Allgemeine Angaben – Datenschutz-Governance

Formular A.2

Unternehmenseinheit: _____ Ausgefüllt von: _____ Stand vom: _____

Arbeitsanweisung:

Auf diesem Formular werden die wichtigsten, im Unternehmen vorhandenen Instrumente der Datenschutz-Governance erfasst und dokumentiert. Eine Beurteilung dieser Instrumente erfolgt im Rahmen dieses Formulars jedoch noch nicht. Dies ist Gegenstand anderer Formulare. Das Formular ist entsprechend dem aktuellen Stand auszufüllen.

Q1	**Interne Weisungen und andere interne Leitlinien zum Datenschutz (genereller Natur)** Will ein Unternehmen Datenschutz betreiben, muss es den Mitarbeitern Vorgaben machen, wie sie mit Personendaten umzugehen haben. Hierzu ist mindestens eine unternehmensweite Datenschutzrichtlinie oder -weisung erforderlich, welche die Grundsätze des Datenschutzes erklärt und den Mitarbeitern auferlegt. In → Formular F.3 kann geprüft werden, ob die Weisungen die nötigen Inhalte aufweisen.	☐ Wir haben keine Weisungen etc. zum Datenschutz ☐ Folgende Weisungen regeln den Datenschutz in genereller Weise (d.h. ohne fachbereichsspezifische Weisungen): ☐ Gemäss Beilage ☐ Es sind dies Vorgaben von der Gruppe	Überprüfung mit → Formular F.3

Q2	**Interne Weisungen und andere interne Leitlinien zur Datensicherheit** 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. Technische Massnahmen sind z.B. die Verschlüsselung bzw. Pseudonymisierung, Zugang nur mit persönlichem Login, Firewalls, Protokolle. Organisatorische Massnahmen sind Weisungen, Schulungen, Audits, Kontrollen. Die Datensicherheit ist als eher technische Disziplin meist getrennt vom Datenschutz geregelt. Auch Unternehmen, die keine Datenschutzweisungen haben, haben oft Weisungen zur IT-Sicherheit, zum Business Continuity Management, zur Verwendung von Internet oder zur Vertraulichkeit von Dokumenten.	☐ Wir haben keine Weisungen etc. zur Datensicherheit ☐ Folgende Weisungen etc. regeln die Datensicherheit im Unternehmen: ☐ Gemäss Beilage ☐ Es sind dies Vorgaben von der Gruppe	
Q3	**Datenschutzerklärung(en)** Jedes Unternehmen muss die betroffenen Personen, über die es Daten bearbeitet, über diese Bearbeitungen informieren. Dazu werden Datenschutzerklärungen verwendet. Häufig wird zwischen Datenschutzerklärungen an die Adresse der eigenen Mitarbeiter und solchen für Kunden und andere Dritte unterschieden. Ob für die einzelnen Datenbearbeitungen die nötigen Datenschutzerklärungen bestehen, wird im Rahmen des Compliance Checks der einzelnen Datenbearbeitungen mit → Formular E.1 geprüft.	☐ Wir haben keine Datenschutzerklärung ☐ Wir haben Datenschutzerklärung(en) ☐ Auf unserer Website: ☐ Auf unserem Intranet: ☐ In unseren Vertragsunterlagen ☐ In unseren Lokalitäten ☐ Gemäss Beilage	Überprüfung mit → Q7 + Q24 in Formular E.1

Q4	**Gruppen-interne Verträge zum Datenschutz bzw. zur Datenbekanntgabe und Auslagerung** Werden Daten zwischen verschiedenen Unternehmen oder grenzüberschreitend (auch innerhalb desselben Unternehmens) bekanntgegeben, so erfordert dies unter dem DSG und der DSGVO gewisse Vorkehrungen. Das gilt auch innerhalb einer Unternehmensgruppe. Unter verbundenen Unternehmen wird häufig auf Intra Group Data Transfer Agreements (IGDTA) zurückgegriffen, die alle Gruppengesellschaften unterzeichnen und die den Datenfluss innerhalb der Gruppe datenschutzkonform regeln.	☐ Wir haben keine Gruppen-interne Verträge zum Datenschutz. ☐ Wir haben folgende Gruppen-internen Verträge: ☐ Wir haben ein multilaterales, gruppenweites Vertragswerk für diesen Zweck ☐ Gemäss Beilage	Überprüfung mit → Q16 + Q20 in Formular E.1 und mit → Formular F.1
Q5	**Binding Corporate Rules (BCR)** BCR sind eine Spezialvariante gruppen-interner Verträge zur Regelung des gruppeninternen Datenflusses. Sie sind deshalb speziell, weil hierfür nicht die von der Europäischen Kommission verwendeten Musterklauseln zur Regelung des grenzüberschreitenden Datenflusses verwendet werden, sondern individualisierte Regelungen. Damit sind individuellere, flexiblere Verträge möglich. Allerdings hat dies zur Folge, dass solche BCR von den zuständigen EU-Datenschutzbehörden genehmigt werden müssen (und ggf. auch vom EDÖB).	☐ Wir haben keine BCR ☐ Wir haben folgende BCR: ☐ Sie sind vom EDÖB genehmigt ☐ Sie sind von den EU-Datenschutzbehörden genehmigt ☐ Gemäss Beilage	Überprüfung mit → Q16 in Formular E.1

Q6	**Schulung zum Datenschutz** Weisungen zum Datenschutz (und zur Datensicherheit) alleine genügen unter Umständen nicht. Je nach Vorwissen, Erfahrung und vorbestehender Sensibilisierung und dem mit den Datenbearbeitungen des Unternehmens verbundenen Risiken müssen Mitarbeiter (und weitere beigezogene Dritte) im Umgang mit Personendaten auch geschult werden. Sie müssen verstehen, was sie mit Personendaten tun dürfen und wie sie auf Anfragen von betroffenen Personen reagieren sollten.	☐ Jeder Mitarbeiter muss sich einer Datenschutzschulung unterziehen. ☐ Mitarbeiter in gewissen Bereichen müssen sich einer Datenschutzschulung unterziehen: ☐ Wir haben ein Datenschutz-Schulungs-Konzept: ☐ Gemäss Beilage ☐ Keine nennenswerte Schulung	Überprüfung mit → Formular D.2/D.3
Q7	**Überprüfung der Einhaltung des Datenschutzes** Nebst dem Erlass von Weisung, der Schulung der Mitarbeiter (und beigezogener Dritter) kann es je nach Risiko der Datenbearbeitung und weiteren Faktoren wie die Grösse des Unternehmens und Qualifikation der Mitarbeiter auch angezeigt sein, die Einhaltung des Datenschutzes auch ohne konkreten Anlass zu überprüfen. Im Falle eines Verdachts auf eine Verletzung des Datenschutzes sollte eine Überprüfung in jedem Fall vorgesehen sein.	☐ Die Einhaltung des Datenschutzes wird von Zeit zu Zeit durch die interne Revision als eines von vielen Themen überprüft. ☐ Wir prüfen die Einhaltung des Datenschutzes eigenständig durch: ☐ Regelmässige Audits ☐ Stichprobenweise Kontrollen ☐ Vorab-Kontrollen ☐ Kontrollen auf Verdacht hin ☐ Es erfolgt keine nennenswerte Überprüfung	Überprüfung mit → Formular D.2/D.3

	Q8	**Datenschutz-Zertifizierung** Das DSG wie auch die DSGVO sehen vor, dass ein Unternehmen gewisse oder alle Prozesse mit Bezug auf die Einhaltung des Datenschutzes zertifizieren lassen kann (zertifiziert wird diesfalls das Datenschutz-Management-System des Unternehmens). Es gibt auch einige private, nicht regulierte Zertifizierungen im Bereich Datenschutz. Zertifizierungen im Bereich Datenschutz sind mit ganz wenigen Ausnahmen (in der Schweiz z.B. im Bereich des KVG) rechtlich nicht vorgeschrieben. Datenschutz-Zertifizierungen sind bisher eher selten. Davon zu unterscheiden sind Zertifizierungen im Bereich der Datensicherheit, wie z.B. nach ISO 27001. ISO 27001 ist heute ein de-facto-Standard im Bereich von Anbietern von IT-Dienstleistungen.	☐ Wir verfügen über keine Datenschutz-Zertifizierung ☐ Wir verfügen jedoch über Zertifizierungen im Bereich der Datensicherheit (z.B. ISO 27001). ☐ Wir verfügen in folgenden Bereichen über eine Datenschutz-Zertifizierung: ☐ Gemäss Beilage	

Q9	**Vertraulichkeitserklärungen durch Mitarbeiter mit Zugang zu Personendaten** Die Wahrung der Vertraulichkeit von Personendaten ist ein Aspekt des Datenschutzes. Weder DSG noch DSGVO schreiben ausdrücklich vor, dass Mitarbeiter zur Vertraulichkeit verpflichtet werden müssen (Ausnahme: Verträge mit Auftragsbearbeitern müssen dies gemäss Art. 28 DSGVO vorsehen). Wird Mitarbeitern Zugang zu etwas heikleren Personendaten gewährleistet, kann es angezeigt sein, sie ausdrücklich zur Geheimhaltung zu verpflichten. Das Schweizer Arbeitsrecht wie auch das DSG verpflichtet Arbeitnehmer allerdings bereits in weiten Bereichen zur Geheimhaltung, so dass eine separate Erklärung nur dort sinnvoll erscheint, wo dies von Kunden verlangt wird oder es um besonders heikle Daten geht und es daher angezeigt ist, die Mitarbeiter an ihre Geheimhaltungspflicht zu erinnern. Das gilt auch in Fällen, in denen das Schweizer Recht ein spezielles Berufsgeheimnis vorsieht (z.B. Ärzte, Revisoren, Anwälte, Banken, Sozialversicherung). Nicht zu vergessen ist die Verpflichtung zur Geheimhaltung im Falle des Beizugs von Dritten. Wird einem Unternehmen und seinen Mitarbeitern Zugang zu eigenen Daten gewährt, kann es sinnvoll sein, von den Mitarbeitern des Dritten eine Geheimhaltungserklärung zu verlangen (die allerdings nicht kundenspezifisch sein muss).	☐ Die Arbeitsverträge der Mitarbeiter enthalten grundsätzlich eine Geheimhaltungsklausel. ☐ Gilt nur für folgende Bereiche: ☐ Gemäss Beilage ☐ Gilt analog für "externe" Mitarbeiter mit Zugang ☐ Gilt analog für Besucher mit Zugang ☐ Die Mitarbeiter müssen grundsätzlich eine separate Geheimhaltungserklärung unterzeichnen. ☐ Gilt nur für folgende Bereiche: ☐ Gemäss Beilage ☐ Gilt analog für "externe" Mitarbeiter mit Zugang ☐ Gilt analog für Besucher mit Zugang ☐ Die Mitarbeiter unterstehen bezüglich der Personendaten einer gesetzlichen Geheimhaltungspflicht. ☐ Gilt nur für folgende Bereiche: ☐ Gilt analog für "externe" Mitarbeiter mit Zugang ☐ Gilt analog für Besucher mit Zugang ☐ Die Mitarbeiter sind nicht zur Geheimhaltung verpflichtet.	Überprüfung mit → Formular F.2

Weitere Bemerkungen: