Compliance Check III – Weisungswesen

Formular F.3

Unternehmenseinheit: _____ Ausgefüllt von: _____ Stand vom: _____

Unterbereich(e) der Unternehmenseinheit: _____

Die Verantwortung für die Richtigkeit und Vollständigkeit der Angaben und der Entscheide in dieser Prüfung des Weisungswesens tragen:

☐ Ich/wir
☐ Folgende Person/en (Name, Kontakt, Thema): _____

Arbeitsanweisung:

- Dieses Formular dient dazu, das **Weisungswesen** des Unternehmens mit Bezug auf den Datenschutz zu beurteilen. Da es innerhalb ein- und derselben Unternehmenseinheit unterschiedlich ausgestaltet sein kann, kann das Formular für einzelne **Unterbereiche** separat ausgefüllt werden. Die grundsätzlichen Bemerkungen von Formular E.1 zur Methodik gelten auch hier.

- Die Beurteilung funktioniert so, dass in der mittleren Spalte die Bereiche und Themen aufgezählt werden, bei denen sich das Unternehmen fragen sollte, **ob die Mitarbeiter wissen, wie sie sich in der jeweiligen Situation verhalten sollten**. In einem kleinen Betrieb kommen gewisse Situationen (z.B. Löschgesuche) unter Umständen gar nie vor, dann braucht sich der Betrieb damit auch nicht unbedingt "auf Vorrat" auseinanderzusetzen. In gewissen Betrieben genügt es, die Themen vorab zu besprechen oder die Zuständigkeiten festzulegen, damit sich der Verantwortliche damit auseinandersetzen kann. In grösseren Betrieben wird es nötig sein, die für die Mitarbeiter wichtigsten Punkte schriftlich festzuhalten oder sogar detailliert darzulegen. Bei vielen Personen oder komplexen Verhaltensregeln kann schliesslich auch eine Schulung angezeigt sein. Die Spannbreite ist gross.

- Mit dem Formular kann nicht beurteilt werden, ob diese Weisungen inhaltlich korrekt und angemessen sind. Es kann lediglich geprüft werden, **ob die typischen Themen berücksichtigt** wurden – sofern sie überhaupt im Einzelfall von Relevanz sind, was nicht zwingend der Fall ist. Q2 und Q3 sind daher *optional* und eher für grössere Unternehmen gedacht. So gesehen hat dieses Formular eher die Funktion einer Checkliste von Themen, die bei der Ausgestaltung von Reglementen, Richtlinien und Weisungen zum Datenschutz berücksichtigt werden sollen. Das Formular gibt daher auch nicht vor, wie die Themen im Unternehmen adressiert werden müssen; das Gesetz verlangt lediglich, dass dies in angemessener Form geschieht. Der Vorteil der schriftlichen Weisung ist freilich, dass sie dokumentiert ist.

		Anforderung	Anforderung erfüllt?	Was zu tun ist
	Q1	**Grundweisung und -schulung zum Datenschutz** Die Mitarbeiter haben ein grundsätzliches Verständnis über die Anforderungen des Datenschutzes und wissen ungefähr, welche Regeln sie im eigenen Umgang mit Personendaten zu beachten haben bzw. wo sie sich erkundigen können. Falls sie nicht selbst dafür zuständig sind, wissen sie, wohin sie sich in speziellen Fällen wie Begehren von betroffenen Personen, Datensicherheitsverletzungen oder neuen, datenschutzrelevanten Vorhaben wenden müssen. Die internen diesbezüglichen Zuständigkeiten sind klar oder geregelt. *Art. [6] f. DSG, Art. 5 Abs. 2, Art. 24 f., Art. 32 DSGVO* Es genügt nicht, die diversen Datenbearbeitungen auf ihre Konformität mit dem Datenschutz hin zu beurteilen oder zu strukturieren. Eine zentrale Anforderung zur Sicherstellung des Datenschutzes ist auch die relevanten Mitarbeiter wissen, was sie mit den Daten tun dürfen und was nicht aus Sicht des Datenschutzes. Das Gesetz definiert nicht, wie das zu geschehen hat. Es hängt letztlich auch stark von der Unternehmensgrösse, -art und -kultur ab, wie es geschieht. Ein kleiner Betrieb wird nichts oder nur wenig schriftlich haben; alles andere wäre oft ein Overkill. Es kann ohne Weiteres genügen, dass eine zuständige Person (z.B. auch der Geschäftsführer) sich mit dem Thema beschäftigt und seinen Mitarbeitern situativ die entsprechenden Anweisungen erteilt, oder dass eine Gruppe von Mitarbeitern das Thema gemeinsam erarbeitet. Eine Weisung braucht es in	*Kurz und bündig:* ☐ Wir haben eine DSGVO-konforme, allgemeine Datenschutzweisung, alle relevanten Mitarbeiter werden im Umgang mit Personendaten geschult, und die Verantwortlichkeiten für den Datenschutz sind bei uns klar geregelt. → **hier alles OK** ☐ Bei uns wissen vielleicht einzelne Leute, was zu tun ist, aber obwohl wir mit Personendaten zu tun haben, war Datenschutz bei uns im Betrieb bisher kein Thema und die Mitarbeiter wissen auch nicht, wie damit umgehen. Wir haben uns um das Thema bisher nicht wirklich gekümmert. *Im Detail:* ☐ Wir haben uns bzw. **unsere Mitarbeiter** über folgende Punkte **sensibilisiert** und soweit erforderlich instruieren lassen bzw. **instruiert**, wie damit im Rahmen der bei uns praktizierten Datenbearbeitungen umzugehen ist: → **1. OK** ☐ **Anwendungsbereich** des Datenschutzes (Bearbeiten von Personendaten). ☐ Welche **Bearbeitungsgrundsätze** gelten und was sie bedeuten. ☐ Wann es welche **Rechtsgrundlage** braucht *(nur DSGVO und Bundesorgane gemäss DSG).* ☐ Welche **Betroffenenrechte** es gibt und wie sie einzuhalten sind: ☐ Informationspflicht bei der Datenbeschaffung. ☐ Auskunftsrecht. ☐ Berichtigungsrecht. ☐ Lösch- und Widerspruchsrecht. ☐ Recht auf Datenübertragbarkeit *(nur DSGVO).* ☐ Recht, nicht einem automatisierten Einzelentscheid unterworfen zu sein. ☐ Unter welchen Bedingungen Personendaten **ins Ausland bekanntgegeben** werden dürfen.	☐ Wir sehen **keinen Handlungsbedarf**, da wir die Anforderung grundsätzlich erfüllen. ☐ Optimierungsbedarf gibt es immer, aber darum werden wir uns bei Gelegenheit kümmern. Für den Moment sollten wir hinreichend aufgestellt sein. ☐ Wir sehen **Handlungsbedarf**, da wir die Anforderung in relevanten Punkten nicht oder nicht so erfüllen, wie wir das für nötig erachten: ☐ Wir sollten eine Datenschutzweisung erstellen lassen. ☐ Wir sollten eine Schulung entwickeln (oder einkaufen) und in das Programm für unsere Mitarbeiter aufnehmen. ☐ Wir sollten eine passende externe Schulung suchen und die relevanten Mitarbeiter dorthin schicken. ☐ Wir sollten mit den Mitarbeitern einen Workshop zum Datenschutz machen, damit sie sensibilisiert sind. ☐ Wir sollten die nötigen Verantwortlichkeiten intern festlegen, insbesondere zu folgenden Themen: ☐ Wir sollten jemandem bestimmen, der sich in das Thema einarbeitet und uns so intern helfen kann, mit den diversen Themen umzugehen. ☐ Wir sollten jemanden extern finden, an den wir uns bei Bedarf kurzfristig wenden können, wenn wir Fragen haben oder sonst Unterstützung brauchen. ☐ Andere Massnahme:

		diesen Fällen oft nicht, wenn allen klar ist, was zu tun ist. In einem etwas grösseren Betrieb wird es wiederum schon aus organisatorischen Gründen erforderlich sein, die nötigen Regeln schriftlich vorzugeben, damit sie dokumentiert, aber auch für alle einheitlich zugänglich sind. Eine Dokumentation hat auch den Vorteil, dass damit eine erteilte Weisung belegt werden kann, sollte sich ein Mitarbeiter in einem konkreten Fall nicht daran halten. Allgemein wird empfohlen, dass ein Unternehmen aber einer gewissen Grösse eine "Grundweisung" zum Datenschutz hat, in welcher die Vorgaben des Datenschutzes in Grundsätzen dargelegt werden, die der Arbeitgeber im Rahmen seines Weisungsrechts seinen Angestellten auferlegt. Diese Weisung muss nicht Teil des Arbeitsvertrags sein; es genügt, sie den Mitarbeitern aufzuerlegen. Weiter wird mit wachsender Grösse und Breite der Arbeitnehmerschaft empfohlen, diese über entsprechende Schulungen zu sensibilisieren, namentlich dort, wo nicht erwartet werden kann, dass diese sich mit den Weisungen von sich aus auseinandersetzen oder sie verstehen. Weisungen sollten und können auch dazu benutzt werden, interne Zuständigkeiten festzulegen (z.B. wer für die Beantwortung von Auskunftsersuchen verantwortlich ist). Dies kann mehr oder weniger aufwändig ausgestaltet sein. Die Grundweisung in einem Konzern wird typischerweise vorsehen, wie der Datenschutz konzernweit organisiert ist und entsprechend diverse Funktionen und Verantwortlichkeiten definieren. In einem mittleren Betrieb wird sich Grundweisung möglicherweise darauf beschränken festzuhalten, dass es eine interne Stelle gibt, die für alle Datenschutzfragen zuständig ist und direkt an das Management berichtet. Weisungen dienen schliesslich auch dazu, die Einhaltung des Datenschutzes zu dokumentieren. Es ist zwar immer möglich, dass Mitarbeiter sich falsch verhalten. Wenn das Unternehmen aber zeigen kann, dass es sie richtig unterwiesen hat, mildert	☐ Welche Massnahmen beim Beizug von Dienstleistern, insb. zur **Auftragsbearbeitung**, zu treffen sind. ☐ Verhalten bei **Verletzungen der Datensicherheit**, damit das Unternehmen seinen Meldepflichten nachkommen kann. ☐ Vorgaben, damit das Unternehmen seinen Pflichten im Bereich der **Inventarisierung** seiner Datenbearbeitungen, der Durchführung von **Datenschutz-Folgenabschätzungen** und dem **Nachweis der Einhaltung** des Datenschutzes nachkommen kann. ☐ Möglichkeit von **Ausnahmen** von den oben erwähnten Regeln (insb. Bearbeitungsgrundsätze, Betroffenenrechte). ☐ **Verantwortlichkeiten** im Unternehmen für die vorstehenden Punkte und wo Fragen gestellt werden können. ☐ Einhaltung des Datenschutzes generell. ☐ Erledigung von Begehren von betroffenen Personen (z.B. Auskunftsersuchen, Löschgesuche, etc.), Behandlung von Beschwerden. ☐ Sicherstellung der Informationspflichten (insb. Datenschutzerklärung). ☐ Festlegung und Einhaltung der Datensicherheit. ☐ Meldepflichten von Verletzungen der Datensicherheit. ☐ Sicherstellung der Einhaltung des Datenschutzes beim Abschluss von Verträgen mit Dritten, die Zugang zu Personendaten erhalten können. ☐ Prüfung und Erfüllung der formalen Pflichten, wenn im Betrieb neue oder geänderte Datenbearbeitungen eingeführt werden sollen (Nachführung Inventar, Datenschutz-Folgenabschätzung, Beurteilung des Datenschutzes, etc.). ☐ Kommunikation mit Behörden, und – soweit relevant – dem Vertreter nach Art. 27 DSGVO und externen Datenschutzbeauftragten. ☐ Verantwortlich für Datenschutz-Governance (inkl. Weisungswesen).	☐ **Situation unklar** Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren

		das bereits massiv etwaige Folgen. Es stellt sich dann noch die Frage, ob die Einhaltung der Weisungen nicht hinreichend kontrolliert wurde (vgl. Q3).	☐ Folgende **weitere Punkte**: ☐ Wir haben dies auf folgende Weise getan: ☐ Durch eine allgemeine **Datenschutzweisung**. Wir gehen davon aus, dass die Mitarbeiter auch ohne Schulung damit umgehen können und sonst wissen, wo sie fragen müssen. → **2. OK** ☐ Durch eine **persönliche Instruktion**; der Erlass einer schriftlichen Weisung macht bei unserer Firmengrösse keinen Sinn. → **2. OK** ☐ Durch eine allgemeine **Datenschutzweisung** verbunden mit einer **Datenschutzschulung**, weil wir sonst nicht davon ausgehen können, dass die Weisung von allen verstanden oder zur Kenntnis genommen wird. → **2. OK** ☐ Wir haben **nichts davon, weil** eine schriftliche Weisung oder Datenschutzschulung uns bei unserem Betrieb als **Overkill** erscheint, aber folgende Kriterien sind erfüllt: → **2. OK** ☐ Die relevanten Personen haben sich mit dem Thema beschäftigt und sind daher **sensibilisiert**. Sie wissen auch, wohin sie sich bei Fragen wenden müssen. ☐ Es ist klar, wer für die einzelnen Punkte (wie z.B. Betroffenenrechte, Datensicherheit und Meldung deren Verletzung, Verträge mit Dienstleistern, Beurteilung neuer Projekte) **verantwortlich ist**. ☐ Bei uns ist **nicht sichergestellt**, dass die Personen, die mit Personendaten zu tun haben, wirklich wissen, was gilt oder an wen sie sich wenden können. ☐ Bei uns ist es anders:	

			☐ Wenn die Mitarbeiter bei uns bei einer Datenschutzfrage **nicht weiterwissen** (z.B. Umgang mit Auskunfts- oder Löschersuchen, Erstellung einer Datenschutzerklärung oder Vorliegen einer Datensicherheitsverletzung), dann haben wir: ☐ **Intern** eine Person, die über ein gewisses oder sogar gutes Datenschutz-Know-how verfügt und bei Bedarf weiss, wohin sie sich extern für Rat hinwenden kann. → **3. OK** ☐ **Extern** einen Berater, der über das erforderliche Datenschutz-Know-how verfügt, und an den wir uns kurzfristig wenden können, falls wir nicht weiterwissen. → **3. OK** ☐ **Extern** einen Rechtsberater, der sich über sein Netzwerk sicherlich das nötige Know-how beschaffen kann, falls er es nicht hat. → **3. OK** ☐ Niemanden, der uns weiterhelfen kann. ☐ Bei uns ist es anders: ☐ Wir möchten noch Folgendes vermerken:	
	Q2	*Optional:* **Spezialthemen zum Datenschutz** In den Bereichen, wo die Bearbeitung von Personendaten entweder mit besonderen Risiken für die betroffenen Personen verbunden sind oder die Anforderungen etwas komplexer sind, wissen die Mitarbeiter, wie sie sich aus der Sicht des Datenschutzes korrekt zu verhalten haben. Wo im Einzelfall nötig	☐ Unsere Mitarbeiter insbesondere im Personalwesen und Vorgesetzte wissen, was bei folgenden Punkten zum **Thema HR-Daten** (soweit für uns überhaupt relevant) von ihnen verlangt wird: → **1. OK** ☐ Umgang mit Daten von Bewerbern. ☐ Sicherheitsüberprüfungen (*Background Checks*). ☐ Führung der Personalakte, der Zugang dazu und die Rechte der Mitarbeiter (Auskunft, Berichtigung, Löschung). ☐ Beurteilungen durch Vorgesetzte und Kollegen. ☐ Prozesse beim Eintritt in das Unternehmen.	☐ Wir sehen **keinen Handlungsbedarf**, da wir die Anforderung grundsätzlich erfüllen. ☐ Optimierungsbedarf gibt es immer, aber darum werden wir uns bei Gelegenheit kümmern. Für den Moment sollten wir hinreichend aufgestellt sein. ☐ Wir sehen **Handlungsbedarf**, da wir die Anforderung in relevanten Punkten nicht oder nicht so erfüllen, wie wir das für nötig erachten: ☐ Wir sollten zu folgenden Themen eine Datenschutzweisung erstellen lassen: ☐ HR-Daten.

	und passend, ist dies mit Weisungen zu spezifischen Themenbereichen im Unternehmen konkret zu dokumentieren und es ist ggf. auch eine entsprechende Schulung vorzunehmen. *Art. [6] f. DSG, Art. 5 Abs. 2, Art. 24 f., Art. 32 DSGVO* Eine Grundweisung kann in aller Regel nur die allgemeinen Grundsätze (wie z.B. das Verbot der Zweckentfremdung von Daten oder die Informationspflicht) festhalten, aber nicht, wie sie im konkreten Alltag umzusetzen sind. In manchen, vor allem kleineren Unternehmen, braucht dies nicht formal geregelt und dokumentiert zu werden, wenn die Mitarbeiter wissen, was sie in den für sie relevanten Situation zu tun haben oder wissen, wo sie fragen können. Daher ist diese Anforderung als "optional" vermerkt. Sie richtet sich an Personen, die in oder für in der Regel etwas grössere Unternehmen oder Unternehmen in heiklen Bereichen weitergehende Weisungen aufbauen müssen, damit die Mitarbeiter vernünftig instruiert werden können. Dies muss für jeden Bereich, wo sich solche Fragen stellen, gesondert überprüft werden. Darum geht es hier. Die "Vorgaben" in der mittleren Spalte sind lediglich Erfahrungswerte und Anregungen. In jedem Unternehmen wird der Regelungsbedarf in einem bestimmten Bereich anders sein, gewisse Punkte fallen weg, andere kommen hinzu. Was schlussendlich wie schriftlich geregelt oder gar geschult werden muss, ist nach den Umständen zu beurteilen. Es sollte allerdings nicht übertrieben werden. Entscheidend ist nicht die Dokumentation, sondern die Beachtung des Datenschutzes in den diversen Themengebieten. Wichtig ist daher auch hier, dass ein vernünftiges Mass an Governance gewahrt wird. Weisungen sollen ein Hilfsmittel dazu sein, nicht ein Selbstzweck sein.	☐ Prozesse beim Austritt aus dem Unternehmen, inkl. Umgang mit privaten und geschäftlichen Daten des Mitarbeiters. ☐ Umgang mit Daten über Krankheiten und Gebrechen, Arztzeugnissen. ☐ Weitergabe von Daten an Versicherungen, Pensionskassen, Behörden. ☐ Weitergabe von Daten an andere Konzerngesellschaften (z.B. für internes *Career Development*) ☐ Weitergabe von Daten an Dritte, die Leistungen für Mitarbeiter erbringen (z.B. Vergünstigungen, Ausbildung, Kreditkarten, Mobiltelefonabos). ☐ Zuständigkeiten. ☐ Unsere Mitarbeiter insbesondere im Marketing und Verkauf wissen, was bei folgenden Punkten zum **Thema Marketing und Verkauf** (soweit für uns überhaupt relevant) von ihnen verlangt wird: → **2. OK** ☐ Voraussetzungen und Vorgaben für den Versand von Newslettern und Werbe-E-Mails, Umgang mit Beschwerden. ☐ Voraussetzungen und Vorgaben für Telefonwerbung, Umgang mit Beschwerden. ☐ Beschaffung von Daten über Kunden und prospektive Kunden, inkl. Einkauf und Abgleich von bestehenden Kundendaten (z.B. Adressen). ☐ Auswertung und Analyse von Kundendaten zwecks Marktforschung und Marketing, inkl. *Profiling* und personalisiertem Marketing und Voraussetzungen dafür. ☐ Veredelung von Adressen (z.B. durch Ergänzung mit Daten aus sozialen Medien, Adresshändler). ☐ Informationspflicht gegenüber betroffenen Personen, das Einholen von Einwilligungen. ☐ Führung des *Customer-Relation-Management*-Systems (CRM), wer es wozu nutzen darf. ☐ Datenbearbeitung an Messen und Veranstaltungen, Durchführung solcher Anlässe (z.B. Einladungen).	☐ Marketing und Verkauf. ☐ Betroffenenrechte. ☐ Datensicherheit, IT- und Internet-Nutzung. ☐ Kontrollen und Überwachung. ☐ Aufbewahrung (*Records Retention*). ☐ Meldung von Verletzungen der Datensicherheit. ☐ Einführung neuer oder geänderter Datenbearbeitungen. ☐ Andere: ☐ Wir sollten die Schulung unserer Mitarbeiter zu folgenden Themen vorsehen bzw. ausbauen: ☐ HR-Daten. ☐ Marketing und Verkauf. ☐ Betroffenenrechte. ☐ Datensicherheit, IT- und Internet-Nutzung ☐ Kontrollen und Überwachung. ☐ Aufbewahrung (*Records Retention*). ☐ Meldung von Verletzungen der Datensicherheit. ☐ Einführung neuer oder geänderter Datenbearbeitungen. ☐ Andere: ☐ Wir sollten unsere Weisungen der folgenden Bereichen daraufhin prüfen, ob sie noch den heutigen Anforderungen entsprechen:

☐ Auskunfts-, Berichtigungs- und Löschgesuche von betroffenen Personen.

☐ Markt- und Medienbeobachtung.

☐ Zusammenstellen von Dossiers über Kunden und prospektive Kunden aus öffentlichen und anderen Quellen.

☐ Betrieb der Website, Tracking der Benutzer, Einsatz von *Cookies* zu anderen als rein funktionalen und betrieblichen Zwecken.

☐ Zuständigkeiten.

☐ Unsere Mitarbeiter insbesondere im Kundendienst und der Informatik wissen, was bei folgenden Punkten zum **Thema Betroffenenrechte** (soweit für uns überhaupt relevant) von ihnen verlangt wird: → **3. OK**

☐ Auskunftsrecht.

☐ Berichtigungsrecht.

☐ Löschrecht, Recht auf Vergessen.

☐ Sperr- und Beschränkungsrecht, sonstige Widerspruchsrechte.

☐ Gesetzliche Ausnahmetatbestände (z.B. Schutz von Geschäftsgeheimnissen, Schutz von Dritten).

☐ Umgang in der Praxis (z.B. Identifikation, Fristen, Kostenpflicht, Schwärzungen, Form der Auskunft und Berichtigung, Protokollierung, etwaige Standardformulierungen).

☐ Pflicht zur Mitteilung an Dritte oder Offenlegung von Dritten.

☐ Zuständigkeiten.

☐ Unsere Mitarbeiter wissen, was bei folgenden Punkten der Themen **Datensicherheit** und **IT- und Internet-Nutzung** (soweit für uns überhaupt relevant) von ihnen verlangt wird: → **4. OK**

☐ Verhalten zur Gewährleistung der Datensicherheit (z.B. Verwendung von Speichermedien, Sicherung von Notebooks, Umgang mit Akten ausser Haus, Einsatz privater Mail-Accounts, Umgang mit Schlüsseln, Badges und Zugangscodes und Verhalten bei Verlust).

☐ HR-Daten.

☐ Marketing und Verkauf.

☐ Betroffenenrechte.

☐ Datensicherheit, IT- und Internet-Nutzung.

☐ Kontrollen und Überwachung.

☐ Aufbewahrung (*Records Retention*).

☐ Meldung von Verletzungen der Datensicherheit.

☐ Einführung neuer oder geänderter Datenbearbeitungen.

☐ Andere:

☐ Wir sollten die nötigen Verantwortlichkeiten intern festlegen, insbesondere zu folgenden Themen:

☐ Andere Massnahme:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

		☐ Verhalten zur Wahrung von Geschäftsinteressen (z.B. Vermeidung von Gesetzesverletzungen, Belästigung, Rufschädigung, Verlust von Geschäftsgeheimnissen). ☐ Umgang mit Mails und Dokumenten mit privaten Inhalten, auch, wo sie zu speichern sind, damit eine Überwachung der geschäftlichen Aktivitäten erleichtert wird. ☐ Einsatz privater Geräte (*"bring your own device"*), inkl. Zugriffsmöglichkeiten und Ortung durch den Arbeitgeber. ☐ Zugang zu Mails und Dokumenten bei Abwesenheit und im Notfall. ☐ Vorgaben wie Daten zu sichern sind, die Funktion der Sicherung getestet werden muss, und wie bei Personal- oder Systemausfällen kritische Funktionen weiterhin sichergestellt werden können (*Business Continuity Management*). ☐ Zuständigkeiten. ☐ Unsere Mitarbeiter insbesondere im Bereich der Informatik und Geschäftsführung wissen, was bei folgenden Punkten zum **Thema Kontrollen und Überwachung** (soweit für uns überhaupt relevant) von ihnen verlangt wird: → **5. OK** ☐ In welchen Fällen überwacht wird (Sicherheit, Schutz vor Verlust von Geschäftsgeheimnissen, Untersuchung bei geschäftlichem Fehlverhalten, etc.) ☐ Unter welchen Voraussetzungen und wie dies im Einzelfall geschehen kann (z.B. Verdacht, nicht-personenbezogene vs. personenbezogene Auswertung von Daten, automatische Alarm- und Filtersysteme). ☐ Welche Formen vorkommen (z.B. automatische Filterung von E-Mails, Aufzeichnung Internet-Verkehr, Aufzeichnung von Zugangskontrollsystemen, Kameras, Telefonaufzeichnungen, Sichtung von E-Mails und Dokumenten). ☐ Welche Rechte die betroffenen Personen haben (z.B. Auskunftsrecht, Gehörsrecht) und wie sie geschützt werden (z.B. Vorgaben für Sichtung von E-Mails, zum Aufstellen von Kameras, zur Protokollierung von Internet-Aktivitäten). ☐ Ob es eine Meldestelle für Unregelmässigkeiten gibt (Whistleblowing-Hotline), wie sie geregelt ist, was wie gemeldet werden kann, was mit den Meldungen geschieht und welche	

Rechte betroffene Personen haben (dieses Thema wird häufig separat geregelt).

- ☐ Zuständigkeiten.

☐ Unsere Mitarbeiter generell und insbesondere im Bereich der Informatik wissen, was bei folgenden Punkten zum **Thema Aufbewahrung (*Records Retention*)** (soweit für uns überhaupt relevant) von ihnen verlangt wird: → **6. OK**

- ☐ Grundlagen für die Aufbewahrung von Daten und Dokumenten (gesetzliche Anforderungen, vertragliche Pflichten, weitere Geschäftsinteressen).
- ☐ Aufbewahrungsfristen der diversen Daten- und Dokumentenkategorien, vorbehältlich abweichender Regelungen des lokalen Rechts.
- ☐ Wie nach Ablauf der Aufbewahrungsfrist oder sonst bei Nichtmehrgebrauch von Daten und Dokumenten vorzugehen ist (Löschung, zuverlässige Anonymisierung, datenschutzkonforme Entsorgung von Papierakten, etc.).
- ☐ Ausnahmen (z.B. *Legal Hold* im Falle einer gerichtlichen Auseinandersetzung oder behördlichen Untersuchung).
- ☐ Zuständigkeiten.

☐ Unsere Mitarbeiter generell und insbesondere im Bereich der IT-Sicherheit wissen, was bei folgenden Punkten zum **Thema Meldung von Verletzungen der Datensicherheit** (soweit für uns überhaupt relevant) von ihnen verlangt wird: → **7. OK**

- ☐ Was mit Verletzungen der Datensicherheit gemeint ist.
- ☐ Interne Meldepflicht für Vorfälle, Sammelstelle für solche Meldungen.
- ☐ Abklärung und Beurteilung eines Vorfalls (Einschätzung des Risikos, Hilfestellung zur Einschätzung).
- ☐ Vornahme von (Sofort-)massnahmen, um das Risiko aufgrund der Verletzung der Datensicherheit zu minimieren oder eliminieren.
- ☐ Entscheid über Meldungen an Behörden und Betroffene gemäss anwendbarem Datenschutzrecht.
- ☐ Durchführung der Meldung.

			☐ Zuständigkeiten. ☐ Unsere Mitarbeiter insbesondere im Bereich der Informatik und Produkteentwicklung wissen, was bei folgenden Punkten zum Thema **Einführung neuer oder geänderter Datenbearbeitungen** (soweit für uns überhaupt relevant) von ihnen verlangt wird: → **8. OK** ☐ In welchen Fällen diese Weisung beachtet werden muss und von wem (z.B. datenschutzrechtliche Vorprüfung von neuen Projekten, Entwicklung neuer Apps). ☐ Durchführung eines Compliance Checks (z.B. mit Formular E.1). ☐ Durchführung einer Datenschutz-Folgenabschätzung, soweit sie erforderlich ist (z.B. mit Formular G.1). ☐ Nachführung des Inventars der Datenbearbeitungen (z.B. mit den Formularen B.1 und B.2). ☐ Vorgaben an Entwickler, wie sie bei der Gestaltung von Software und anderen Produkten- und Dienstleistungen die Grundsätze *Privacy by Design* und *Privacy by Default* zu beachten haben. ☐ Zuständigkeiten. ☐ Unseren Mitarbeiter **fehlt** zu gewissen oder allen der oben genannten Themen klar **das erforderliche Wissen** darüber, was unser Unternehmen bzw. sie selbst zu tun haben, obwohl diese Themen für uns durchaus relevant sind. ☐ Wir möchten noch Folgendes vermerken:	
	Q3	*Optional:* **Einhaltung der Weisungen wird kontrolliert** Das Unternehmen kontrolliert, dass die Massnahmen und Verhaltensweisen, für	☐ Wir haben zur Ergänzung unserer Bemühungen im Bereich des Datenschutzes auch ein **Prüfkonzept** erstellt, in dessen Rahmen von Zeit zu Zeit überprüft wird, ob die Weisungen tatsächlich gelebt werden, sich nach wie vor eignen und ob und wo sie allenfalls verbessert werden können. → **hier alles OK**	☐ Wir sehen **keinen Handlungsbedarf**, da wir die Anforderung grundsätzlich erfüllen. ☐ Optimierungsbedarf gibt es immer, aber darum werden wir uns bei Gelegenheit kümmern. Für den Moment sollten wir hinreichend aufgestellt sein.

	die es sich entschieden hat, tatsächlich befolgt werden, es prüft deren Eignung und Wirksamkeit und es passt sie bei Bedarf an. *Art. [6] f. DSG, Art. 5 Abs. 2, Art. 24 f., Art. 32 DSGVO* Vorgaben zur Einhaltung des Datenschutzes genügen nicht, wenn sie nicht eingehalten werden oder ggf. nicht einmal mehr passen. Daher sollte ein Unternehmen sich auch Gedanken dazu machen, wie es diese beiden Dinge sicherstellen kann. Je grösser das Unternehmen, desto formalisierter sollte dieser Prozess abgewickelt werden. Hierbei kann und sollte die Revisionsstelle bzw. das Audit des Unternehmens eingebunden werden, soweit es den Punkt der Einhaltung des Datenschutzes nicht schon von sich aus auf dem Programm hat (wie das an sich nötig wäre). In der Praxis als sehr wirksam erwiesen hat sich, dass den Stellen, die den Datenschutz an der Front umsetzen müssen, konkrete Angaben gemacht werden, wie dies später überprüft wird, auch wenn ein Audit immer nur mit Stichproben arbeitet.	☐ Wir sind ein kleiner Betrieb. Wo wir uns Regeln auferlegt haben, halten wir diese auch ein, sonst macht das keinen Sinn. Wenn es mit einer Regel ein Problem gibt oder sonst Verbesserungsbedarf besteht, **merken wir das** und passen sie an. → **hier alles OK** ☐ Wir lassen unsere Datenschutzbemühungen regelmässig von einem **externen Experten** überprüfen, haben aber kein eigentliches Audit- oder sonstiges Prüfkonzept in diesem Bereich. → **hier alles OK** ☐ Wir haben zwar Weisungen, aber **wir wissen nicht**, ob und wie sie befolgt werden, und ob die Weisungen noch passend sind. ☐ Bei uns ist es anders: ☐ Wir möchten noch Folgendes vermerken:	☐ Wir sehen **Handlungsbedarf**, da wir die Anforderung in relevanten Punkten nicht oder nicht so erfüllen, wie wir das für nötig erachten: ☐ Wir sollten ein Konzept erarbeiten, wie wir sicherstellen wollen, dass unsere Weisungen im Bereich des Datenschutzes eingehalten und wenn nötig angepasst werden. ☐ Wir sollten unsere Weisungen daraufhin prüfen und ergänzen, dass sie selbst im operativen Bereich Massnahmen zur Kontrolle ihrer Einhaltung vorsehen (*1st line of defence*), regelmässig auf Eignung und Wirksamkeit überprüft werden (*2nd line of defence*), und das Audit all dies regelmässig unter die Lupe nimmt (*3rd line of defence*). ☐ Wir sollten vorsehen, dass ein Experte unsere Bemühungen im Bereich Datenschutz in regelmässigen Abständen unter die Lupe nimmt. ☐ Das sollte eine externe Person tun. ☐ Das sollte eine interne Person tun. ☐ Wir sollten vorsehen, dass ein Experte unsere Bemühungen im Bereich Datenschutz in regelmässigen Abständen unter die Lupe nimmt. ☐ Andere Massnahme: ☐ **Situation unklar** Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren

Weitere Bemerkungen: