Inventar – Datenbearbeitung (für Auftragsbearbeiter) — Formular B.3

Unternehmenseinheit: _____ Ausgefüllt von: _____ Stand vom: _____

Die Ausführungen gelten für folgende Kategorie von Datenbearbeitungen: _____ **DB-Nr:** _____

Die Ausführungen in diesem Formular gelten ☐ für einen Auftraggeber ☐ für mehrere Auftraggeber (gemäss Formular bzw. beiliegender Liste)

Beilagen: _____

Es wird davon ausgegangen (→ Formular B.1), dass folgende Regelungen erfüllt werden müssen: ☐ DSG ☐ DSGVO ☐ _____

Arbeitsanweisung:

- In diesem Formular werden die Mindestangaben für das **Verzeichnis der Datenbearbeitungen** erfasst, die sowohl nach dem revidierten DSG (Art. 11) als auch der DSGVO (Art. 30) vom Auftragsbearbeiter zu führen sind.

- Der Auftragsbearbeiter muss dazu Angaben über die jeweilige Datenbearbeitung, aber auch über seinen Auftraggeber machen. Wird dieselbe Art von Datenbearbeitung **für mehrere Auftraggeber parallel** vorgenommen, so ist dies oben anzugeben. Es genügt aber, dieses Formular *einmal* für alle auszufüllen, wobei die Daten der einzelnen Auftraggeber in diesem Fall unten oder separat in einer Beilage zu diesem Formular zu erfassen sind.

- Die Beurteilung, ob die Datenbearbeitung auch aus Sicht des Auftragsbearbeiters den **gesetzlichen Anforderungen** entspricht, erfolgt über ein anderes Formular (→ Formular E.2); der Auftraggeber wird selbst einen Compliance-Check durchführen müssen.

- Im vorliegenden Formular ist der **momentane Zustand** anzugeben. Dieser kann sich im Rahmen von zu treffenden Massnahmen ändern. In diesem Falle ist dieses Formular nachzuführen. Dieses Formular ist auf Unternehmen mit Sitz in der Schweiz ausgerichtet, deckt aber sowohl die Anforderungen nach DSGVO als auch nach dem revidierten DSG ab.

		Anforderung	Anforderung erfüllt?	Was zu tun ist
Q1	**Name und Kontaktdaten des Auftrags-bearbeiters** Gemeint ist die Unternehmenseinheit, welche die Auftragsbearbeitung durchführt (nicht die unternehmensinterne Stellte; diese wird hier nicht verzeichnet).	→ Q1 in Formular A.1	☐ Bemerkungen:	
Q2	**Name und Kontaktdaten der Verant-wortlichen, in deren Auftrag die Daten-bearbeitung erfolgt** Hier muss angegeben werden, für wen die hier abgehandelte Auftragsbearbeitung durchgeführt wird, d.h. für welche anderen Unternehmenseinheiten (gemeint sind die juristischen Personen). Im Falle einer gruppeninternen Auftragsbearbeitung kann angegeben werden, wo im System bzw. in der Dokumentation sich herausfinden lässt, welche Gruppengesellschaften das sind; eine namentliche Nennung in diesem Formular ist nicht nötig. Bei anderen Auftraggebern kann analog verfahren werden. Sie sind entweder hier anzugeben, in einer Beilage oder es kann auf ein Verzeichnis im internen System verwiesen werden, wo nachgeschaut werden kann.	☐ Die anderen Gesellschaften der Gruppe: ☐ Andere Auftraggeber: ☐ Auftraggeber gem. Beilage ☐ Auftraggeber gem. Angaben im System:	☐ Bemerkungen: ☐ Situation unklar Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren

Q3

Falls DSGVO anwendbar:

Name und Kontaktdaten der Vertreter und Datenschutzbeauftragten des bzw. der Verantwortlichen, in deren Auftrag die Datenbearbeitung erfolgt

Die DSGVO verlangt, dass nicht nur die Name und die Kontaktdaten der Auftraggeber verzeichnet werden, sondern auch deren Vertreter nach Art. 27 DSGVO und deren Datenschutzbeauftragten nach Art. 37 DSGVO, falls es einen solchen gibt. Dies kann hier im Formular oder in einer separaten Beilage oder sonst in den Systemen des Auftragsbearbeiters erfasst werden.

☐ Gesellschaften der Gruppe:

- ☐ Derselbe Vertreter wie jener des Auftragsbearbeiters: → Q4 in Formular A.1
- ☐ Derselbe Datenschutzbeauftragte wie jener des Auftragsbearbeiters: → Q5 in Formular A.1
- ☐ Andere (Namen, Kontaktdaten oder Verweis darauf, wo diese Angaben abgelegt sind):

☐ Andere Auftraggeber:

Name	Vertreter (Art. 27 DSGVO)	Datenschutzbeauftragter (Art. 37 DSGVO)

☐ Angaben gem. Beilage

☐ Angaben sind im System:

☐ Bemerkungen:

☐ Situation unklar

Grund:

- ☐ Weitere Abklärungen sind nötig
- ☐ Experte konsultieren

	Q4	**Kategorien der Bearbeitungen, die für den bzw. die Verantwortlichen durchgeführt werden** Es ist anzugeben, welche Bearbeitungen im Auftrag durchgeführt werden. Es wird hier keine detailierte Aufstellung verlangt. Es genügen Angaben darüber, wozu die Leistungen dienen, die im Rahmen der Auftragsbearbeitung erbracht werden, damit sich der Leser eine ungefähre Vorstellung darüber machen kann, was der Auftragsbearbeiter tut. Bei kommerziellen Services kann jedoch nach den einzelnen Services unterschieden werden, ggf. auch durch Verweis auf einen Service-Katalog, falls dies die Dinge vereinfacht.	☐ IT-Betriebsleistungen ☐ IT-Leistungen im Zusammenhang mit bestimmten Projekte ☐ Betriebliches Personalwesen ☐ Betriebliches Rechtswesen ☐ Interne Aus- und Weiterbildung ☐ Internes Know-How Management ☐ Finanzbuchhaltung ☐ Finanzverwaltung ☐ Gebäude- und Betriebslogistik ☐ Sicherheitsdienst ☐ Andere: ☐ Dienstleistungen gem. Beilage	☐ Bemerkungen: ☐ Situation unklar Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren
	Q5	**Angabe der Länder, in welche Personendaten womöglich übermittelt werden** Dieser Punkt soll letztlich Auskunft darüber geben, ob die Personendaten vom Unternehmen aus in Länder gelangen können, die über keinen angemessenen gesetzlichen Datenschutz verfügen. Der Begriff der Übermittlung oder Bekanntgabe umfasst dabei auch den Fernzugriff bzw. das Gewähren eines solchen, nicht nur die aktive Versendung ins Ausland. Welche Länder über einen angemessenen Schutz verfügen, entscheidet die Europäische Kommission bzw. unter dem neuen DSG der Bundesrat, der die Entscheide der EU nachvollzieht (eine Liste findet sich hier: https://goo.gl/WqctY9).	☐ Keine Übermittlungen in andere Länder vorgesehen ☐ Übermittlung(en) in folgende Länder möglich ☐ Ausschliesslich in Länder der EU bzw. des EWR ☐ Alle Länder der Erde ☐ Alle Länder, in welchen die Gruppe Standorte hat ☐ In folgende Länder:	☐ Bemerkungen: ☐ Situation unklar Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren

	Relevant sind hier nur Auslandsübermittlungen, die vom Auftragsbearbeiter kontrolliert werden, z.B. an Subunternehmen. Die Übermittlung von und zum Auftraggeber ist hier nicht zu erfassen, auch wenn sich dieser in einem anderen Land befindet. Der Blickwinkel dieser Regelung ist aus der Sicht der DSGVO und des DSG etwas unterschiedlich. Aus der Sicht des DSG sind alle Fälle aufzuführen, in denen die Daten die Schweiz verlassen (soweit sie sich zuvor auf Schweizer Boden befinden), aus der Sicht der DSGVO sind hingegen nur jene Fälle relevant, in welchen die Daten in sog. Drittstaaten gelangen, d.h. Staaten ausserhalb der EU (und des EWR). Der Datentransfer zwischen den Mitgliedstaaten der EU ist nicht erfasst. Hier sollte allerdings der Einfachheit halber erfasst werden, wohin die Daten gehen, ob dies rechtlich relevant ist oder nicht. Unter der DSGVO muss auch angegeben werden, wenn die Daten an eine internationale Organisation mit rechtlichem Sonderstatut (der UN, etc.) übermittelt werden, nicht nur in Drittstaaten. Im Weiteren verlangen DSG und DSGVO, dass Angaben darüber gemacht werden, wie der Verantwortliche damit umgeht, wenn die Daten in ein Land ohne angemessenen Datenschutz gelangen. Unter der DSGVO muss angegeben werden, welche alternativen Instrumente (z.B. Datenübermittlungsvertrag) zum Einsatz kommen, um einen angemessenen Datenschutz zu garantieren (Art. 49 DSGVO). Unter dem DSG sind diese ebenfalls anzugeben (vgl. Art. [13] DSG), aber auch, falls keine solchen zum Einsatz kommen, weil der Verantwortliche sich auf einen anderen Rechtfertigungsgrund nach Art. [14] DSG (wie z.B. bei ausländischen Gerichtsverfahren) beruft.	*Falls DSG anwendbar:* ☐ Die Übermittlung in unsichere Drittstaaten wird abgesichert durch ☐ einen völkerrechtlichen Vertrag ☐ dem EDÖB mitgeteilte vertragliche Datenschutzklauseln ☐ dem EDÖB mitgeteilte behördliche Datenschutzgarantien ☐ vom EDÖB oder der EU genehmigte BCR ☐ EU- oder andere vom EDÖB akzeptierte Standardvertrags-klauseln ☐ Die Übermittlung in unsichere Drittstaaten auf anderer Basis *Falls DSGVO anwendbar:* ☐ Übermittlung(en) an internationale Organisationen möglich ☐ Übermittlungen sind auch aufgrund der Sondervorschrift von Art. 49(1) Unterabsatz 2 DSGVO vorgesehen, in welchem Falle folgende Garantien zum Einsatz kommen: ☐ Gemäss Beilage	

Q6

Massnahmen zur Datensicherheit

Hier wird ("wenn möglich") eine allgemeine Beschreibung der technischen und organisatorischen Massnahmen der Datensicherheit verlangt. Datensicherheit ist ein Aspekt des Datenschutzes. Sie zielt darauf ab, die Vertraulichkeit, Integrität und Verfügbarkeit der bearbeiteten Personendaten zu schützen, die Belastbarkeit der Systeme sicherzustellen, eine rasche Wiederherstellung von Personendaten nach einem Zwischenfall zu gewährleisten und umfasst auch Verfahren zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Massnahmen (vgl. Art. 32 DSGVO). Technische Massnahmen sind z.B. die Verschlüsselung bzw. Pseudonymisierung, Zugang nur mit persönlichem Login, Firewalls, Protokolle. Organisatorische Massnahmen sind Weisungen, Schulungen, Audits, Kontrollen.

Normaler- und sinnvollweise sind die Massnahmen zur Datensicherheit in entsprechenden Weisungen geregelt. In diesen Fällen kann direkt auf diese verwiesen werden (sie sind in → Formular A.2 zu erfassen). Ist dies nicht der Fall, sollten hier einige Stichworte zu den getroffenen Massnahmen aufgezählt werden. Einige Beispiele sind angegeben.

☐ Es gelten die Massnahmen gemäss den Weisungen zur Datensicherheit des Unternehmens → Formular A.2, insb. Q2

☐ Es bestehen folgende Massnahmen zur Datensicherheit:

- ☐ Passwortschutz für Mitarbeiter des Auftraggebers (wird durch diesen verwaltet)
- ☐ Passwortschutz für Mitarbeiter des Auftragsbearbeiters
- ☐ Zugang zu Kundendaten nur durch ausgewählte Mitarbeiter des Auftragsbearbeiters
- ☐ Kundendaten werden verschlüsselt gespeichert
- ☐ Übermittlungen vom und zum Kunden erfolgen verschlüsselt, alle Weiterübermittlungen innerhalb der Organisation des Auftragsbearbeiters ebenfalls
- ☐ Protokollierung aller Zugriffe (Audit Trails)
- ☐ IT-Systeme sind physisch geschützt (verschlossen)
- ☐ Systeme haben einen Internet-Zugang, der jedoch mit einer Firewall geschützt ist
- ☐ Systeme haben einen aktuellen Viren- und Malwareschutz
- ☐ Systeme werden automatisch mit Updates nachgeführt
- ☐ Systemkonfiguration wurde fachmännisch auf Sicherheit geprüft
- ☐ Instruktion der Mitarbeiter betr. Datensicherheit

☐ Es bestehen keine besonderen Massnahmen zur Datensicherheit

☐ Bemerkungen:

☐ Situation unklar

Grund:

- ☐ Weitere Abklärungen sind nötig
- ☐ Experte konsultieren

Weitere Bemerkungen: