Merkblatt «Datenbearbeitung im Auftrag» i.S.v. § 7 IDG

1. Gesetzliche Grundlage

Nach § 7 Abs. 1 Gesetz über die Informationen und den Datenschutz (Informations- und Datenschutzgesetz, IDG, SGS 162) kann ein öffentliches Organ das Bearbeiten von Informationen einer Auftragsdatenbearbeiterin oder einem Auftragsdatenbearbeiter übertragen.

Dies ist aber nur möglich, wenn dem keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht (§ 7 Abs. 1 Bst. a IDG). Ausserdem muss sichergestellt werden, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte (§ 7 Abs. 1 Bst. b IDG).

Das öffentliche Organ bleibt für den Umgang mit Informationen nach dem IDG verantwortlich (§ 7 Abs. 2 IDG).

2. Begriff «Datenbearbeitung im Auftrag»

Von einer Auftragsdatenbearbeitung wird allgemein gesprochen, wenn ein (kantonales oder kommunales) öffentliches Organ (Auftraggeber) Informationen zur Erfüllung seiner gesetzlichen Aufgabe ausserhalb der öffentlichen Organisation durch externe Dritte (Auftragnehmer) bearbeiten lässt. Im Zusammenhang mit der Auftragsdatenbearbeitung werden oftmals synonym die Begriffe «Auslagerung der Datenbearbeitung», «Outsourcing» oder «Auftragsbearbeitung» verwendet.

Das Bearbeiten umfasst begrifflich jeden Umgang mit Informationen wie das Beschaffen, Aufbewahren, Lesen, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten sowie Durchführen logischer und/oder rechnerischer Operationen mit diesen Informationen (§ 3 Abs. 5 IDG).

So können beispielsweise private (IT-)Firmen mit der Unterstützung bei der Geschäftsverwaltung durch eine kantonale oder kommunale Behörde beauftragt werden. Beispiele dafür sind der Beizug eines privaten Unternehmens zum Druck und Versand von Rechnungen, zum Betrieb und zur Wartung der Infrastruktur, zum Webhosting oder auch für Support.

> Abgrenzung: Die Übertragung bzw. Auslagerung oder Ausgliederung einer öffentlichen Aufgabe unterscheidet sich von einer Auftragsdatenbearbeitung. Hier wird eine bestimmte öffentliche Aufgabe, die ein öffentliches Organ (Auftraggeber) im Rahmen einer gesetzlichen Bestimmung wahrnimmt, auf externe private Dritte übertragen. Die extern beauftragten privaten Dritten erfüllen dabei die übertragene öffentliche Aufgabe in eigener Verantwortung. Beispiele für diesen Bereich sind Privatspitäler mit kantonalen Leistungsaufträgen oder private Institutionen wie Spitex oder Sonderschulen, die mit öffentlichen Aufgaben betraut sind. Im Rahmen dieser selbstständigen Aufgabenwahrnehmung werden sie selber zu einem öffentlichen Organ im Sinne von § 3 Abs. 1 Bst. c IDG und das IDG findet somit direkt Anwendung auf den beauftragten privaten Dritten. Die Vorgaben des kantonalen Gesetzes hinsichtlich der Datenbearbeitung und der Informationssicherheit sind bei der Erfüllung der Aufgabe zu beachten. Ebenso gilt die auf dem IDG basierende Informations- und Datenschutzverordnung (IDV, SGS 162.11).

3. Anwendbarkeit des IDG auf die Datenbearbeitung im Auftrag

Die durch die Auftragsdatenbearbeitung ausgelagerten Informationen können zu schützende Sach-, Personen- und/oder besondere Personendaten enthalten.

Zu beachten ist, dass die beauftragten Dritten im Rahmen der Auftragsdatenbearbeitung keine öffentlichen (gesetzlichen) Aufgaben selbstständig bzw. eigenverantwortlich erfüllen. Vielmehr bleibt das beauftragende öffentliche Organ weiterhin für den Umgang mit den ausgelagerten Informationen verantwortlich (§ 7 Abs. 2 IDG). Das IDG findet demzufolge nicht direkt Anwendung auf die

beauftragten Dritten, sondern auf dessen Datenbearbeitung. Dem beauftragenden öffentlichen Organ folgt aus der eigenen Verantwortlichkeit die Pflicht zur Sicherstellung der Einhaltung des kantonalen Datenschutzgesetzes durch den Dritten (§ 7 Abs. 1 Bst. b IDG).

4. Konkrete Massnahmen zur Sicherstellung datenschutzrechtlicher Anforderungen

Die rechtlichen, organisatorischen und technischen Anforderungen, die sich aus dem IDG ergeben, müssen im Vorfeld der Auftragsdatenbearbeitung vom potentiellen Auftragnehmer dem öffentlichen Auftraggeber ausgewiesen werden können. Das öffentliche Organ als Auftraggeber hat darauf die Offerten und Risiken[1], die mit der jeweiligen Auslagerung einher gehen, zu prüfen. Die Elemente der Anforderungen an den Datenschutz und die Informationssicherheit müssen in einem Vertrag mit dem Auftragnehmer schriftlich festgelegt und die Vertragseinhaltung auf geeignete Weise sichergestellt sein – beispielsweise durch die Festsetzung einer Konventionalstrafe. Der Auftragnehmer muss sorgfältig ausgewählt und instruiert und im Verlauf des Auftrags auf Einhaltung der Anforderungen überprüft werden. Können die Anforderungen durch die Auftragnehmerin nicht eingehalten werden oder resultiert ein zu hohes Restrisiko, muss ein Verzicht in Betracht gezogen werden.

Hat die Auslagerung aufgrund der Art (beispielsweis durch den allfälligen Kontrollverlust bei Cloud-Diensten) zur Folge, dass das verbleibende Restrisiko zwar noch tragbar, aber höher gegenüber einer gleichwertigen Lösung «on premise» oder gegenüber risikoärmeren Lösungen anderer Anbieter ist, so ist vom öffentlichen Organ im Einzelfall darzulegen, durch welche unverzichtbaren Vorteile die neuen Risiken aufgewogen werden.

Die wichtigsten Datenschutzanforderungen finden sich in der tabellarischen Übersicht ab der nächsten Seite.

V 1.1 / Stand 15. November 2022

Aufsichtsstelle Datenschutz
Kanonengasse 20
4410 Liestal

T 061 552 64 30
datenschutz@bl.ch
www.bl.ch/datenschutz

[1] Wenn vorliegend von Risiken die Rede ist, sind damit jene für die von der ausgelagerten Datenbearbeitung betroffenen Personen gemeint. Weitere Aspekte wie «business continuity», Abhängigkeit vom Anbieter, Reputation, usw. sind zusätzlich zu berücksichtigen.

5. Wichtigste Datenschutzanforderungen an eine Auftragsdatenbearbeitung

Vorliegend *nicht* aufgeführt sind Anforderungen, die unabhängig von einer Auftragsdatenbearbeitung erfüllt sein müssen.

Thema	Anforderung	Referenz	Einstufung		
			Muss	Umstritten	Risikoanalyse
Zweckbindung	Die Bearbeitung der Personendaten darf ausschliesslich zum gesetzlich vorgegebenen Zweck sowie zur Auftragserfüllung erfolgen. Dieser Zweck muss im Vertrag beschrieben sein. Jede Bearbeitung zu einem anderen Zweck als der Auftragserfüllung ist ausdrücklich untersagt. (Bspw. Werbezwecke, Bonitätsprüfungen etc.)	§ 7 Abs. 2 IDG i.V.m. § 11 Abs. 1 IDG	x		
	Die Zweckbindung umfasst auch die Daten über die Nutzerinnen und Nutzer (bspw. Randdaten, personenbezogen für Analytics etc.).		x		
Rechtmässigkeit	Es darf keine rechtliche (oder vertragliche) Bestimmung entgegenstehen. Die Auftragnehmerin darf die Daten (inkl. Randdaten) bezüglich Umfang und Dauer nur so bearbeiten, wie das öffentliche Organ gemäss seinen (gesetzlichen) Vorgaben dies tun dürfte.	§ 7 Abs. 1 Bst. a und b IDG § 9 IDG	x		
Nachweis der Rechtmässigkeit	Der Umfang der Datenbearbeitung muss vertraglich festgelegt werden.	§ 7 Abs. 1 Bst. b IDG i. V. m. § 8 IDV	x		
Betroffenenrechte	Die Auftragnehmerin hat allfällig an sie gerichtete Gesuche um Zugang zu den eigenen Personendaten nach §§ 24 f IDG an das auftraggebende öffentliche Organ weiterzuleiten und diesem sämtliche für die Beantwortung des Gesuchs erforderlichen Angaben zu liefern.	§§ 24f. IDG	x		
Anwendbares Recht, Gerichtsstand	Für das Vertragsverhältnis gilt grundsätzlich schweizerisches Recht. Der Gerichtsstand befindet sich in der Schweiz.	§ 8 Abs. 2 IDV, Merkblatt privatim			x
	Abweichend von obigem Grundsatz kann die Anwendbarkeit des Rechtes eines anderen Staates und ein ausländischer Gerichtsstand vereinbart werden, wenn es sich um nicht-sensitive Daten handelt und der Staat über ein gleichwertiges Datenschutzniveau verfügt (z.B. Staaten, die der Europaratskonvention K-108 beigetreten sind, vgl. Liste der Staaten mit angemessenem Schutzniveau des EDÖB).				x
Ort der Datenbearbeitung	Der Anbieter muss offenlegen, in welchen Staaten er seine Infrastruktur für die Bearbeitung von Personendaten betreibt, damit die Zulässigkeit von Datenübermittlungen ins Ausland beurteilt und die Risiken in Bezug auf die Serverstandorte bei der Risikoabwägung mitberücksichtigt werden können.	§ 7 Abs. 2 i.V.m. § 8 Abs. 1 IDG § 21 Abs. 1 Bst. a,b IDG	x		
	Datenbearbeitungen an ausländischen Standorten sind nur in Staaten zulässig, die über ein gleichwertiges Datenschutzniveau verfügen oder in denen ein angemessener Datenschutz vertraglich erreicht werden kann. Dabei ist darauf zu achten, dass die fehlende Angemessenheit des Datenschutzniveaus im Drittland nicht darin begründet ist, dass der Vertragspartner die Einhaltung seiner vertraglichen Pflichten aufgrund der auf ihn anwendbaren Gesetzgebung rechtlich oder faktisch nicht gewährleisten kann.	§§ 8 und 9 IDG		x[2]	

Thema	Anforderung	Referenz	Einstufung		
			Muss	Umstritten	Risikoanalyse
Vertraulichkeit / Geheimnisschutz, Verschlüsselung und Schlüsselmanagement	Werden Daten in einer Cloud oder in einer anderen Form mit einem vergleichbaren Gesamtrisiko bearbeitet, sind bei besonderen Personendaten und Daten, die einem Berufs- oder besonderen Geheimhaltungspflichten unterstehen, zusätzliche Anforderungen an die Verschlüsselung und das Schlüssel-management zu stellen und in der Risikoabwägung zu berücksichtigen. - Die Daten sind zu verschlüsseln und die Verschlüsselung hat durch das öffentliche Organ zu erfolgen. Die Schlüssel dürfen nur für das öffentliche Organ verfügbar sein. Sie sind vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme zu schützen - Nur wenn sich daraus keine untragbaren Risiken für die Grundrechte der betroffenen Personen ergeben (was vom öffentlichen Organ nachvollziehbar darzulegen ist), kann eine Verschlüsselung beim Anbieter geprüft werden. Hierbei muss die Ebene, auf welcher die Verschlüsselung erfolgt (Applikation, Datenbank oder Festplatte), berücksichtigt werden. Die Schlüssel können beim Anbieter aufbewahrt werden, wenn dieser sich vertraglich verpflichtet, sie nur mit der ausdrücklichen Zustimmung des öffentlichen Organs zu verwenden. Zugriffe sind zu protokollieren. Ausserdem muss der Anbieter die Schlüssel vor Verlust, Entwendung sowie unrechtmässiger Bearbeitung und Kenntnisnahme schützen und sicherstellen, dass die Daten beim Verschlüsselungsvorgang nicht kompromittiert werden können.	§§ 8 und 9 IDG		x[3]	x
	Der Dienstleister und seine Mitarbeiter sind vertraglich zur Geheimhaltung zu verpflichten.	§ 7 Abs. 1 lit. b IDG (völkerrechtskonforme Auslegung (Art. 22 Abs. 3 Bst. b EU-RL 2016/680)) Art. 320 StGB	x		
	Daten (data in transit) sind nach dem aktuellen Stand der Technik zu verschlüsseln.	§ 8 Abs. 2 IDG	x		
	Daten (data at rest) sind (nach dem aktuellen Stand der Technik) zu verschlüsseln.	§ 8 Abs. 2 IDG			x
	Zusätzliche Anforderungen, die sich aus den Bestimmungen zum Berufs- sowie (besonderen) Amtsgeheimnissen ergeben, müssen separat berücksichtigt werden.	§ 7 Abs. 1 IDG	x		
Vertrag	Das öffentliche Organ schliesst mit dem Dienstleister einen schriftlichen Vertrag. Alternativ schliesst es sich einem Rahmenvertrag an oder akzeptiert die Allgemeinen Geschäftsbedingungen (AGB), bspw. AGB-SIK, welche die hier erwähnten Anforderungen erfüllen und nicht einseitig abänderbar sein dürfen.	§ 7 Abs. 2 IDG § 8 Abs. 1 IDV	x		

Thema	Anforderung	Referenz	Einstufung		
			Muss	Umstritten	Risikoanalyse
Konventionalstrafe	Für den Fall einer vorsätzlichen oder fahrlässigen Verletzung der (Datenschutz-)Vertragsbestimmungen ist als organisatorische Massnahme eine angemessene Konventionalstrafe zu vereinbaren.	§ 8 IDG			x
Subcontracting	Das öffentliche Organ bleibt auch für Datenbearbeitungen verantwortlich, welche der Anbieter seinerseits an Dritte (einschliesslich Mutter- und Tochter) überträgt. Der Anbieter muss für Unterauftragsverhältnisse vorgängig das Einverständnis des öffentlichen Organs einholen, damit dieses die Risiken in Bezug auf die beteiligten Erbringer von Dienstleistungen bei der Risikoabwägung mitberücksichtigen kann. Das Einverständnis kann auch darüber erfolgen, dass das öffentliche Organ mit genügender Vorlaufzeit über den Beizug eines neuen Subunternehmens informiert wird, und vertraglich vereinbart wurde, dass die Ablehnung des Subunternehmens durch das öffentliche Organ einen Vertragskündigungsgrund darstellt.	§ 7 Abs. 2 und 3 IDG § 8 Abs. 2 IDV (Ausstieg)	x		
	Für den Fall einer Vertragsauflösung muss als organisatorische Massnahme das Ausstiegsszenario vorab geklärt sein.	§ 8 Abs. 1 IDG			x
Meldung von Datenschutzverletzungen	Der Dienstleister hat dem öffentlichen Organ Änderungen in der Art und Weise der Datenbearbeitung (insbesondere Datenbearbeitungsorte, Unterauftragsverhältnisse) sowie entsprechend dem anwendbaren Datenschutzrecht Sicherheitsvorfälle und getroffene Massnahmen zu deren Bewältigung zu melden, damit dieses seinerseits rechtzeitig Massnahmen treffen kann.	§ 7 Abs. 2 IDG und § 15a Abs. 3 IDG	x		
Gesuche um Bekanntgabe	Gesuche um Bekanntgabe von Informationen, welche an die Leistungserbringerin gelangen, sind an das öffentliche Organ weiterzuleiten. Dies betrifft Gesuche von Privatpersonen sowie in- und ausländischen Behörden.	§§ 18, 23 IDG	x		
Kontrollrecht und -Möglichkeiten	Das öffentliche Organ hat sich ein Kontrollrecht vorzubehalten: Der Anbieter ist zu verpflichten, regelmässige Kontrollen seiner Services nach anerkannten und dem Schutzbedarf entsprechenden Audit-Standards vorzunehmen. Die Prüfberichte sind dem öffentlichen Organ und der zuständigen Datenschutzaufsichtsbehörde auf Verlangen vorzulegen. Bei Bedarf (namentlich wenn die Kontrollen des Anbieters nicht alle Themen abdecken und sich z.B. auf Sicherheitsaspekte beschränken) müssen Prüfungen des Organs selbst bzw. seiner Aufsichtsbehörde oder durch diese beauftragte Dritte möglich sein.	Merkblatt privatim, abgeleitet aus § 6, § 7 Abs. 2 und § 41 Abs. 1 und 2 IDG	x		
Informationssicherheitsmassnahmen	Das öffentliche Organ hat sicherzustellen, dass ein dem Schutzbedarf entsprechender Schutz gewährleistet wird. Um das zu beurteilen, hat es den Dienstleister zu verpflichten, in Bezug auf die Infrastruktur darzulegen, welche Schutzziele er mit welchen Informationssicherheitsmassnahmen erreicht.	§ 8 IDG i:V.m. § 7 Abs. 2 IDG	x		

Thema	Anforderung	Referenz	Einstufung		
			Muss	Umstritten	Risikoanalyse
Trennung der Daten (Mandantentrennung)	Durch ein geeignetes Mandantentrennungskonzept soll sichergestellt werden, dass Anwendungs- und Datenkontexte verschiedener Outsourcing-Kunden klar getrennt sind. Das Mandantentrennungskonzept wird dem Outsourcing-Kunden zur Verfügung gestellt und sollte für den Schutzbedarf angemessene Sicherheit bieten.	§ 6 und § 8 IDG			x
Pflichten bei Auflösung	Ungeachtet des Grundes der Vertragsauflösung verpflichtet sich die Auftragnehmerin, die für das auftraggebende öffentliche Organ bearbeiteten Informationen umgehend und unentgeltlich im [tbd] Format übertragen. Die Erfüllung dieser Pflicht kann von der Auftragnehmerin selbst dann nicht aufgeschoben werden, wenn zwischen den Parteien Auseinandersetzungen bestehen sollten. Die Auftragnehmerin ist verpflichtet, die für das öffentliche Organ bearbeiteten Informationen unentgeltlich zu übertragen oder vernichten (inkl. Festsetzung der Frist oder Bedingung). Die Vernichtung bei der Auftragnehmerin kann das auftraggebende öffentliche Organ selbst überprüfen oder durch einen Dritten überprüfen lassen.	§ 8 Abs. 2 IDV	x		
Portabilität von Services	Die Vorgaben für eine Portabilität (Wechsel des Anbieters, Zurückholen in die eigene Infrastruktur) sind vertraglich zu vereinbaren. Regelmässige Portabilitätstests sind einzuplanen. Ausgenommen sind Fälle, bei denen von Beginn weg klar ist, dass die Informationen nicht über das Vertragsende hinaus benötigt und deshalb beim Anbieter vernichtet werden.	§ 8 Abs. 2 IDV	x		

---

[2] Ist die fehlende Gleichwertigkeit des Datenschutzniveaus vertraglich mit grosser Wahrscheinlichkeit nicht kompensierbar, müssen sensitive Informationen in jedem Fall beim öffentlichen Organ verschlüsselt werden (end-to-end). Bei allen anderen Informationen sind Ausnahmen vom Grundsatz der Verschlüsselung restriktiv zu handhaben.

[3] Derzeit besteht noch keine höchstrichterliche Rechtsprechung zur Frage, unter welchen Voraussetzungen ein Outsourcing der Bearbeitung von Informationen, die dem Amtsgeheimnis unterstehen, zulässig ist. Diese Frage stellt sich bei allen Kategorien von Informationen, die dem allgemeinen oder einem spezialgesetzlichen Amtsgeheimnis unterstehen. Die ASD geht davon aus, dass mit der Verankerung einer spezialgesetzlichen Geheimhaltungspflicht der Schutzbedarf der davon erfassten Informationen demjenigen von besonderen Personendaten entspricht. Daraus folgt, dass identische Schutzmassnahmen vorzusehen sind. Es muss im Einzelfall durch Auslegung ermittelt werden, ob eine spezialgesetzliche Geheimhaltungspflicht einer Auslagerung grundsätzlich entgegensteht (vgl. Rechtmässigkeit). Ist dies der Fall, stellt sich die Frage der Tragbarkeit der Risiken durch das öffentliche Organ schon gar nicht und eine Auslagerung kann ausschliesslich in Betracht gezogen werden, wenn die Verschlüsselung der Informationen durch das öffentliche Organ sichergestellt ist.

Die Frage, ob die Möglichkeit eines sog. «lawful access» (bspw. in Anwendung des Cloud-Acts, wobei sich die Rechtmässigkeit lediglich auf das Rechtssystem der zugreifenden Behörde bezieht) einer Auslagerung ohne Verschlüsselung durch das öffentliche Organ grundsätzlich entgegensteht oder lediglich ein Risiko darstellt, ist umstritten. Die ASD geht aktuell davon aus, dass diesbezüglich ein risikobasierter Ansatz zulässig ist. Die Notwendigkeit der Verschlüsselung sensitiver Daten insbesondere bei Cloud-Lösungen ergibt sich aus Sicht der ASD somit nicht aus einer grundsätzlichen Unzulässigkeit der Auslagerung unverschlüsselter Daten, sondern aufgrund der Gesamtrisikobetrachtung.