien, wie sie im DSchG vorgesehen sind und entsprechend den Weisungen des Verantwortlichen der Datenbearbeitung (Auftraggeber), zu bearbeiten;

4.2. der Auftragsbearbeiter (Auftragnehmer) muss sich verpflichten, die Daten nicht zu einem anderen Zweck zu verwenden als vom Auftraggeber kommuniziert, selbst dann wenn es sich um pseudonymisierte oder anonymisierte Daten handelt;

4.3. es wird empfohlen, eine Informationspflicht für den Fall einer Bekanntgabe von Personendaten (oder eines entsprechenden Risikos) an eine ausländische Behörde (Art. 19 Abs. 1 Bst. b Ziff. 6 DSchG), die Pflicht zur Datenaufbewahrung in der Schweiz oder in einem Staat mit gleichwertigem Datenschutzniveau (Art.18 Abs. 2 DSchG) oder die Pflicht, hinreichende Garantien vorzulegen (geeignete technische und organisatorische Massnahmen, um die massgeblichen gesetzlichen Anforderungen zu erfüllen, hinreichende Mittel, um die Einhaltung der verschiedenen Verpflichtungen, wie die Datenportabilität gemäss Art. 19 Abs. 1 Bst. d DSchG usw. sicherzustellen), vorzusehen;

4.4. es wird empfohlen, Weisungen zur Aufbewahrung, Vernichtung/Löschung und Archivierung von elektronischen Daten wie auch von solchen in Papierform zu erteilen.

5. Kaskadenartige Weitervergabe an Subunternehmer/Unter-Auftragsbearbeiter (Art. 19 Abs. 1 Bst. b Ziff. 5 DSchG)

Die Fragen einer eventuellen weiteren Auftragsbearbeitung sind ebenfalls zu regeln. Es wird empfohlen, die Zulässigkeit oder das Verbot, einen weiteren Subunternehmer mit der Bearbeitung zu beauftragen, wer die Subunternehmer/Unter-Auftragnehmer sind und welche Sicherheitsmassnahmen durch diese umzusetzen sind, ausdrücklich zu regeln. Es ist zu beachten, dass die Unter-Auftragsbearbeitung ohne vorausgehende Zustimmung des Verantwortlichen der Datenbearbeitung ausgeschlossen ist.

6. Sicherheitsmassnahmen (Art. 19 DschG und Reglement vom 29. Juni 1999 über die Sicherheit der Personendaten, DSR; SGF 17.15)

6.1. Der Auftragsbearbeiter ist verpflichtet, alle technischen und organisatorischen Sicherheitsmassnahmen umzusetzen, um die Unversehrbarkeit, die Verfügbarkeit und Vertraulichkeit der Daten zu gewährleisten, und den Verantwortlichen der Bearbeitung (Auftraggeber) sofort über jeden Sicherheitsverstoss, jeden unbewilligten Zugriff und jeden Datenverlust zu informieren;

6.2. diese Massnahmen sind in einem Dokument, das als Anhang beigefügt werden kann, zu beschreiben (wenn nötig). Diese Sicherheitsmassnahmen haben insbesondere folgende Punkte zum Gegenstand:

- Beschreibung der Verschlüsselungsmechanismen ISDS bei betroffenen Daten (sowohl bei Aufbewahrung als auch beim Transport);
- Beschreibung der Mechanismen zur Schlüsselverwaltung (Angaben zur Aufbewahrung, zur Schlüsselhaltung). Es wird empfohlen, dass die Verschlüsselung durch das öffentliche Organ ausgeführt wird und dieses auch den Schlüssel aufbewahrt («Hold Your Own Key»);
- Beschreibung der Risiken, der Restrisiken, Massnahmen, Back-up Konzept, Resilienz usw. (empfohlen als Anhang, z.B. in Form eines ISDS-Dokuments);

> Nachweise von eventuellen Zertifizierungen und anderen erlangten, international anerkannten Standards.

7. Rechte der betroffenen Personen

Der Auftragsbearbeiter (Auftragnehmer) muss sich verpflichten, dem Verantwortlichen der Datenbearbeitung (Auftraggeber) bei Gesuchen von betroffenen Personen innert kürzester Zeit alle Informationen und notwendigen Angaben zu liefern, damit der Verantwortliche die Gesuche zu beantworten kann. Es handelt sich dabei um die Zugangsgesuche zu den eigenen Daten (Auskunftsrecht, Art. 27 ff. DSchG), um das Recht auf Löschung von unerlaubten Daten, auf Berichtigung von Daten usw.

8. Kontrolle, Sanktionen und Aufsicht (Art. 19 Abs. 1 Bst. b Ziff. 4 DSchG)

8.1. Der Verantwortliche der Datenbearbeitung (Auftraggeber) muss sicherstellen, dass der Auftragsbearbeiter (Auftragnehmer) und seine allfälligen Unter-Auftragsbearbeiter (beigezogen mit Zustimmung des Verantwortlichen) den Vertrag und die Verpflichtungen aus Datenschutz einhalten. Der Verantwortliche der Datenbearbeitung muss jederzeit zu allen Dokumenten Zugriff haben müssen, um die Einhaltung der Vertragspflichten zu prüfen (Journal, Auditberichte usw.);

8.2. das Auditrecht des Verantwortlichen der Datenbearbeitung gegenüber dem Auftragsbearbeiter (Auftragnehmer) und seiner eventuellen, nachfolgenden Unter-Auftragsbearbeiter muss vereinbart sein;

8.3. Es ist darauf hinzuweisen, dass die Kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation die Möglichkeit hat, Kontrollen durchzuführen.

9. Personal des Auftragsbearbeiters und Vertraulichkeit

9.1. Der Auftragsbearbeiter (Auftragnehmer) stellt im Rahmen des erwähnten Auftrags nur Personal ein, das vorgängig eine «Verpflichtung für das Personal» unterzeichnet hat, worin sich die Unterzeichnenden verpflichten, die datenschutzrechtlichen Anforderungen zu befolgen und Informationen, die sie bei der Ausübung des Mandats erfahren, geheim zu behalten;

9.2. der Auftragsbearbeiter (Auftragnehmer) verpflichtet sich, die Anforderungen an den Datenschutz einzuhalten wie auch das Amtsgeheimnis durch seine Angestellten und seine nachfolgenden Unter-Auftragsnehmer/Subunternehmer zu wahren (in diesem Zusammenhang sei auf die Kriterien von Auswahl, Weisung und adäquater Überwachung des Personals hingewiesen), und dies auch nach Beendigung des Mandats.

10. Verantwortung und Entschädigung

10.1. Der Verantwortliche der Datenbearbeitung stellt vertraglich sicher, dass der Auftragsbearbeiter (Auftragnehmer) angemessene Massnahmen gemäss DSchG für die im Rahmen der Auftragsbearbeitung übertragene Bearbeitung von Daten trifft;

10.2. der Auftragsbearbeiter (Auftragnehmer) ist verantwortlich für die Handlungen der nachfolgenden Unter-Auftragnehmer/Subunternehmer, unbesehen davon, ob sie bewilligt sind oder nicht. Eine volle Entschädigung für die Gesamtheit des direkten und indirekten Schadens, den der Verantwortliche der Datenbearbeitung (Auftraggeber) erleidet und durch den Auftragnehmer oder seine nachfolgenden Unter-Auftragsbearbeiter/Subunternehmer verursacht worden ist, ist geschuldet.

11. Dauer und Kündigung des Vertrags

11.1. Es ist ein Kündigungsrecht des Verantwortlichen der Datenbearbeitung (Auftraggebers) vorzusehen, mit einer Voranzeige bzw. einer Kündigungsfrist; vorbehalten bleibt die fristlose Kündigung aus wichtigen Gründen (diese sind im Vertrag vorzusehen, wie z.B. bei schwerwiegenden Problemen der Datensicherheit);

11.2. die Rechtsfolgen der Kündigung sollten geregelt werden. Es handelt sich insbesondere um die Pflicht, alle Daten dem Verantwortlichen der Datenbearbeitung innert kurzen Fristen zurückzugeben und sämtliche Kopien dieser Daten zu vernichten;

11.3. es ist ebenfalls hilfreich, die Datenübergabe an einen anderen Auftragsbearbeiter bereits vorzusehen (vgl. die Datenportabilität im Sinne von Art. 19 DSchG).

12. Gerichtsstand und anwendbares Recht

Ist Schweizer Recht anwendbar und ist ein Gerichtsstand in der Schweiz vorgesehen? Es wird dringend empfohlen, über einen Gerichtsstand in der Schweiz zu verfügen.

Anhang 2

***

Charta

***

Muster einer Erklärung «Verpflichtung des Personals» zum Datenschutz für jene Mitarbeitenden, die Zugriff auf Personendaten im Rahmen der Mandatsbearbeitung haben.

1. Die unterzeichnende Person hat aufgrund ihrer Tätigkeit Zugriff auf Personendaten.

2. Die unterzeichnende Person verpflichtet sich, die Datenschutzvorschriften einzuhalten und die Vertraulichkeit von Informationen, von denen sie im Rahmen der Ausübung des Mandats Kenntnis erhält, zu wahren. Sie verpflichtet sich, die Personendaten einzig zum Zweck, der das Mandat vorsieht, zu bearbeiten, diese nicht wieder zu verwenden noch sie weiterzugeben oder sie nur mit Zustimmung des Auftraggebers zu einem anderen Zweck zu verwenden.

3. Die unterzeichnende Person verpflichtet sich, nach Weisung des Auftragnehmers sämtliche notwendigen Massnahmen zu treffen, damit unberechtigte Personen keinen Zugriff auf Personendaten im Rahmen des erwähnten Auftrags haben und dass keine Datenverluste auftreten.

4. Die unterzeichnende Person hat dem Auftragnehmer unaufgefordert alle Probleme, Lücken oder Schwachstellen im Datenschutzbereich, die sie während der Ausübung des Mandats beobachtet, mitzuteilen.

Hiermit bestätige ich, von den obgenannten Pflichten Kenntnis genommen zu haben und verpflichte mich, diese einzuhalten.

Name _____

Funktion _____

Unterschrift _____

Ort und Datum _____