Merkblatt

25.09.2024

Datenbearbeitung im Auftrag

Das vorliegende Merkblatt richtet sich an die öffentlichen Organe des Kantons Aargau. Es erläutert, was zu beachten ist, wenn Auftragnehmende mit der Bearbeitung von Personendaten beauftragt werden.

1. Gesetzliche Grundlage

Lässt ein öffentliches Organ Personendaten durch Dritte bearbeiten, hat es nach § 18 IDAG[1] den Datenschutz durch Vereinbarungen, Auflagen oder in anderer Weise sicherzustellen. Es bleibt für die Einhaltung des Datenschutzes verantwortlich.

Wenn die Voraussetzungen der Datenbearbeitung im Auftrag erfüllt sind, gilt der oder die Auftragnehmende als verlängerter Arm des auftraggebenden öffentlichen Organs. Die Rechtsgrundlage, auf die sich das auftraggebende öffentliche Organ für seine Datenbearbeitungen stützt, gilt auch für den oder die Auftragnehmenden. Es handelt sich um eine Privilegierung und die Vorschriften über die Datenbekanntgabe an Dritte sind nicht anwendbar. Sind die Voraussetzungen der Auftragsdatenbearbeitung erfüllt, stehen nach der aargauischen Gesetzeslage das Amtsgeheimnis oder besondere Amtsgeheimnisse einer Auslagerung nicht grundsätzlich entgegen[2]. Allfällige spezialgesetzliche Geheimhaltungsvorschriften, die einer Übermittlung an Auftragnehmende entgegenstehen, bleiben aber zu beachten. Eine besondere Rechtsgrundlage ist erforderlich, wenn die Erfüllung einer öffentlichen Aufgabe ausgelagert wird (vgl. nachfolgend Ziffer 2).

2. Begriff «Datenbearbeitung im Auftrag»

Kennzeichnend für die Auftragsdatenbearbeitung ist, dass Daten durch Dritte bearbeitet werden, die nicht derselben Verwaltungsabteilung angehören bzw. unterstellt sind und dass der oder die Auftragnehmende diese Daten nicht zur Erfüllung einer ihm übertragenen gesetzlichen Aufgabe benötigt, d.h. Personendaten nicht im Rahmen der Amtshilfe bekanntgegeben werden. Eine Auftragsdatenbearbeitung liegt nur vor, wenn der Auftraggeber nicht nur rechtlich, sondern zumindest prinzipiell auch tatsächlich in der Lage ist, dem oder der Auftragnehmenden jeden Arbeitsschritt vorzuschreiben und letztlich auch die korrekte Durchführung

---

1 Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006 (SAR 150.700).

2 Die Anforderungen an die Verhältnismässigkeit und die Datensicherheit können aber erhöht sein. Entscheidend ist, ob der Auftragnehmende den durch das besondere Amtsgeheimnis eingeräumten Schutz des Persönlichkeitsrechts organisatorisch und technisch sicherstellt, wobei ein strenger Massstab anzulegen ist.

des Datenumgangs kontrollieren zu können. Typisches Merkmal einer Auftragsdatenbearbeitung ist der Umstand, dass sich der Auftraggeber die Entscheidungsbefugnis vorbehält und dem oder der Auftragnehmenden keinerlei inhaltlichen Ermessensspielraum gestattet.

Im Zusammenhang mit der Auftragsdatenbearbeitung werden oftmals synonym die Begriffe «Auslagerung der Datenbearbeitung», «Outsourcing» oder «Auftragsbearbeitung» verwendet.

Das Bearbeiten umfasst begrifflich jeden Umgang mit Personendaten, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben oder Vernichten (§ 3 lit. g IDAG). So können beispielsweise private (IT-)Firmen mit der Unterstützung bei der Geschäftsverwaltung durch eine kantonale oder kommunale Behörde beauftragt werden. Weitere Beispiele 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 selbst zu einem öffentlichen Organ im Sinne von § 3 lit. c Ziff. 2 IDAG und das IDAG findet somit direkt Anwendung auf den beauftragten privaten Dritten. Dieser hat die Vorgaben des IDAG und der VIDAG[3] hinsichtlich der Datenbearbeitung und der Informationssicherheit eigenverantwortlich einzuhalten.

3. Strafbarkeit

Die Verantwortlichkeit für die Einhaltung der Datenschutzbestimmungen liegt zwar beim auftraggebenden öffentlichen Organ. Auftragnehmende können aber bei vertragswidrigem Verhalten haftpflichtig werden. Zudem können Auftragnehmende auch persönlich strafrechtlich belangt werden:

> ***§ 41 Verwaltungsstrafe***
>
> *[1]Wer als Auftragnehmerin oder Auftragnehmer für das Bearbeiten von Personendaten ohne ausdrückliche Ermächtigung des auftraggebenden Organs Personendaten für sich oder andere verwendet oder anderen bekannt gibt, wird mit Busse bis zu Fr. 10'000.– bestraft.*
>
> *[2]Handelt die Täterin oder der Täter aus Gewinnsucht, ist das Gericht an diesen Höchstbetrag nicht gebunden.*
>
> *[3]Strafbar ist die vorsätzliche oder fahrlässige Widerhandlung.*
>
> *[4]Im Übrigen gelten die Bestimmungen des Schweizerischen Strafgesetzbuches vom 21. Dezember 1937.*

[3] Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG) vom 26. September 2007 (SAR 150.711).

4. Konkrete Massnahmen zur Sicherstellung datenschutzrechtlicher Anforderungen

Die rechtlichen, organisatorischen und technischen Anforderungen, die sich aus IDAG und VIDAG ergeben, müssen im Vorfeld der Auftragsdatenbearbeitung durch den oder die potentiellen Auftragnehmenden gegenüber dem öffentlichen Auftraggeber ausgewiesen werden können. Das öffentliche Organ als Auftraggeber und weiterhin Verantwortlicher hat darauf die Offerten und Risiken[4], die mit der jeweiligen Auslagerung einhergehen, zu prüfen.

Die Elemente der Anforderungen an den Datenschutz und die Informationssicherheit müssen in einem Vertrag mit dem oder der Auftragnehmenden schriftlich festgelegt und die Vertragseinhaltung auf geeignete Weise sichergestellt sein – beispielsweise durch die Festsetzung einer Konventionalstrafe. Die VIDAG schreibt vor:

> ***§ 12a Datenverarbeitung im Auftrag***
>
> *[1]Auftragnehmende für die Bearbeitung von Personendaten sind vom öffentlichen Organ unter besonderer Berücksichtigung der von jenen getroffenen technischen und organisatorischen Massnahmen sorgfältig auszuwählen. Durch Vertrag oder Auflagen sind festzulegen:*
>
> *a) Gegenstand und Dauer des Auftrags,*
> *b) Umfang, Art und Zweck der vorgesehenen Datenbearbeitung, die Art der Daten und der Kreis der Betroffenen*
> *c) die zur Einhaltung der Datensicherheit zu treffenden technischen und organisatorischen Massnahmen, deren Kontrolle und Dokumentation,*
> *d) Durchsetzung von Ansprüchen betroffener Personen*
> *e) Verpflichtung zur Verschwiegenheit und Überbindung dieser Pflicht auf alle Datenbearbeitenden*
> *f) allfällige Berechtigung zur Vergabe von Unteraufträgen*
> *g) Kontrollrechte des auftraggebenden öffentlichen Organs und entsprechende Duldungs- und Mitwirkungspflichten des Auftragnehmenden*
> *h) Mitteilungspflicht des Auftragnehmenden bei Verletzungen der Datensicherheit*
> *i) Weisungsbefugnis des öffentlichen Organs*
> *j) die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmenden gespeicherter Daten.*
>
> *[2]Stellt die Bearbeitung von Personendaten nicht die Hauptpflicht des Auftragnehmenden dar, haben sich die Vereinbarung oder die Auflagen sinngemäss am Inhalt gemäss Abs. 1 zu orientieren.*

Der oder die Auftragnehmende muss sorgfältig ausgewählt und instruiert und im Verlauf des Auftrags auf Einhaltung der Anforderungen überprüft werden. Können die Anforderungen durch den oder die Auftragnehmende 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.

[4] 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.

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.)	§ 18 Abs. 2 IDAG i.V.m. § 11 IDAG; § 12a Abs. 1 lit. b VIDAG	x		
	Die Zweckbindung umfasst auch die Daten über die Nutzerinnen und Nutzer (bspw. Randdaten, personenbezogen für Analytics etc.).		x		
Rechtmässigkeit	Der Auslagerung darf keine rechtliche (oder vertragliche) Bestimmung entgegenstehen. Der oder die Auftragnehmende darf die Daten (inkl. Randdaten) bezüglich Umfang und Dauer nur so bearbeiten, wie das öffentliche Organ gemäss seinen (gesetzlichen) Vorgaben dies tun dürfte.	§ 18 Abs. 2 IDAG i.V.m. § 8 IDAG	x		
Nachweis der Rechtmässigkeit	Der Umfang der Datenbearbeitung muss vertraglich festgelegt werden.	§ 18 Abs. 1 IDAG i.V.m. § 12a VIDAG	x		
Betroffenenrechte	Der oder die Auftragnehmende hat allfällig an sie gerichtete Gesuche um Zugang zu den eigenen Personendaten nach §§ 23 f IDGA an das auftraggebende öffentliche Organ weiterzuleiten und diesem sämtliche für die Beantwortung des Gesuchs erforderlichen Angaben zu liefern.	§§ 23 f. IDAG i.V.m. § 12a Abs. 1 lit. d VIDAG	x		
Anwendbares Recht, Gerichtsstand	Für das Vertragsverhältnis gilt grundsätzlich schweizerisches Recht. Der Gerichtsstand befindet sich in der Schweiz.	§ 14 Abs. 3 IDAG, privatim - Merkblatt Cloud-spezifische Risiken und Massnahmen			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	§ 14 Abs. 3 IDAG i.V.m. § 12 Abs. 1 IDAG	x		

Thema	Anforderung	Referenz	Einstufung		
			Muss	Umstritten	Risikoanalyse
	Ausland beurteilt und die Risiken in Bezug auf die Serverstandorte bei der Risikoabwägung mitberücksichtigt werden können.				
	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[5+6].	§ 14 Abs. 3 und 4 IDAG		x[i]	
Vertraulichkeit / Geheimnisschutz, Verschlüsselung und Schlüsselmanagement	- Werden Daten in einer Cloud oder in einer anderen Form mit einem vergleichbaren Gesamtrisiko bearbeitet, sind bei besonders schützenswerten Personendaten und Daten, die besonderen Geheimhaltungspflichten unterstehen, zusätzliche Anforderungen an die Verschlüsselung und das Schlüsselmanagement 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. Zu-	§ 9 IDAG, § 12 Abs.1 IDAG, § 14 Abs. 3 IDAG		x[ii]	x

5 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.

6 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 ÖDB 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 ÖDB somit nicht aus einer grundsätzlichen Unzulässigkeit der Auslagerung unverschlüsselter Daten, sondern aufgrund der Gesamtrisikobetrachtung.

Thema	Anforderung	Referenz	Einstufung		
			Muss	Umstritten	Risikoanalyse
	griffe 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.				
	Der Dienstleister und seine Mitarbeiter sind vertraglich zur Geheimhaltung zu verpflichten.	§ 12a lit. e VIDAG; Art. 320 StGB	x		
	Daten (data in transit) sind nach dem aktuellen Stand der Technik zu verschlüsseln.	§ 4 Abs. 1 lit. c VIDAG i.V.m. § 4 Abs. 2 VIDAG	x		
	Daten (data at rest) sind (nach dem aktuellen Stand der Technik) zu verschlüsseln.	§ 12a Abs. 1 lit. e – g VIDAG			x
	Zusätzliche Anforderungen, die sich aus besonderen Geheimhaltungsvorschriften ergeben, müssen separat berücksichtigt werden.	§ 8 IDAG; Art. 320 StGB	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.	§ 18 Abs. 1 IDAG	x		
Strafen	Für den Fall einer vorsätzlichen oder fahrlässigen Verletzung der (Datenschutz-)Vertragsbestimmungen ist als organisatorische Massnahme eine angemessene Konventionalstrafe zu vereinbaren. Der oder die Auftragnehmende ist auf die Strafbestimmung von § 41 IDAG hinzuweisen.	§ 8 IDAG			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.	§ 18 Abs. 1 Satz 2 IDAG	x		

Thema	Anforderung	Referenz	Einstufung		
			Muss	Umstritten	Risikoanalyse
	Für den Fall einer Vertragsauflösung muss als organisatorische Massnahme das Ausstiegsszenario vorab geklärt sein.	§ 4 Abs. 1 VIDAG (Schutzziel: Verfügbarkeit)			x
Meldung von Datenschutzverletzungen	Der Dienstleister hat dem öffentlichen Organ Änderungen in der Art und Weise der Datenbearbeitung (insbesondere Datenbearbeitungsorte, Unterauftragsverhältnisse) sowie Datensicherheitsvorfälle und getroffene Massnahmen zu deren Bewältigung zu melden, damit dieses seinerseits rechtzeitig Massnahmen treffen kann.	§ 18 Abs. 2 IDAG und § 12a lit. h VIDAG	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.	§ 12a Abs. 1 lit. d VIDAG	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.	§ 12a Abs. 1 lit. g VIDAG	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.	§ 18 Abs. 1 IDAG i.V.m. § 12 Abs. 1 IDAG; § 4 Abs. 3 VIDAG i.V.m. § 12a Abs. 1 lit. c VIDAG	x		
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.	§ 4 VIDAG (Schutzziel: Vertraulichkeit)			x
Pflichten bei Auflösung	Ungeachtet des Grundes der Vertragsauflösung verpflichtet sich der oder die Auftragnehmende, die für das auftraggebende öffentliche Organ bearbeiteten Informationen umgehend und unentgeltlich im [tbd] Format zu übertragen. Die Erfüllung dieser Pflicht kann von dem oder der Auftragneh-	§ 4 VIDAG (Schutzziel: Verfügbarkeit)	x		

Thema	Anforderung	Referenz	Einstufung		
			Muss	Umstritten	Risikoanalyse
	menden selbst dann nicht aufgeschoben werden, wenn zwischen den Parteien Auseinandersetzungen bestehen sollten. Der oder die Auftragnehmende ist verpflichtet, die für das öffentliche Organ bearbeiteten Informationen unentgeltlich zu übertragen oder vernichten (inkl. Festsetzung der Frist oder Bedingung). Die Vernichtung bei dem oder der Auftragnehmenden kann das auftraggebende öffentliche Organ selbst überprüfen oder durch einen Dritten überprüfen lassen.				
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.	§ 4 VIDAG (Schutzziel: Verfügbarkeit)	x		

[i] 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.

[ii] Derzeit besteht noch keine höchstrichterliche Rechtsprechung zur Frage, unter welchen Voraussetzungen ein Outsourcing der Beauftragten von Informationen, die dem Amtsgeheimnis unterstehen, zulässig ist. Diese Frage stellt sich bei allen Kategorien von Informationen, die dem allgemeinen oder einem spezialgesetzlichen Amtsgeheimnis untersteht. Die ÖDB 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 ÖDB 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 ÖDB somit nicht aus einer grundsätzlichen Unzulässigkeit der Auslagerung unverschlüsselter Daten, sondern aufgrund der Gesamtrisikobetrachtung.