Inventar – Datenbearbeitung (für Verantwortliche) — Formular B.2

Unternehmenseinheit: _____ Ausgefüllt von: _____ Stand vom: _____

Die Ausführungen gelten für folgende Datenbearbeitung: _____ **DB-Nr:** _____

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) zu führen ist. Für jede Datenbearbeitung ist dieses Formular separat auszufüllen. Die Beurteilung, ob die Datenbearbeitung den gesetzlichen Anforderungen entspricht, erfolgt über ein anderes Formular (→ Formular E.1). Im vorliegenden Formular ist der momentane Zustand zu dokumentieren. 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 Verantwortlichen** Gemeint ist die Unternehmenseinheit, welche für die Datenbearbeitung verantwortlich zeichnet (nicht die unternehmensinterne Verantwortlichkeit; diese wird hier nicht verzeichnet).	→ Q1 in Formular A.1	☐ Bemerkungen:
		Q2	*Falls DSGVO anwendbar:* **Name und Kontaktdaten des Vertreters im Sinne von Art. 27 DSGVO** Anzugeben ist der vom Unternehmen allenfalls bestellte Vertreter nach Art. 27 DSGVO (ob ein solcher zu bestellen ist, ergibt sich aus → Formular D.1).	→ Q4 in Formular A.1	☐ Bemerkungen:
		Q3	*Falls DSGVO anwendbar:* **Name und Kontaktdaten des Datenschutzbeauftragten** Anzugeben ist der vom Unternehmen allenfalls bestellte Datenschutzbeauftragte nach Art. 37 DSGVO (ob ein solcher zu bestellen ist, ergibt sich aus → Formular D.1).	→ Q5 in Formular A.1	☐ Bemerkungen:

Q4

Zwecke der Bearbeitung

Jede Datenbearbeitung muss einem oder mehreren Zwecken dienen. Beispiele sind angegeben.

Ob es genügt, den "Überzweck" anzukreuzen (z.B. "Personaladministration"), hängt davon ab, ob die betreffende Datenbearbeitung tatsächlich so breit angelegt ist. Ist der Bereich der Personaladministration auf verschiedene Datenbearbeitungen verteilt, sollte dementsprechend mit Unterkategorien gearbeitet werden.

☐ Personaladministration

- ☐ Salär, Bonus
- ☐ Versicherung
- ☐ Ferien und Spesen
- ☐ Kontrolle Arbeitszeit
- ☐ Aus- und Weiterbildung
- ☐ Steuern
- ☐ Leistung & Disziplin
- ☐ Karriereentwicklung
- ☐ Einsatzplanung
- ☐ Arbeitssicherheit
- ☐ Andere:

☐ Rekrutierung neuer Mitarbeiter

- ☐ Abklärungen im Zusammenhang mit Bewerbungen
- ☐ Bewerbungsgespräche
- ☐ Vertragsverhandlungen
- ☐ Andere:

☐ Finanzen und Buchhaltung

- ☐ Buchhaltung
- ☐ Kreditwesen
- ☐ Revision
- ☐ Andere:

☐ Bemerkungen:

☐ Situation unklar

Grund:

- ☐ Weitere Abklärungen sind nötig
- ☐ Experte konsultieren

☐ Logistik

- ☐ Einkauf
- ☐ Transport und Logistik
- ☐ Unterhalt Systeme
- ☐ Physisches Archiv
- ☐ Andere:

☐ IT & Telekommunikation, Sicherheit

- ☐ Betrieb Website
- ☐ Betrieb Anwendungen & Netz
- ☐ Arbeitsplatzsysteme
- ☐ Gebäudezugang
- ☐ Mobile Devices
- ☐ Videoüberwachung
- ☐ Elektronisches Archiv
- ☐ IT-Überwachung
- ☐ Andere:

☐ Customer Relationship Management (CRM)

- ☐ Kommunikation mit Kunden
- ☐ Kundenverträge
- ☐ Werbung und Marketingprodukte
- ☐ Marktforschung
- ☐ Andere:

☐ Andere Zwecke:

Q5

Kategorien der betroffenen Personen

Anzugeben ist, von welchen Kategorien von Personen in der Datenbearbeitung Personendaten vorkommen. Anzugeben sind auch Personengruppen, die nur am Rande vorkommen.

Nicht angegeben werden müssen Mitarbeiter des Unternehmens, soweit deren Daten lediglich für die Zwecke des technischen Betriebs der Datenbearbeitung bearbeitet werden (Zugriffskontrolle, Audit Trails).

- ☐ Mitarbeiter (auch ehemalige, temporäre und künftige, und auch Externe, die vor Ort arbeiten)
- ☐ Kunden (bzw. Mitarbeiter von Kunden), inkl. potenzielle
- ☐ Geschäftspartner (bzw. Mitarbeiter von Geschäftspartnern), inkl. potenzielle
- ☐ Besucher der Website
- ☐ Personen, die mit dem Unternehmen kommunizieren
- ☐ Andere:

- ☐ Bemerkungen:
- ☐ Situation unklar

  Grund:

  - ☐ Weitere Abklärungen sind nötig
  - ☐ Experte konsultieren

Q6

Kategorien der betroffenen Daten

Anzugeben ist, welche Kategorien von Daten bearbeitet werden. Es muss nicht jedes Datenfeld aufgeführt werden (allerdings wäre dies erlaubt). Dies soll es unter anderem ermöglichen einzuschätzen, wie heikel die Datenbearbeitung ist. Werden besonders heikle Daten bearbeitet, sollte dies also an der Beschreibung erkennbar sein.

- ☐ Name, Titel
- ☐ Geburtstag
- ☐ Zivilstand
- ☐ Nationalität
- ☐ Arbeitgeber
- ☐ Angaben aus CVs
- ☐ Kontoverbindungen
- ☐ Persönliche Vorlieben
- ☐ Korrespondenz
- ☐ Opt-ins / Opt-outs
- ☐ Kontaktdaten, Wohnsitz
- ☐ Geschlecht
- ☐ Sprache
- ☐ Identifikatoren (AHV-Nr. etc.)
- ☐ Aus- und Weiterbildung
- ☐ Buchungen, Transaktionen
- ☐ Angaben zu Familie, Ehepartner
- ☐ Teilnahmen an Anlässen
- ☐ Verträge und Vertragsdaten
- ☐ Bonität
- ☐ Gesundheitsdaten (Krankheiten, Allergien, Behinderung, etc.)
- ☐ *Permanent Cookies*
- ☐ Biometrische Erkennungsdaten
- ☐ Login-Daten
- ☐ Server-Logs, IP-Addressen
- ☐ Andere:

- ☐ Gemäss Beilage

- ☐ Bemerkungen:
- ☐ Situation unklar

  Grund:

  - ☐ Weitere Abklärungen sind nötig
  - ☐ Experte konsultieren

Q7	**Kategorien der Empfänger** Anzugeben ist, wem Daten bekanntgegeben werden oder wer darauf Zugriff erhält. Die Kategorien können sehr allgemein gehalten werden. Die Identität der Empfänger muss im Inventar nicht angegeben werden. Im Inventar sind sowohl solche Stellen aufzuführen, welche die Daten für eigene Zwecke erhalten (d.h. die als Verantwortliche gelten) als auch die Tatsache, dass Auftragsbearbeiter die Daten erhalten, obwohl diese datenschutzrechtlich an sich nicht als Dritte gelten. Es sind auch jene Stellen zu nennen, die nur ausnahmsweise Zugang erhalten (nicht aber Fälle, in denen das Unternehmen behördlich oder gerichtlich zur Herausgabe von Daten gezwungen werden könnte, sie diese Daten von sich aus aber nicht zugänglich machen würde).	☐ Andere Gruppengesellschaften (die Verantwortliche sind) ☐ Auftragsbearbeiter (auch gruppeninterne) ☐ Behörden ☐ Kunden ☐ Lieferanten ☐ andere Geschäftspartner ☐ Öffentlichkeit ☐ Andere: [ ]	☐ Bemerkungen [ ] ☐ Situation unklar Grund: [ ] ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren
Q8	**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). Sie gelten als "sichere" Staaten, alle anderen als "unsichere".	☐ 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 die Schweiz ☐ In folgende Länder: [ ] *Falls DSG anwendbar:* ☐ Die Übermittlung in unsichere Drittstaaten wird abgesichert durch: ☐ Einen völkerrechtlichen Vertrag ☐ Dem EDÖB mitgeteilte vertragliche Datenschutzklauseln ☐ Dem EDÖB mitgeteilte behördliche Datenschutzgarantien	☐ Bemerkungen: [ ] ☐ Situation unklar Grund: [ ] ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren

		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. Aus Sicht der Schweiz sind alle Staaten ausser der Schweiz Drittstaaten. 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 Instrumente (z.B. Datenübermittlungsvertrag) zum Einsatz kommen, um trotz fehlendem gesetzlichen Datenschutz 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. Es kann natürlich sein, dass ein Unternehmen hier nichts ausfüllen kann, weil es keine Vorkehrungen getroffen hat. Das ist dann im Rahmen der Beurteilung von Formular E.2 zu berücksichtigen. Dort wird die Frage nach der Sicherstellung des Datenschutzes bei Exporten ebenfalls thematisiert.	☐ Vom EDÖB oder der EU genehmigte BCR ☐ EU- oder andere vom EDÖB akzeptierte Standardvertrags-klauseln ☐ Wir haben eine Absicherung, aber dem EDÖB wurde sie nicht gemeldet bzw. nicht von ihm genehmigt ☐ Die Übermittlung in unsichere Drittstaaten erfolgt 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	

Q9

Fristen für die Löschung der diversen Kategorien der bearbeiteten Personendaten oder Kriterien zur Festlegung der Fristen

Im Inventar ist aufzuführen, wie lange im Rahmen der Datenbearbeitung die Daten (in nicht-anonymisierter Form) aufbewahrt oder sonst bearbeitet werden. Hintergrund der Regelung ist, dass Personendaten nur solange aufbewahrt werden dürfen, als dies für die Erfüllung des Zwecks nötig ist.

Relevant ist allerdings nur die Zeit, in welcher die

Daten personenbezogen sind, d.h. sie sich auf eine bestimmte oder bestimmbare Person beziehen lassen. Sobald die Daten anonymisiert sind (was irreversibel geschehen muss), gelten sie nicht mehr als Personendaten. Sie können dann ewig aufbewahrt und vom Datenschutz ungeachtet genutzt werden. Zu beachten ist, dass die Anonymisierung so gut sein muss, dass eine Reidentifikation später nicht doch möglich ist, weil die Personen im Datenpool mit Hilfe weiterer Daten doch möglich wird.

Die meisten Unternehmen bewahren ihre Daten länger auf als gesetzlich erlaubt bzw. können ihre Daten gar nicht wirklich löschen, wenn sie sie nicht mehr benötigen. In diesen Fällen sind entsprechende Massnahmen zu treffen oder zu begründen, warum dies so gerechtfertigt ist (dazu dient das → Formular E.1). Hier ist anzugeben, wie die Situation tatsächlich ist. Zu beachten ist allerdings, dass die Aufsichtsbehörden dieses Inventar herausverlangen können.

☐ Die Daten werden normalerweise gelöscht nach:

☐ 3 ☐ 6 M. ☐ 1 ☐ 2 ☐ 5 ☐ 10 ☐ 20 J.

- ☐ Nachdem wir sie erhalten/erstellt haben
- ☐ Nach Vertragsende
- ☐ Nach Fall- bzw. Projektende
- ☐ Nach dem Geschäftsjahr, in dem sie angefallen sind

☐ Anderen Regeln:

☐ Die Daten werden nicht gelöscht oder jedenfalls nicht systematisch.

- ☐ Die Daten werden jedoch archiviert und der Zugriff darauf wird eingeschränkt auf jene, die die Daten brauchen.
- ☐ Wir müssen die Daten aufbewahren, solange das Unternehmen existiert.
- ☐ Weil wir es technisch nicht können.
- ☐ Weil wir es nicht wollen.
- ☐ Anderer Grund:

☐ Für bestimmte Daten gelten abweichende Regeln:

☐ Bemerkungen:

☐ Situation unklar

Grund:

- ☐ Weitere Abklärungen sind nötig
- ☐ Experte konsultieren

		Anzugeben ist, wie lange die Daten aufbewahrt werden. Ist eine konkrete Dauer nicht möglich, kann auch angegeben werden, nach welchen Kriterien bestimmt wird, wie lange Daten aufbewahrt bzw. nach welchen Kriterien sie gelöscht werden. Die Angaben beziehen sich auf die "Hauptdaten" der Bearbeitung. Wenn für bestimmte andere Daten der Datenbearbeitung längere oder kürzere Fristen gelten, kann dies ebenfalls vermerkt werden.	☐ Es ist bei uns anders: [ ]	
	Q10	**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 (gemeinsamer Zugangscode) ☐ Passwortschutz (Login pro Benutzer) ☐ Daten werden verschlüsselt gespeichert ☐ Daten werden verschlüsselt übermittelt ☐ Daten sind pseudonymisiert ☐ Protokollierung der 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	☐ Bemerkungen: [ ] ☐ Situation unklar Grund: [ ] ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren

		☐ Systemkonfiguration wurde fachmännisch auf Sicherheit geprüft ☐ Instruktion der Mitarbeiter betr. Datensicherheit ☐ Speicherung in der Cloud (Betreiber des Dienstes gewährleistet die Datensicherheit) ☐ Es bestehen keine besonderen Massnahmen zur Datensicherheit	

Weitere Bemerkungen:
