dsb
datenschutzbeauftragte
des kantons zürich

Leitfaden

Leitfaden Bearbeiten im Auftrag

Inhalt

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch, X: @dsb_zh

1 Einleitung

Dieser Leitfaden richtet sich an die öffentlichen Organe des Kantons Zürich, die das Bearbeiten von Informationen Dritten übertragen. Das Gesetz über die Information und den Datenschutz (IDG, LS 170.4) spricht von einem Bearbeiten im Auftrag.

Im Folgenden werden die rechtlichen, organisatorischen und technischen Anforderungen von § 6 IDG und § 25 Verordnung über die Information und den Datenschutz (IDV, LS 170.41) präzisiert und das Vorgehen aufgezeigt. Es wird auf die im Praxiskommentar zum § 6 IDG[1] gemachten Ausführungen und Zitate abgestützt.

Folgende Dokumente stehen zum Thema Bearbeiten im Auftrag zur Verfügung:
- Checkliste Vorgehen (Ziffer 7 dieses Leitfadens)
- Überblick AGB (Anhang 1 dieses Leitfadens)
- Überblick Informationssicherheitsmassnahmen (Anhang 2 dieses Leitfadens)
- Überblick Kriterien für die Vertragsprüfung (Anhang 3 dieses Leitfadens)
- Allgemeine Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen (AGB Auslagerung Informatikleistungen)
- Allgemeine datenschutzrechtliche Geschäftsbedingungen bei der Datenbearbeitung durch Dritte (AGB Datenbearbeitung durch Dritte)
- Datenschutzrechtliche Vertragsbestimmungen
- Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung
- Leitfaden Besondere datenschutzrechtliche Aspekte der Cloud Nutzung unter Berücksichtigung des CLOUD Act
- Leitfaden Nutzung externer Cloud-Dienste
- Muster Geheimhaltungserklärung
- Merkblatt Cloud Computing
- Merkblatt privatim Cloud Computing im Schulbereich
- Merkblatt privatim Cloud-spezifische Risiken und Massnahmen
- Merkblatt Dienste Dritter auf Websites
- Merkblatt Online-Speicherdienste

2 Bearbeiten im Auftrag

2.1 Allgemeines

Ein Bearbeiten im Auftrag im Sinne von § 6 IDG liegt vor, wenn ein öffentliches Organ Informationen, das heisst Sach-, Personen- oder besondere Personendaten durch Private oder andere öffentliche Organe bearbeiten lässt. Man spricht auch von Auslagerung, Outsourcing, Auftragsbearbeitung oder Datenbearbeitung durch Dritte. Unter «Bearbeiten» fällt jeder Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Zugänglichmachen oder Vernichten (§ 3 Abs. 5 IDG).

2.2 Arten des Bearbeiten im Auftrag

Je nach Art der durch den Auftragnehmer zu bearbeitenden Informationen und Inhalt des Auftrags sind drei Arten des Bearbeitens im Auftrag zu unterscheiden:
- Inanspruchnahme von Informatikleistungen
- Datenbearbeitung durch Dritte
- Inanspruchnahme von Dienstleistungen ausserhalb der ersten beiden Kategorien

[1] VERONICA BLATTMANN, § 6 Bearbeiten im Auftrag, in: Bruno Baeriswyl / Beat Rudin, (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich (IDG), Zürich / Basel / Genf 2012.

2.2.1 Inanspruchnahme von Informatikleistungen

Beispiele der Inanspruchnahme von Informatikleistungen sind:
- Betrieb, Wartung der IT-Infrastruktur (Netzwerk, Server, Anwendungen)
- Wartung von Software
- Hosting von Webangeboten und Services (Websites, Analysetools)
- Inanspruchnahme von Cloud Services

Die datenschutzrechtlichen Anforderungen werden in den AGB Auslagerung Informatikleistungen konkretisiert.

Werden Wartungsverträge abgeschlossen, in deren Rahmen der Auftragnehmer keine Daten bei sich bearbeitet und speichert, finden die folgenden Bestimmungen der AGB Auslagerung Informatikleistungen keine Anwendung:
- Ziffer 5: Bekanntgabe von Informationen
- Ziffer 7: Informationszugangsgesuche
- Ziffer 8: Teile der Informationssicherheit wie das Unterhalten eines Sicherheitsmanagements und die Trennung der Informationsbestände (dies bedeutet nicht, dass der Auftragnehmer seine Informationen nicht schützen muss, sondern nur, dass in Bezug auf dieses Auftragsverhältnis diese Anforderungen nicht aufgezeigt werden müssen)
- Ziffer 9: Audit durch Externe und Kontrolle durch den Auftraggeber (da die Daten beim Auftraggeber verbleiben und er direkte Kontrolle über diese innehat)
- Ziffer 13: Cloud Computing
- Ziffer 17: Vertragsauflösung (Übertragung der Daten kommt bei einem Wartungsvertrag ohne Datenhaltung des Auftragnehmers nicht zur Anwendung)

Weitere Informationen
- Leitfaden Nutzung externer Cloud-Dienste
- Merkblatt Cloud Computing
- Merkblatt privatim Cloud Computing im Schulbereich
- Merkblatt privatim Cloud-spezifische Risiken und Massnahmen
- Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung
- Leitfaden Besondere datenschutzrechtliche Aspekte der Cloud Nutzung unter Berücksichtigung des CLOUD Act

2.2.2 Datenbearbeitung durch Dritte

Beispiele, bei denen das Bearbeiten von Informationen durch Auftragnehmer in dem Sinne im Zentrum steht, dass «ein Produkt» aus Informationen des öffentlichen Organs für das öffentliche Organ entsteht, sind:
- Auftrag einer Gemeinde an einen Berater zwecks Formulierung eines Beschlusses
- Auftrag zur Durchführung von Bildungsprogrammen
- Auslagerung des Inkassos ausstehender Rechnungen
  Beratungen im Sinn von Stellungnahmen

Die datenschutzrechtlichen Anforderungen werden in den AGB Datenbearbeitung durch Dritte konkretisiert.

2.2.3 Inanspruchnahme von Dienstleistungen

Beispiele der Inanspruchnahme von Dienstleistungen, die nicht ohne Informationen des öffentlichen Organs erbracht werden können, deren Hauptinhalt jedoch Eigenleistungen des Auftragnehmers sind und in deren Rahmen das Bearbeiten der Informationen des öffentlichen Organs nicht Schwerpunkt ist, sind

- Coaching
- Wartung von Geräten
- Druck und Versand von Steuerrechnungen
- Durchführung von Workshops und Weiterbildungen
- Beratungen allgemeiner Art

Der Vertragsinhalt richtet sich nach der Sensitivität und dem Schutzbedarf der Informationen und muss im Einzelfall bestimmt werden. Musterformulierungen finden sich in den datenschutzrechtlichen Vertragsbestimmungen.

3 Abgrenzung zum Bearbeiten im Auftrag

3.1 Selbstständige Aufgabenerfüllung

Kein Bearbeiten im Auftrag im Sinne von § 6 IDG ist, wenn Organisationen und Personen des öffentlichen und privaten Rechts selbstständig öffentliche Aufgaben erfüllen, weil sie damit betraut wurden (§ 3 Abs. 1 lit. c IDG). Beispiele:

- Spitäler mit kantonalen Leistungsaufträgen gemäss Spitalliste
- Selbstständige öffentlich-rechtliche Anstalten des Kantons, beispielsweise das Universitätsspital
- Private Beratungsstellen gemäss § 13 lit. c Sozialhilfegesetz (LS 851.1)

3.2 Bearbeiten von Personendaten innerhalb einer Verwaltungseinheit

Das Bearbeiten von Personendaten innerhalb einer im Anhang 2 VOG RR (LS 172.11) definierten Verwaltungseinheit fällt nicht unter die Voraussetzungen von § 6 IDG. Diese Verwaltungseinheiten erfüllen als Ganzes eine gesetzliche Aufgabe und unterstehen demselben Weisungs- und Aufsichtsrecht. Das Abschliessen eines Vertrags erübrigt sich.

4 Gesetzliche Grundlagen und Voraussetzungen

4.1 Gesetzliche Grundlagen

Für das Bearbeiten im Auftrag gelten folgende gesetzliche Grundlagen:

- IDG (LS 170.4)
- IDV (LS 170.41)
- Gesetz über die Auslagerung von Informatikleistungen (LS 172.71)
- Verordnung über die Informationsverwaltung und -sicherheit (LS 170.8)

Für die kantonale Verwaltung gelten auch die Allgemeine Informationssicherheitsrichtlinie des Regierungsrates (AISR) und die Besonderen Informationssicherheitsrichtlinien (BISR). Letztere sind im Intranet der kantonalen Verwaltung unter dem Amt für Informatik abrufbar. Sie legen die Schlüsselanforderungen für die massgeblichen Informationssicherheitsbereiche fest.

4.2 Kein Entgegenstehen rechtlicher Bestimmungen

Dem Bearbeiten im Auftrag dürfen keine rechtlichen Bestimmungen entgegenstehen. Zu denken ist vorab an Geheimnispflichten wie das Amts- oder Berufsgeheimnis. Werden die Informationen verschlüsselt und verbleibt das Schlüsselmanagement beim Auftraggeber, kann auch bei umfassenden Geheimnispflichten ausgelagert werden.

Amtsgeheimnis (Art. 320 StGB)

Das Amtsgeheimnis steht einer Auslagerung grundsätzlich nicht entgegen. Wichtig ist, dass die Schweigepflicht vertraglich festgehalten wird.

– Dennoch müssen verschiedene Faktoren wie die Art der von der Auslagerung betroffenen Daten (Personendaten oder besondere Personendaten) sowie das Datenschutzniveau des Landes berücksichtigt werden, in das ausgelagert werden soll. Allenfalls sind besondere vertragliche und/oder technische Sicherheitsvorkehrungen umzusetzen. Siehe Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung und Leitfaden Besondere datenschutzrechtliche Aspekte der Cloud Nutzung.

Berufsgeheimnis (Art. 321 StGB)

Ob das Berufsgeheimnis auch für Auftragnehmer gilt, ist umstritten. Deshalb sind bei solchen Bearbeitungen im Auftrag spezifische Massnahmen zum Schutz der Daten umzusetzen. Vorbehalten bleiben Datenbearbeitungen durch Dritte, bei denen die Kenntnisnahme der Informationen für die Leistungserbringung durch den Berufsgeheimnisträger unabdingbar ist. Dies kann beispielsweise bei der Wartung von medizinischen Geräten der Fall sein.

Ansonsten sind folgende Varianten möglich:

– Die Daten werden verschlüsselt. Siehe Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung.
– Es werden vertragliche Massnahmen umgesetzt. Siehe dazu die Einschränkungen im Leitfaden Besondere datenschutzrechtliche Aspekte der Cloud Nutzung unter Berücksichtigung des CLOUD Act.
– Die datenbearbeitenden Personen werden in die funktionale Hierarchie des Auftraggebers eingebunden, wie dies § 3 Abs. 1 Gesetz über die Auslagerung von Informatikleistungen für die kantonale Verwaltung festhält. Dazu werden Mitarbeitende des Auftragnehmers explizit für die konkrete Datenbearbeitung bestimmt, dem Kontroll- und Weisungsrecht des Auftraggebers unterstellt und durch eine Geheimhaltungserklärung an das Amts- und/oder Berufsgeheimnis gebunden. Musterformulierung für den Vertrag: Die Mitarbeitenden des Auftragsnehmers (Namen) unterstehen dem Weisungsrecht des öffentlichen Organs (Name). Sie unterstehen dem Berufsgeheimnis (Art. 321 StGB).

Andere Geheimnispflichten

Es gibt eine Vielzahl von weiteren gesetzlich verankerten Schweigepflichten:
§ 8 GG (LS 131.1), § 120 StG (LS 631.1), § 47 SHG, Art. 11 OHG (SR 312.5), Art. 73 StPO (SR 312). Es ist im Einzelfall zu beurteilen, ob die Schweigepflicht einer Auslagerung entgegensteht.

Andere rechtliche Bestimmungen

Gewisse Aufgaben können nicht ausgelagert werden, beispielsweise die Vornahme von Zwangsmassnahmen durch die Polizei.

4.3 Kein Entgegenstehen vertraglicher Vereinbarungen

Vertragliche Vereinbarungen können einem Bearbeiten im Auftrag entgegenstehen oder dieses nur unter bestimmten Auflagen zulassen. Beispielsweise dürfen Subauftragnehmer bei Einbezug der AGB Auslagerung Informatikleistungen nach Abschluss des Vertrags nur mit schriftlicher Zustimmung des öffentlichen Organs beauftragt werden.

4.4 Verantwortlichkeit

Das öffentliche Organ bleibt für ausgelagerte Datenbearbeitungen verantwortlich, auch wenn das Bearbeiten im Ausland stattfindet, beispielsweise bei der Inanspruchnahme von Cloud Services (§ 6 Abs. 2 IDG). Es muss in der Lage sein, die Pflichten zum Schutz der Informationen wahrzunehmen. Eine sorgfältige Auswahl ist deshalb unabdingbar. Eine Zertifizierung nach anerkannten Standards und die dieser zugrunde liegende Qualitätssicherung sowie Auditberichte können beispielsweise bei der Auswahl behilflich sein. Im Rahmen einer sorgfältigen Risikoanalyse muss das öffentliche Organ unter Berücksichtigung aller relevanten Fakten wie Art der Daten, Ort der Datenbearbeitung, Datenschutzniveau des Auftragnehmers, Unterauftragsverhältnisse, durch den Auftraggeber umgesetzte Informationssicherheitsmassnahmen, anwendbares Recht und Gerichtsstand entscheiden, ob eine Auslagerung vertretbar ist.

Für den Auftragnehmer bedeutet dies insbesondere, dass er die Informationen nur so wie das öffentliche Organ bearbeiten darf und dass er dieselben Sicherheitsanforderungen in Bezug auf die Gewährleistung von Vertraulichkeit, Verfügbarkeit und Integrität erfüllen muss.

4.5 Schriftlicher Vertrag

Verträge müssen schriftlich abgeschlossen werden, es sei denn, das Bearbeiten im Auftrag ist gesetzlich geregelt (§ 25 Abs. 1 IDV). Sind vom Bearbeiten im Auftrag besondere Personendaten betroffen, muss der Auftrag durch die vorgesetzte Stelle genehmigt werden (§ 25 Abs. 3 IDV). Dem Bearbeiten im Auftrag unter Inanspruchnahme von Informatiksystemen und -anwendungen mit strategischer Bedeutung für die kantonale Verwaltung muss der Regierungsrat zustimmen (§ 1 Abs. 2 Gesetz über die Auslagerung von Informatikdienstleistungen (LS 172.71).

5 Bearbeiten im Auftrag im Ausland

Wenn das Bearbeiten im Auftrag im Ausland stattfindet, nehmen die Risiken für das öffentliche Organ und für die von der Datenbearbeitung betroffenen Personen zu. Ausländische rechtliche Bestimmungen können die Bekanntgabe der Informationen erzwingen oder den Rechtsschutz vereiteln. Diese Risiken müssen durch zusätzliche Massnahmen analog derjenigen in § 19 IDG und § 22 IDV minimiert werden.

Ein dem schweizerischen Datenschutz angemessenes Schutzniveau wird denjenigen Staaten attestiert, welche das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Europaratskonvention 108, SR 0.235.1) unterzeichnet und ratifiziert haben. Eine Liste dieser Staaten findet sich beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten. In diesen Fällen müssen keine zusätzlichen Informationssicherheitsmassnahmen implementiert werden.

Je nach Land können auch andere Mechanismen greifen. Im Nachgang zum Urteil des Europäischen Gerichtshofes im Fall Schrems[2] hat der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte die im Juni 2021 in Kraft getretenen Standardvertragsklauseln der EU anerkannt. Das Vorgehen beim Abschluss der Standardvertragsklauseln bei der Übermittlung von Daten in Länder mit nicht angemessenem Datenschutzniveau ist wie folgt[3]

- Auswahl der Module
- Abänderungen gemäss Vorgabe des EDÖB
  - Anhang I C
    Aufführen der Datenschutzbeauftragten des Kantons Zürich als zuständige Aufsichtsbehörde
  - Klausel 17
    Festhalten des anwendbaren schweizerischen Rechts für vertragliche Ansprüche

[2] EuGH, C-311/18, Urteil vom 16. Juli 2020 - «Schrems II».

[3] Siehe Dokument des EDÖB «Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf anerkannte Standardvertragsklauseln und Musterverträge» vom 27. August 2021

- Klausel 18b
  Festhalten eines schweizerischen Gerichtsstands
- Klausel 18c
  Anpassungen in einem Anhang betreffend Gerichtsstand für Klagen von betroffenen Personen in dem Sinne, dass der Begriff Mitgliedstaat nicht so verstanden werden darf, dass betroffene Personen ihre Rechte in der Schweiz nicht einklagen könnten.
  Anpassungen in einem Anhang, dass Verweise auf die DSGVO als Verweise auf schweizerisches Datenschutzrecht zu verstehen sind

Bei besonderen Personendaten oder anderen sensitiven Informationen sollte ein Bearbeiten im Ausland aufgrund der hohen Risiken unterlassen werden. Wenn auf gewisse Dienste nicht verzichtet werden kann, sind europäische Länder zu bevorzugen und die Informationen durch spezielle Massnahmen[4] zu schützen. Dazu gehören beispielsweise

- die Verschlüsselung, wobei der Schlüssel beim öffentlichen Organ liegt (Hold Your Own Key)
- Pseudonymisierung der Personendaten
- die Nutzung einer hybriden Cloud, also einer Mischung aus einer lokalen und einer öffentlichen Cloud, insbesondere bei Daten, die unter speziellen Geheimnispflichten stehen (medizinische Daten, Steuerdaten, Daten aus dem Sozialhilfebereich)
- Implementierung einer treuhänderischen Cloud
- eine vertragliche Vereinbarung, dass Zugriffe nur mit Einwilligung des öffentlichen Organs erfolgen

Siehe Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung
Siehe Leitfaden Besondere datenschutzrechtliche Aspekte der Cloud Nutzung unter Berücksichtigung des CLOUD Act

6 Vorgehen

Fünf Schritte zu einem datenschutzkonformen Bearbeiten im Auftrag:

1. Prüfen, ob rechtliche oder vertragliche Bestimmungen entgegenstehen
2. Prüfen, ob die Sensitivität der Informationen der Auslagerung entgegensteht
3. Auswahl des Auftragnehmers
4. Vertragsgestaltung oder Prüfung der Nutzungsbedingungen / AGB
5. Umsetzung der Massnahmen

Siehe Leitfaden Nutzung externer Cloud-Dienste

6.1 Prüfen, ob rechtliche oder vertragliche Bestimmungen entgegenstehen

Die auszulagernden Informationen sind auf Geheimhaltungspflichten zu überprüfen. Es ist zu entscheiden, ob diese einem Bearbeiten im Auftrag entgegenstehen. Allenfalls sind geeignete Massnahmen wie die Verschlüsselung umzusetzen.

Weiter sind andere rechtliche oder vertragliche Vorbehalte in Bezug auf ein Bearbeiten im Auftrag zu berücksichtigen.

Wenn die Daten im Ausland bearbeitet werden, ist zu prüfen, ob die Verantwortung noch wahrgenommen respektive die Kontrolle noch ausgeübt werden kann. Es ist zu prüfen, ob der entsprechende Staat über ein der Schweiz gleichwertiges Datenschutzniveau verfügt oder ob zusätzliche Massnahmen umgesetzt werden müssen.

[4] Siehe dazu auch die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses.

6.2 Prüfen, ob die Sensitivität der Daten dem Bearbeiten im Auftrag entgegensteht

Das öffentliche Organ muss die Risiken in Bezug auf die Vertraulichkeit, Verfügbarkeit und Integrität analysieren, die Informationen einer Schutzstufe zuordnen und die Informationssicherheitsmassnahmen definieren. Die Informationen dürfen nicht unberechtigten Dritten zugänglich sein, verloren gehen und unbefugt abgeändert werden können. Aus diesen Beurteilungen resultieren die Massnahmen und somit die Anforderungen an den Auftragnehmer.

Grundsätzlich gilt für die Anforderungen die Kaskade Sachdaten, Personendaten, besondere Personendaten. Je sensitiver die Informationen, desto umfangreicher sind die rechtlichen, organisatorischen und technischen Anforderungen, die das öffentliche Organ und somit auch der Auftragnehmer zu erfüllen haben.

6.3 Auswahl des Auftragnehmers

Stehen dem Bearbeiten im Auftrag keine Geheimhaltungspflichten entgegen, ist der Schutzbedarf bestimmt und sind die Massnahmen definiert, kann ein Auftragnehmer ausgewählt werden. Das öffentliche Organ ist verpflichtet, die analog Art. 55 OR auferlegten Sorgfaltspflichten zu treffen. Zertifizierungen nach anerkannten Datenschutz- und Informationssicherheitsstandards oder Kontrollberichte von unabhängigen Dritten können bei der Auswahl behilflich sein.

6.4 Vertragsgestaltung oder Prüfung der Nutzungsbedingungen / AGB

Die Verträge für ein Bearbeiten im Auftrag müssen:

- schriftlich abgeschlossen werden (§ 25 Abs. 1 IDV). Das Akzeptieren der AGB genügt, sofern sie die datenschutzrechtlichen Anforderungen erfüllen und nicht einseitig abgeändert werden können.
- durch die vorgesetzte Stelle genehmigt werden, falls besondere Personendaten betroffen sind (§ 25 Abs. 3 IDV)
- vom Regierungsrat bewilligt werden, falls Informatiksysteme und Anwendungen mit strategischer Bedeutung für die kantonale Verwaltung betroffen sind (§ 1 Abs. 2 Gesetz über die Auslagerung von Informatikdienstleistungen)

Der Inhalt eines Vertrags respektive der AGB umfassen insbesondere (siehe auch Anhang 3):

- Gegenstand und Umfang der Datenbearbeitung
- Verantwortung (wer ist wofür verantwortlich)
- Verfügungsmacht (muss beim öffentlichen Organ liegen)
- Zweckbindung (Daten dürfen nur für Vertragszwecke bearbeitet werden)
- Bekanntgabe von Informationen
- Geheimhaltungsverpflichtungen
- Rechte Betroffener (Auskunft)
- Informationssicherheitsmassnahmen
- Kontrollmöglichkeit des öffentlichen Organs oder externer Prüfstellen
- Unterauftragsverhältnisse (Offenlegung, Änderung nur mit Bewilligung oder mindestens einer Information auf der Website oder per E-Mail oder anderweitige Ankündigung mit möglicher Vertragsbeendigung)
- Entwicklung und Wartung
- Orte der Datenbearbeitung (Schweiz oder bei Bearbeiten im Ausland gleichwertiges Datenschutzniveau oder zusätzliche Massnahmen)
- Cloud Computing (den zusätzlichen Risiken angepasste Massnahmen)
- Geschäftsgeheimnis
- Werbung
- Sanktionen
- Vertragsdauer und Voraussetzungen der Vertragsauflösung
- Löschung nach Vertragsauflösung

- Datenportabilität
- Haftung
- Verhältnis zu anderen geltenden AGB
- Anwendbares Recht (schweizerisches Recht)
- Gerichtsstand (schweizerischer Gerichtsstand)

6.5 Umsetzung der Massnahmen

Die Umsetzung der im Vertrag festgehaltenen Massnahmen muss durch das öffentliche Organ periodisch kontrolliert werden. Bei grossen Anbietern wird dies in der Regel nicht möglich sein. In diesen Fällen können Auditberichte von unabhängigen Prüfstellen in Anspruch genommen werden.

7 Checkliste Vorgehen

1. Bestimmen der Art und des Umfangs der auszulagernden Datenbearbeitung
   - Art der Informationen (Sachdaten, Personendaten, besondere Personendaten)
   - Art des Bearbeitens im Auftrag (Informatikleistung, Datenbearbeitung durch Dritte, Inanspruchnahme anderer Dienstleistungen)
   - Umfang

2. Prüfen, ob rechtliche Bestimmungen dem Bearbeiten im Auftrag entgegenstehen
   - Amtsgeheimnis
   - Berufsgeheimnis
   - Andere Geheimnispflichten
   - Andere rechtliche Bestimmungen
   - Auslagerung ins Ausland: angemessenes Datenschutzniveau
     → Eventuell Massnahmen bestimmen / auf das Bearbeiten im Auftrag verzichten

3. Prüfen, ob vertragliche Bestimmungen dem Bearbeiten im Auftrag entgegenstehen
   - Eventuell Massnahmen bestimmen / auf das Bearbeiten im Auftrag verzichten

4. Bestimmung des Schutzbedarfs und der Massnahmen
   - Siehe Übersicht Anhang 2
   - Siehe Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung
   - Siehe Leitfaden Besondere datenschutzrechtliche Aspekte der Cloud Nutzung unter Berücksichtigung des CLOUD Act

5. Bestimmen des Vertragsinhalts
   - Siehe Übersicht Anhang 1

6. Auswahl der AGB
   - Informatikleistung: AGB Auslagerung Informatikleistungen
   - Datenbearbeitung durch Dritte: AGB Datenbearbeitung durch Dritte

7. Auswahl des Auftragnehmers und/oder des Produkts

8. Vertragsabschluss
   - Informatikleistung: Vertrag aushandeln, AGB ist integraler Bestandteil
   - Datenbearbeitung: Vertrag aushandeln, AGB ist integraler Bestandteil
   - Andere Dienstleistung: individuellen Vertrag aushandeln
   - Vom Auftragnehmer vorgelegte AGB: auf Inhalt anhand Anhang 1 überprüfen

9. Bearbeiten im Auftrag mit besonderen Personendaten
   - Vertrag durch vorgesetzte Stelle genehmigen

10. Bearbeiten im Auftrag mit strategischer Bedeutung für die kantonale Verwaltung
    - Zustimmung des Regierungsrats einholen

11. Umsetzung der Massnahmen periodisch kontrollieren, kontrollieren lassen, Audit-Bericht einsehen

8 Anhang 1 – Überblick AGB

Inhalt Vertrag	AGB Auslagerung Informatik-leistungen	AGB Daten-bearbeitung durch Dritte	Datenschutz-relevante Vertrags-bestimmungen*	Im Vertrag regeln / präzisieren Siehe Anhang 3
Gegenstand und Umfang der Datenbearbeitung				✓
Umgang mit Personendaten – Verantwortung – Verfügungsmacht – Zweckbindung – Bekanntgabe von Informationen	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓	✓	
Geheimhaltungsverpflichtungen – Amtsgeheimnis – andere Geheimnispflichten	✓	✓	✓	 ✓
Rechte Betroffener	✓			
Informationssicherheitsmassnahmen	✓	✓	✓	✓
Kontrolle der Auftragserfüllung	✓	✓		
Unterauftragsverhältnisse	✓	✓		
Entwicklung und Wartung	✓			
Ort der Datenbearbeitung – Schweiz – Ausland / angemessenes Datenschutzniveau – Ausland / kein angemessenes Datenschutzniveau	✓ ✓			 ✓ ✓
Cloud Computing	✓			✓
Geschäftsgeheimnisse	✓	✓		
Werbung	✓	✓	✓	
Sanktionen	✓	✓	✓	✓
Vertragsdauer und Voraussetzung Vertragsauflösung	✓	✓	✓	✓
Haftung				✓
Verhältnis zu anderen AGB				✓
Anwendbares Recht	✓	✓	✓	
Gerichtsstand	✓	✓	✓	

*Musterformulierungen betreffend Vertragsinhalt bei individueller Gestaltung

9 Anhang 2 – Überblick Informationssicherheitsmassnahmen

A	– Verschlüsselung des Transportwegs – Authentisierung mittels Benutzer-ID und Passwort – Gewährleistung der Passwort-Sicherheit – Verhinderung der Top-Risiken (OWASP) im Web – Protokollierung der Datenänderungen – Umsetzungsplanung gemäss ISO 27002 – Notfallplanung – Back-up-Konzepte – Kontrolle des IT-Betriebs – Informationspflicht Auftraggeber (Schutzbedarf, Aufbewahrungsfristen) – Informationspflicht Auftragnehmer (Methoden, Prozesse, Unterauftragnehmer, besondere Vorkommnisse) – Mandantentrennung – Patch-Management
B	– Portabilität
C	– Verschlüsselung der Datenablage, Key-Management beim Auftraggeber – Zwei-Faktor-Authentisierung
D	– Managementsystem für Informationssicherheit (ISMS) ISO 27001 / BSI 200–1 – Vollständige Protokollierung – Regelmässige Überprüfung der Anwendungen auf Schwachstellen

	Personendaten[1]	**Besondere Personendaten**
Auslagerung CH	A	A C D
Cloud CH	A B	A B C D
Auslagerung Ausland Cloud Ausland Angemessener Datenschutz[2]	A B	A B C D
Auslagerung Ausland Cloud Ausland[3] Kein angemessener Datenschutz	A B C	A B C D

[1] Sachdaten: der Schutzbedarf der Informationen und die daraus resultierenden organisatorischen und technischen Massnahmen werden im Einzelfall ermittelt.

[2] Liste der Staaten mit angemessenem Datenschutzniveau

[3] Für Cloud Computing gilt zusätzlich der Leitfaden Besondere datenschutzrechtliche Aspekte der Cloud Nutzung unter Berücksichtigung des CLOUD Act

10 Anhang 3 – Überblick Kriterien für die Vertragsprüfung

Prüfung rechtlicher Aspekte

Kriterium	Bemerkung	Fundstelle
Gegenstand und Umfang der Datenbearbeitung / Personendaten / bes. Personendaten[1]		
Umgang mit Personendaten – Verantwortung – Verfügungsmacht – Zweckbindung – Bekanntgabe von Informationen – Meldepflicht bei Vorfällen		
Geheimhaltungsverpflichtungen – Amtsgeheimnis – andere Geheimnispflichten		
Rechte Betroffener		
Kontrolle der Auftragserfüllung		
Unterauftragsverhältnisse		
Entwicklung und Wartung		
Ort der Datenbearbeitung – Schweiz – Ausland / angemess. DS-Niveau – Ausland / kein angemessenes Datenschutzniveau		
Datenregion wählbar		
Cloud Computing / lokal einsetzbar		
Geschäftsgeheimnisse		
Werbung		
Sanktionen		
Vertragsdauer und Voraussetzungen Vertragsauflösung		
Löschung nach Vertragsauflösung		
Datenportabilität		
Haftung		
Verhältnis zu anderen AGB / Abänderbarkeit		

[1] Die mit grau hinterlegten Kriterien dienen einer Ersteinschätzung, ob eine datenschutzkonforme Nutzung überhaupt möglich ist.

Kriterium	Bemerkung	Fundstelle
Anwendbares Recht		
Gerichtsstand		
DSGVO-konform		
CLOUD Act anwendbar		

Prüfung organisatorisch-technischer Aspekte

Kriterium	Bemerkung	Beurteilung
Server-/Datenstandort		
Verschlüsselter Transport (TLS, https)		
Verschlüsselte Datenablage		
Schlüsselmanagement		
E2EE[1]Nachrichten		
E2EE Audio / Video		
Anonyme Nutzung		
Zwei-Faktoren-Authentifizierung möglich (für Admin / für Benutzende)		
Tracking Tools oder Cookies		
Registration notwendig		
E-Mail-Adresse muss neu eröffnet werden		
Quellcode verfügbar		
Zertifizierung der Lösung oder des Anbieters		
Wird regelmässigen Audits unterzogen		
Audit-Berichte einsehbar		
Komplexe Passwortanforderungen		
Zugriffmanagement (IAM)		
Regelmässige Datensicherung (Backup)		
Hohe Verfügbarkeit gewährleistet		
Datenschutzeinstellungen steuerbar		
Mandantentrennung		
Datenportabilität gegeben		

Kriterium	Bemerkung	Beurteilung
Verhinderung der Top-Risiken (OWASP) im Web		
Weitere		

V 1.14 / Oktober 2024