Merkblatt Vereinbarungsinhalt bei der Auftragsdatenbearbeitung

1 Einleitung

Heutzutage erledigt kaum ein Unternehmen sämtliche Aufgaben selbst, sondern lagert einen Teil gegen Entgelt an Drittfirmen aus. Mit dem Outsourcing von Aufgaben ist im Digitalisierungszeitalter regelmässig ein Datentransfer an die Auftragnehmer verbunden. Werden dabei auch personenbezogene Daten an Dritte übermittelt, stellt sich aus datenschutzrechtlicher Sicht die Frage, unter welchen Voraussetzungen die sogenannte Auftragsdatenbearbeitung zulässig ist.

Gemäss dem kantonalen Datenschutzgesetz (sGS 142.1, abgekürzt DSG[1]) ist die Auftragsdatenbearbeitung, die Bearbeitung durch Dritte, zulässig, wenn bestimmte Voraussetzungen erfüllt sind[2]. Ein zentraler Punkt bei der Auswahl des Unternehmens, an das Datenbearbeitungen ausgelagert werden sollen, ist dessen Vertrauenswürdigkeit. Wichtig ist auch zu wissen, dass die Verantwortung beim Organ verbleibt, das die Datenbearbeitung auslagert. Das öffentliche Organ muss für Fehler des Dritten geradestehen, weshalb es ein grosses Interesse haben muss, den Dritten zu grösstmöglicher Sorgfalt zu verpflichten.
In einer schriftlichen Vereinbarung müssen die wesentlichen datenschutzrechtlichen Aspekte geregelt werden. Der Auftragsdatenbearbeiter muss dabei garantieren, geeignete technische und organisatorische Massnahmen implementiert zu haben, so dass die Bearbeitung gesetzeskonform erfolgt und die Rechte der betroffenen Person gewährleistet sind. Der Auftragsdatenbearbeiter darf dabei nur auf Weisung des öffentlichen Organs handeln.

Die Weiterübertragung der Datenbearbeitung vom Dritten an eine weitere Partei bedarf in jedem Fall der vorgängigen schriftlichen Zustimmung des auftraggebenden öffentlichen Organs (Art. 9 Abs. 4 DSG).

Dieses Merkblatt zeigt auf, welche Punkte eine solche Vereinbarung regeln muss. Es lehnt sich an das Merkblatt «Cloud-spezifische Risiken und Massnahmen» von privatim an.[3]

2 Vereinbarungsinhalt

2.1 Vertragsparteien

Weil informations- und datenschutzrechtlich das öffentliche Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgabe bearbeiten lässt, die Verantwortung für die Datenbearbeitung trägt (und nicht einfach «der Kanton St.Gallen»), muss im Vertragstext das verantwortliche (auftraggebende) öffentlichen Organ bezeichnet werden.

2.2 Art und Zweck der Datenbearbeitung (zur Erfüllung der Vertragszwecke)

Der Vertrag legt fest, welche Personendaten zu welchem Zweck (rechtliche Grundlage für das Handeln des öffentlichen Organs) bearbeitet werden. Dabei sind die rechtlichen Grundlagen so präzise wie möglich zu nennen, d.h. mit Angabe eines spezifischen Artikels statt eines pauschalen Verweises auf ein Gesetz.

[1] www.gesetzessammlung.sg.ch/app/de/texts_of_law/142.1
[2] Art. 9 DSG.
[3] https://www.privatim.ch/de/uberarbeitetes-privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen-2/

2.3 Gegenstand und Umfang der Auftragsdatenbearbeitung

Das öffentliche Organ legt fest, welche Aufgaben der Auftragsdatenbearbeiter ausführen darf. Dieser ist daran gebunden und kann nicht einseitig davon abweichen.

2.4 Verantwortlichkeiten (wer ist wofür verantwortlich)

Das öffentliche Organ bleibt für den Umgang mit den Personendaten auch verantwortlich, wenn es die Personendaten durch einen Dritten (die Auftragnehmerin) bearbeiten lässt. Das auftraggebende öffentliche Organ hat dafür zu sorgen, dass die Auftragnehmerin die Personendaten, die sie in seinem Auftrag bearbeitet, nur so bearbeitet, wie es das öffentliche Organ selbst tun dürfte. Die Auftragnehmerin muss vertraglich so eingebunden werden, dass sie mit den Informationen, die sie vom auftraggebenden öffentlichen Organ erhalten hat und/oder im Rahmen des Auftrags bearbeitet, nur macht, was das öffentliche Organ selber auch tun dürfte. Wo die Umschreibung der Pflichten den Vertrag zu umfangreich werden lässt, kann auch auf Zusatzdokumente verwiesen werden.

2.5 Art der Personendaten

Mit dem Auftragsdatenbearbeiter ist eine Auflistung zu vereinbaren, welche Arten von Personendaten an den Auftragsdatenbearbeiter übertragen werden.

2.6 Kategorien möglicher betroffener Personen

In Anlehnung an Ziff. 2.5 wird ausgeführt, wer die Personen(gruppen) sind, von denen die aufgeführten Daten übertragen werden.

2.7 Ort der Datenbearbeitung

Bevorzugt wird eine Bearbeitung im Inland, das heisst, die Rechenzentren stehen in der Schweiz. Ist eine Datenbearbeitung in einem Land mit ungenügendem Datenschutzniveau (bspw. USA) beabsichtigt, muss das öffentliche Organ prüfen, ob das mit Blick auf das Amtsgeheimnis möglich ist und welche zusätzlichen Massnahmen (bspw. Verschlüsselung mit Schlüsselmanagement beim öffentlichen Organ) nötig sind.
Relevant für die Beurteilung des Standorts ist aber auch der Supportzugriff oder der Handhabung der Backups durch den Auftragsdatenbearbeiter. Hier ist darauf zu achten, dass beispielsweise nicht ein Supportzugriff aus den USA auf die Daten im Rechenzentrum in der Schweiz stattfindet. Dies würde eine neue Bewertung und neue Massnahmen betreffend Standort USA benötigen, obwohl das Rechenzentrum auf den ersten Blick die Anforderung als Standort Schweiz erfüllt.

2.8 Pflichten und Rechte des öffentlichen Organs und des Dritten (u.a. Pflicht zur Vertraulichkeit/Verschwiegenheit, Rechenschaft)

Mögliche Vertragspunkte:

- Zuständigkeit und Mitarbeit bei der Wahrung der Rechte Betroffener (Einsichtsgesuche)
- Anforderungen bezüglich Vertraulichkeit, Verfügbarkeit, Integrität (beispielsweise Trennung von Daten verschiedener Kunden)
- Regelung der Zugriffsberechtigungen beim Auftragsdatenbearbeiter
- Regelung der einzusetzenden Verschlüsselung beim Dritten

2.9 Geheimhaltungsverpflichtungen (müssen auch nach Beendigung des Vertragsverhältnisses eingehalten werden)

Es ist festzulegen, welchen Geheimhaltungspflichten der Auftragsdatenbearbeiter unterliegt. Diese sind auf die Zeit nach dem Vertragsverhältnis auszuweiten.

2.10 Beizug von Unterauftragsnehmern

Der Auftragsdatenbearbeiter darf nur weitere (Unter-)Auftragsdatenbearbeiter hinzuziehen, wenn er vorgängig die schriftliche Zustimmung des öffentlichen Organs eingeholt hat. Dies

und die Voraussetzung, dass der Subbearbeiter das gleiche Datenschutzniveau wie der (Haupt)Auftragsbearbeiter zu gewähren hat, ist vertraglich festzuhalten.

2.11 Kontrollrecht des Auftraggebers, Kontrollverfahren des öffentlichen Organs oder beauftragter Kontrollstellen

Der Auftragsdatenbearbeiter ist zu verpflichten, Kontrollen durch das öffentliche Organ nach anerkannten und dem Schutzbedarf entsprechenden Audit-Standards[4] zu akzeptieren.

2.12 Weitere Vertragsausgestaltung

- Bekanntgabe von Informationen an Dritte (zulässig oder nicht und wenn ja, unter welchen Bedingungen)
- Einbezug rechtlicher Veränderungen
- Notfallszenarien (Rückfallebenen, Wiedererstellung, akzeptierte Fristen)
- Meldung von Sicherheitsvorfällen und den dazu getroffenen Massnahmen
- Entwicklung und Wartung der Software (Migrationen, Releasewechsel, Patching)
- Einbezug technischer Entwicklungen (wie erfolgt diese) sowie Wartung von Systemen
- Vertragsdauer und Vertragsanpassungen
- Verhältnis zu andern geltenden Verträgen

2.13 Datenvernichtung und Vertragsauflösung

Das öffentliche Organ darf Daten nur in einem Umfang und einer Dauer bearbeiten, wie es für die Erfüllung der gesetzlichen Aufgabe nötig ist. Sobald der Bearbeitungszweck während der Dauer des Vertrages für gewisse Daten nicht mehr erfüllt ist, sind diese Daten zu vernichten. Eine automatische Vernichtung ist zu bevorzugen. Da die Vernichtung effektiv beim Dritten stattfindet, ist dies vertraglich festzuhalten. Dies umfasst auch allfällige Backups dieser Daten.
Für den Zeitpunkt der Vertragsauflösung ist bereits bei Vertragsabschluss zu regeln, wie der Auftragsdatenbearbeiter mit den Daten umzugehen hat.

2.14 Haftung

Es ist ein Hinweis auf die Strafbestimmung des Datenschutzgesetzes vorzusehen.[5] Für den Fall einer Schlechterfüllung sind die Folgen zu regeln (Sanktionen, mögliche Vertragsauflösung, strafrechtliche Konsequenzen).

2.15 Konventionalstrafe

Zur Stärkung der Vertragsbestimmungen ist für den Fall der Verletzung dieser Bestimmungen eine Konventionalstrafe zu vereinbaren.

2.16 Anwendbares Recht

Das auftraggebende öffentliche Organ muss sicherstellen, dass auf das Vertragsverhältnis schweizerisches Recht anwendbar ist.

2.17 Gerichtsstand

Das auftraggebende öffentliche Organ muss sicherstellen, dass für Streitigkeiten aus diesem Vertrag als Gerichtsstand St.Gallen gilt.

2.18 Zusätzliches

Bei Vereinbarungen zwischen öffentlichen Organen des Kantons St.Gallen nicht zwingend:

- Anwendbares Recht

[4] Beispielsweise ISO 27001.
[5] Art. 40 DSG.

- Gerichtsstand
- Konventionalstrafe

3 Fazit

Grundsätzlich darf die Auslagerung von Datenbearbeitungen für die Grundrechte der betroffenen Personen nicht nachteilig sein. Damit die zusätzlichen Risiken aus der Nutzung von Cloud-Diensten dennoch als tragbar erscheinen können, ist von den öffentlichen Organen im Einzelfall darzulegen, durch welche unverzichtbaren Vorteile des Cloud-Dienstes gegenüber einer gleichwertigen Lösung «on premise» sowie gegenüber risikoärmeren Produkten anderer Anbieter die neuen Risiken aufgewogen werden.
Die öffentlichen Organe, die für ihre Aufgabenerfüllung Cloud-Dienstleistungen in Anspruch nehmen, tragen weiterhin vollumfänglich die Verantwortung für die Datenbearbeitung. Das öffentliche Organ (bzw. seine oberste Leitung) ist angehalten, schriftlich zu bestätigen, dass es die Risiken verstanden hat und das Restrisiko übernimmt.[6]

4 Weitere nützliche Links zur Auftragsdatenbearbeitung

Datenschutzstelle Kanton Basel-Landschaft
www.baselland.ch/politik-und-behorden/besondere-behorden/datenschutz/publikationen/merkblatter-musterschreiben

Datenschutzstelle Kanton Basel-Stadt
www.dsb.bs.ch/handreichungen/leitfaden-auftragsdatenbearbeitung.html

Datenschutzstelle Kanton Zürich
https://datenschutz.ch/datenschutz-in-oeffentlichen-organen/auslagerung

Für Fragen stehen Ihnen die folgenden Stellen gern zur Verfügung:

- Kanton: Kantonale Fachstelle für Datenschutz
  - www.sg.ch/sicherheit/datenschutz.html
  - Tel 058 229 14 14
  - E-Mail: datenschutz@sg.ch
- Gemeinden:www.sg.ch/sicherheit/datenschutz/kontakt-weitere-datenschutzbehoerden/adressen-gemeindefachstellen.html

Oktober 2022

[6] Zitiert aus privatim-Merkblatt, S. 7.