Compliance Check II – Anforderungen an eine Datenbearbeitung (für Verantwortliche) — Formular E.1

Unternehmenseinheit: _____ Ausgefüllt von: _____ Stand vom: _____

Die nachfolgenden Ausführungen gilt für folgende Datenbearbeitung: _____ **DB-Nr:** _____

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

Weiterführende Angaben zur Umsetzung der Massnahmen können liefern (wo nachfolgend nicht anders angegeben):

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

Die Verantwortung für die Richtigkeit und Vollständigkeit der Angaben und die Entscheide in diesem Compliance Check tragen:

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

Für das Risikomanagement (siehe am Ende):

Die Datenbearbeitung betrifft folgende Prozesse: _____

Der oder die Eigner dieser Prozesse sind (Prozessowner): _____

Autor: David Rosenthal Alle Rechte vorbehalten. Fachredaktion: David Rosenthal (david.rosenthal@homburger.ch), David Vasella (david.vasella@walderwyss.com)
Dies ist keine Rechtsberatung. Für den Inhalt wird keine Gewähr übernommen. Nutzung auf eigene Gefahr. Lizenz: Creative Commons "Namensnennung – Keine Bearbeitungen 4.0 International"

Arbeitsanweisung:

- Das Formular funktioniert nach dem Prinzip der **Selbst-Deklaration**, analog der Steuererklärung. Jeder muss selbst entscheiden, wie genau er es nimmt und welchen Anspruch er hat, ist aber auch selbst für seine Deklaration und Einschätzung **verantwortlich**. Das Formular erlaubt dabei auch sehr pragmatische Einschätzungen.

- Das Formular dient dazu, den **"Ist"-Zustand der Datenschutz-Compliance** nach revidiertem DSG und DSGVO zu beurteilen und – wo sich eine Lücke (Gap) abzeichnet – etwaige Massnahmen zu deren Behebung zu ermitteln. Die Einhaltung des heutigen DSG wird mit anderen Worten gar nicht erst geprüft, sondern es wird direkt beurteilt, wie die **heutige Datenbearbeitung unter dem "neuen" Recht wäre**, damit festgestellt werden kann, wo Handlungsbedarf besteht.

- Für jede Anforderung ist daher in der **mittleren Spalte** anzugeben, wie es sich *im Moment* verhält mit Bezug auf die Datenbearbeitung, und zwar durch **Ankreuzen der betreffenden Aussagen** und Unteraussagen und Ausfüllen der Kommentarfelder. Dabei ist zu bedenken, dass die Prüfung im Hinblick auf die Situation unter den Anforderungen des neuen Rechts erfolgt.

- Die Aussagen **"Kurz und bündig"** und **"Im Detail"** sind gleichwertig. Bei Unsicherheit und wenn sich die Situation etwas differenzierter darstellt, sollte die Aussagen "Im Detail" gewählt werden, die den Sachverhalt etwas differenzierter und auf verschiedene Teilaspekte aufgebrochen aufgeteilt darlegen. Wer nicht weiterkommt, gibt dies in der rechten Spalte (**"Situation unklar"**) an und muss dies eskalieren (z.B. mit dem internen Datenschutzverantwortlichen oder Rechtsdienst besprechen).

- Darüber hinaus dient die **rechte Spalte** der -Beurteilung der momentanen Situation (wiederum im Hinblick auf die Lage unter dem "neuen" Recht), wobei das Formular Raum für risikobasierte Entscheide lässt.

- Bei jeder Anforderung ist es das **Ziel**, die vorgesehene Anzahl an OKs zu sammeln (1. OK, 2. OK, etc.). Liegen alle OKs vor, darf angenommen werden, dass die **Anforderung grundsätzlich erfüllt** ist. Das gilt auch, wenn mit einer Aussage ein "hier alles OK" erzielt wird (es darf dann zur nächsten Anforderung bzw. zur rechten Spalte gesprungen werden).

- Liegen nicht alle OKs vor, kann die Bearbeitung **trotzdem konform** sein, bedarf aber einer besonderen Beurteilung (vom internen Datenschutzverantwortlichen, dem Rechtsdienst oder einem externen Experten).

- Bei gewissen Aussagen wird auf separate, vertiefende Formulare verwiesen (z.B. was Rechtfertigungsgründe oder Auftragsdatenbearbeitungen betrifft).

Abgrenzungen: Folgende Datenbearbeitungen im Unternehmen …

☐ **machen sich Daten der hier beurteilten Datenbearbeitung zunutze** oder greifen sonst darauf zu, aber **wir blenden dies** für die vorliegenden Zwecke vollständig **aus** (d.h. gehen nicht darauf ein und erwähnen es nicht), weil diese Datenbearbeitungen separat beurteilt werden (Beispiel: Data-Mining-Anwendungen, die auf verschiedene Daten im Unternehmen zugreifen, um diese zu analysieren):

☐ Gemäss separater Liste: _____

☐ werden hier **als Datenquelle genutzt**, aber hier nicht weiter beurteilt (Beispiel: Verwaltung der Stammdaten von Kunden, die in diversen weiteren Bearbeitungsaktivitäten genutzt werden). Wir gehen für das vorliegende Formular davon aus, dass die Daten im Rahmen dieser Datenquellen **datenschutzkonform** bearbeitet werden (dass also z.B. die in der Stammdatenverwaltung bearbeiteten Daten, auf die hier zugegriffen wird, immer aktuell sind):

☐ **werden im Rahmen der vorliegenden Beurteilung vollständig ausgeblendet, weil sie IT- und andere Basisaktivitäten betreffen**, die auch diverse andere Datenbearbeitungen betreffen und aus Gründen der Effizienz separat und konsolidiert beurteilt werden (z.B. Betrieb und Wartung von IT-Systemen und Anwendungen, in deren Rahmen ebenfalls ein Zugriff auf die damit verwalteten Personendaten erfolgen kann):

☐ Gemäss separater Liste: _____

			Anforderung	Anforderung erfüllt?	Was zu tun ist
		Q1	**Grundsatz der Rechtmässigkeit** Es werden im Zusammenhang mit der Bearbeitung der Personendaten (auch) ausserhalb des Datenschutzes keine gesetzlichen Bestimmungen verletzt und es werden mit der Datenbearbeitung keine rechtswidrigen Zwecke verfolgt. *Art. [5] Abs. 1 DSG* Hintergrund dieser Regel ist, dass es immer auch eine Persönlichkeitsverletzung darstellt, wenn eine Datenbearbeitung auch andere Bestimmungen des Schweizer Rechts verletzt. Ist es einer Krankenkasse z.B. aufgrund des KVG nicht erlaubt, Versicherte unterschiedlich zu behandeln, so verletzt eine Datenbearbeitung, die genau darauf abzielt, nicht nur das KVG, sondern auch den Grundsatz der Rechtmässigkeit. Das Unternehmen sollte sich daher fragen, ob nicht nur das DSG eingehalten wird, sondern auch sonst nicht gegen eine Bestimmung des Schweizer Rechts verstossen wird.	*Kurz und bündig:* ☐ Ja, wir meinen, dass wir mit unserer Datenbearbeitung generell keine Norm des Schweizer Rechts verletzen; soweit für uns aufsichtsrechtliche Normen gelten, halten wir diese im Zusammenhang mit dieser Datenbearbeitung ein. → **hier alles OK** *Im Detail:* ☐ Wir erachten diese Anforderung als **erfüllt**, da wir meinen, dass wir uns im Rahmen unserer Datenbearbeitung im Wesentlichen an das **Schweizer Recht** halten, einschliesslich der auf uns anwendbaren Bestimmungen des Aufsichtsrechts. → **hier alles OK** ☐ Bestimmte Aspekte unserer Datenbearbeitung **verletzen** möglicherweise ausserhalb des Datenschutzes **bestehende rechtliche Bestimmungen** und Regelungen, bzw. wir benutzen die Datenbearbeitung für Dinge, mit denen wir möglicherweise andere Bestimmungen des Schweizer Rechts verletzen: ☐ Spezialgesetzliche Vorgaben, an die wir uns bei unserer Datenbearbeitung halten müssen. ☐ Vorgaben unserer Aufsichtsbehörde. ☐ Gleichbehandlungsgrundsatz (z.B. im Arbeitsrecht, KVG). ☐ Recht am eigenen Bild. ☐ Andere: [ ]	☐ Es sind unseres Erachtens **keine Massnahmen nötig:** ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt. ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist. ☐ Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr. _____ ☐ Anderer Grund: [ ] ☐ Es sind unseres Erachtens **folgende Massnahmen nötig:** ☐ Wir sollten abklären, was zur Einhaltung der möglicherweise verletzten Bestimmungen nötig ist und planen die Umsetzung dieser Schritte. ☐ Wir sollten die Datenbearbeitung so einschränken, dass ein Verstoss vernünftigerweise nicht mehr vorkommen sollte. ☐ Andere Massnahme: [ ]

				☐ Wir möchten noch Folgendes vermerken: ☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern: ☐ **Situation unklar** Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren ☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen ☐ Sollten wir weitermachen wie bisher. ☐ Treffen wir folgende Sofortmassnahmen: ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

Q2

Rechtsgrundlage (nur DSG)

Falls das Unternehmen bei der Datenbearbeitung als Bundesorgan im Sinne des DSG gilt:

Die Datenbearbeitung kann sich auf eine gesetzliche Grundlage des Schweizer Rechts stützen, im Falle eines Profilings (→ Glossar) oder bei besonders schützenswerten Personendaten (→ Glossar) muss das sogar ein Gesetz im formellen Sinn (→ Glossar) sein.

Art. [1] Bst. h DSG, Art. [30] DSG

Soweit das Unternehmen als Bundesorgan Personendaten bearbeitet, gelten für das Unternehmen die strengeren Vorschriften des DSG für Bundesorgane. Als solches gelten auch private Personen, die mit öffentlichen Aufgaben des Bundes betraut sind (z.B. Krankenkassen im Bereich der Grundversicherung).

Die strengeren Vorschriften sehen insbesondere vor, dass sich jede Bearbeitung direkt oder indirekt auf eine entsprechende Ermächtigung im Gesetz zurückführen lassen. Eine direkte Rechtsgrundlage ist eine Bestimmung in einem Gesetz (oder je nach Art der Daten auch sonstigen Erlass), der die Bearbeitung von Personendaten direkt regelt. Eine indirekte Rechtsgrundlage liegt vor, wenn die einschlägigen Erlasse nicht sagen, dass Personendaten bearbeitet werden dürfen, dies aber zur Erfüllung des Gesetzes zwingend erforderlich ist.

In der mittleren Spalte wird das Erfordernis der Rechtsgrundlage abgefragt. Die weiteren Anforderungen an Bundesorgane werden in diesem Formular E.1 nicht abfragt.

Wer als Bundesorgan tätig ist, sollte seine Gesetzesgrundlagen kennen; somit dürfte die Antwort auf

Kurz und bündig:

☐ Wir sind zwar ein privates Unternehmen, nehmen aber eine staatliche Aufgabe wahr und gelten daher für gewisse oder alle Datenbearbeitungen als Bundesorgan im Sinne des DSG. Die vorliegende Datenbearbeitung führen wir durch als:

- ☐ Bundesorgan (ausschliesslich)
- ☐ Bundesorgan und private Person

☐ Wir gelten für gewisse oder alle Datenbearbeitungen als Bundesorgan, können uns aber auf die erforderlichen Rechtsgrundlagen stützen, auch im Hinblick auf die von uns bearbeiteten besonders schützenswerten Personendaten. Wir trennen sauber zwischen den Daten, die wir als Bundesorgan und die wir (ggf.) als private Person bearbeiten. **→ hier alles OK**

☐ Wir sind kein Bundesorgan bzw. sind nicht als solches tätig. **→ hier alles OK**

Im Detail:

☐ Wir erachten diese Anforderung als **erfüllt**, denn unsere Datenbearbeitung erfolgt *entweder*:

- ☐ Zum Zwecke der Erfüllung eines **gesetzlichen Auftrags** des Schweizer Rechts (sog. indirekte Rechtsgrundlage), den wir ohne unsere Datenbearbeitung nicht erfüllen könnten.→ 1. **OK**
- ☐ Auf Basis einer **Bestimmung des Schweizer Rechts**, die uns unsere Datenbearbeitung in diesem Umfang auch erlaubt (sog. direkte Rechtsgrundlage). → 1. **OK**

☐ Wir nutzen die Daten allerdings noch für Zwecke, die das Gesetz **nicht vorsieht** bzw. die für unseren gesetzlichen Auftrag nicht wirklich nötig sind.

☐ Wir meinen, dass wir uns mit unserer Datenbearbeitung möglicherweise auf **keine gesetzliche Grundlage** im Schweizer Recht abstützen können.

☐ Im Rahmen der Datenbearbeitung haben wir es auch mit **besonders schützenswerten Personendaten** (→ Glossar) oder einem **Profiling** (→ Glossar) zu tun (falls nicht: → 2. **OK**).

- ☐ Wir haben eine direkte Rechtsgrundlage, die ein **Gesetz im formellen Sinn** ist. → 2. **OK**

☐ **Wir benötigen keine Rechtsgrundlage**, da wir nach unserer Einschätzung **kein Bundesorgan** im Sinne des DSG sind.

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

- ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.
- ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.
- ☐ Die Anforderung ist zwar möglicherweise nicht erfüllt, aber:
  - ☐ Uns liegt von den betroffenen Personen im Einzelfall eine gültige Einwilligung vor → dokumentiert in Q1 von Formular E.4 zu DB-Nr. _____.
  - ☐ Die betroffene Person hat ihre Personendaten selbst allgemein zugänglich gemacht (oder erlaubt, dass dies geschieht) und uns die Bearbeitung nicht ausdrücklich untersagt.
  - ☐ Wir müssen die Daten bearbeiten, um Leib und Leben zu schützen und haben jeweils keine Zeit, eine Einwilligung zu holen.
  - ☐ Es geht um eine Bekanntgabe von Personendaten und es liegt einer der Fälle von Art. [32] DSG und gleichzeitig kein Fall von Art. [33] DSG vor.
  - ☐ Die Bearbeitung dient nicht personenbezogenen Zwecken, insbesondere Forschung, Planung oder Statistik, und die weiteren Voraussetzungen von Art. [35] DSG (Anonymisierung, etc.) sind erfüllt.
  - ☐ Der Bundesrat hat unsere Datenbearbeitung bewilligt.
- ☐ Anderer Grund:

  [ ]

diese Frage in der Regel nicht schwerfallen. Sind sie nicht bekannt, so ist eine grundsätzliche Überprüfung der Bearbeitung empfehlenswert, da hier möglicherweise ein schwerwiegender Datenschutzverstoss vorliegt.

Besteht keine Gesetzesgrundlage, muss geprüft werden, ob einer der Ausnahmefälle vorliegt (wie z.B. ob die betroffene Person in die Datenbearbeitung eingewilligt hat). Dies wird in der Spalte ganz rechts abgefragt.

- ☐ Wir haben zwar keine direkte Rechtsgrundlage in Form eines formellen Gesetzes, aber unsere Datenbearbeitung ist **nötig**, damit wir eine uns von einem solchen formellen Gesetz übertragene Aufgabe erfüllen können (indirekte Rechtsgrundlage).
  - ☐ Was wir tun mit den Daten hat für die betroffenen Personen in der Regel **keine relevanten Nachteile.** → 2. **OK**
- ☐ Unsere Rechtsgrundlage ist lediglich eine **Verordnung** oder anderer Erlass.
- ☐ Wir **wissen nicht** genau, wie unsere Rechtsgrundlage eingestuft werden muss.

☐ Unsere Datenbearbeitung kann für einzelne betroffene Personen **schwerwiegende Konsequenzen** haben (falls nicht: → 3. **OK**).

- ☐ Wir haben eine direkte Rechtsgrundlage, die ein **Gesetz im formellen Sinn** ist. → 3. **OK**
- ☐ Wir haben **keine direkte Rechtsgrundlage** in einem formellen Gesetz.

☐ Wir bearbeiten Personendaten sowohl als Bundesorgan wie auch als private Person und:

- ☐ **Trennen zwischen den beiden Bereichen**, damit wir die strengeren Vorschriften bei unseren Aktivitäten als Bundesorgan einhalten können. → 4. **OK**
- ☐ Haben **keine klare Trennung** zwischen unseren Bearbeitungsaktivitäten, die für unsere Aktivitäten als Bundesorgan wie für unsere Aktivitäten als private Person fallen, stellen die Einhaltung der strengeren Vorschriften aber nach unserer Ansicht trotzdem sicher. → 4. **OK**
- ☐ Haben **keine klare Trennung**, aber behandeln alle Daten so, als würden wir sie als Bundesorgan bearbeiten. → 4. **OK**
- ☐ Können **nicht ausschliessen**, dass Daten, die wir als Bundesorgan bearbeiten, nicht auch **in die weniger streng geregelte Bearbeitung** von Personendaten als private Person **gelangen.**

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

- ☐ Wir sollten abklären, ob sich eine Rechtsgrundlage finden lässt.
- ☐ Wir sollten abklären, ob wir eine Einwilligung der betroffenen Personen einholen können.
- ☐ Wir sollten unsere Bearbeitung der Daten als Bundesorgan und jene als private Person strikter voneinander trennen, und zwar insbesondere in diesem Bereich:

- ☐ Wir sollten die Datenbearbeitung so einschränken, dass die Anforderung erfüllt ist (z.B. übergesetzliche Nutzung nur noch mit anonymisierten Daten):

- ☐ Wir sollten die Datenbearbeitung aufgeben.
- ☐ Andere Massnahme:

- ☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

				☐ Wir möchten noch Folgendes vermerken: |	☐ **Situation unklar** Grund: |	☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren ☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen ☐ Sollten wir weitermachen wie bisher. ☐ Treffen wir folgende Sofortmassnahmen: |	☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen: |

Q3

Rechtsgrundlage (nur DSGVO)

Die Datenbearbeitung kann sich auf eine hinreichende Rechtsgrundlage wie eine Einwilligung, einen Vertrag, eine gesetzliche Pflicht oder ein berechtigtes Interesse stützen, wobei die Anforderungen an die Rechtsgrundlage je nach Art der bearbeiteten Daten unterschiedlich ist.

Art. 6, 9 und 10 DSGVO

Anders als im Schweizer Recht ist es unter der DSGVO erforderlich, dass sich jede Datenbearbeitung auf eine Rechtsgrundlage abstützen lässt, d.h. einer der in der DSGVO abschliessend aufgeführten Fälle (wie z.B. berechtigtes Interesse, gesetzliche Pflicht, Vertragsanbahnung oder -abwicklung, Einwilligung) vorliegt, in welchen die betreffenden Personendaten bearbeitet werden dürfen. Trifft keiner dieser Fälle zu, ist die Datenbearbeitung rechtswidrig.

Im Einzelfall kann es schwierig sein, eine passende Grundlage auszumachen. Das gilt speziell für besondere Kategorien von Personendaten (z.B. Gesundheitsdaten) und Daten über Straftaten, für welche eine separate, stark eingeschränkte Auswahl an Rechtsgrundlagen zur Verfügung steht.

Intuitiv wird in den meisten Fällen rasch angenommen, dass das Einholen einer Einwilligung die einfachste Möglichkeit ist, um eine Rechtsgrundlage zu schaffen, aber dies täuscht. In der Praxis wird so gut es geht darauf verzichtet, auf Einwilligungen abzustellen, da diese zur Gültigkeit sehr strenge Voraussetzungen erfüllen müssen und jederzeit widerrufen werden können, womit auch die Rechtsgrundlage für die Zukunft wegfällt.

Am beliebtesten sind die Rechtsgrundlagen der gesetzlichen Pflicht, der Vertragsabwicklung und -anbahnung und des berechtigten Interesses (des Verantwortlichen und etwaiger Dritter). Bei der gesetzlichen Pflicht ist zu beachten, dass grundsätzlich nur

Kurz und bündig:

☐ Wir haben mindestens eine Rechtsgrundlage nach DSGVO, auf welche wir uns bei dieser Datenbearbeitung durchgehen abstützen können. Soweit wir besondere Kategorien von Personendaten und Personendaten über strafrechtliche Verurteilungen und Straftaten bearbeiten, genügt sie auch den erhöhten Anforderungen für solche Fälle. → **hier alles OK**

Im Detail:

☐ Wir erachten diese Anforderung als **erfüllt**, denn die Datenbearbeitung und jeder damit verfolgte Zweck kann sich auf **folgende Rechtsgrundlage(n)** stützen (mindestens eine) → dokumentiert in Abschnitt A von Formular E.3 zu DB-Nr. _____ → 1. **OK**

☐ Diese Rechtsgrundlagen sollten eigentlich alle Aspekte und Fälle der Datenbearbeitung abdecken. → 1. **OK**

☐ Folgende Aspekte der Datenbearbeitung sind damit möglicherweise **nicht abgedeckt**:

☐ Im Rahmen der Datenbearbeitung haben wir es auch mit **besonderen Kategorien von Personendaten** (→ Glossar) zu tun (falls nicht: → 2. **OK**):

☐ Wir können uns auf **folgende Rechtsgrundlage(n)** für solche Daten stützen (mindestens eine) → dokumentiert in Abschnitt B von Formular E.3 zu DB-Nr. _____

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.

☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.

☐ Das Schweizer Recht verpflichtet uns zur Datenbearbeitung. Das gilt zwar als berechtigtes Interesse im Rahmen der DSGVO, aber möglicherweise genügt dies nicht als Rechtsgrundlage. Wir sind jedoch der Meinung, unsere Pflichten unter dem Schweizer Recht gehen vor.

☐ Anderer Grund:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

☐ Wir sollten abklären, ob sich eine Rechtsgrundlage finden lässt.

☐ Wir sollten abklären, ob wir eine Einwilligung der betroffenen Personen einholen können.

☐ Wir sollten die Datenbearbeitung so einschränken, dass die Anforderung erfüllt ist (z.B. übergesetzliche Nutzung nur noch mit anonymisierten Daten):

☐ Wir sollten die Datenbearbeitung aufgeben.

Pflichten unter dem Recht der EU (bzw. des EWR) und der Mitgliedstaaten gemeint ist, nicht auch Schweizer Recht, aber in der Praxis wird oft auch Schweizer Recht als miterfasst behandelt. Im Bereich der strafrechtlichen Daten wäre eine Bearbeitung von Daten sonst gar nicht möglich (z.B. durch Banken im Bereich der Geldwäschereiprävention). Es ist davon auszugehen, dass sich der Gesetzgeber über diese Probleme keine Gedanken gemacht hat.

In diesem Formular werden die Rechtsgrundlagen gemäss DSGVO nur im Ergebnis verzeichnet. Die Ermittlung der einzelnen Rechtsgrundlagen erfolgt stattdessen in → Formular E.3, wo für jede Datenkategorie die gemäss DSGVO möglichen Rechtsgrundlagen abfragt und durchgeprüft werden können.

Es ist in der Praxis umstritten, ob eine Datenbearbeitung sich auf mehrere Rechtsgrundlagen gleichzeitig stützen kann (z.B. auf Einwilligung und berechtigtes Interesse oder gesetzliche Pflicht). Dies wird teilweise auch von behördlicher Seite bestritten. Nach der hier vertreten Auffassung sind Konstellationen mit mehreren parallel gegebenen Rechtsgrundlagen jedoch ohne Weiteres möglich. Es ist aber nicht Ziel dieses Formulars und von → Formular E.3, dass für jede Datenbearbeitung möglichst viele Rechtsgrundlagen geschaffen werden. Es genügt letztlich eine, soweit sie alle Bearbeitungszwecke abdeckt.

☐ Ja, diese Rechtsgrundlagen sollten eigentlich alle Aspekte und Fälle der Datenbearbeitung abdecken. → 2. **OK**

☐ Folgende Aspekte der Datenbearbeitung sind damit möglicherweise **nicht abgedeckt**:

☐ Im Rahmen der Datenbearbeitung haben wir es auch mit **Personendaten über strafrechtliche Verurteilungen und Straftaten** (→ Glossar) zu tun (falls nicht: → 3. **OK**).

☐ Wir können uns auf **folgende Rechtsgrundlage(n)** für solche Daten stützen (mindestens eine) → dokumentiert in Abschnitt C von Formular E.3 zu DB-Nr. _____

☐ Ja, diese Rechtsgrundlagen sollten eigentlich alle Aspekte und Fälle der Datenbearbeitung abdecken. → 3. **OK**

☐ Folgende Aspekte der Datenbearbeitung sind damit möglicherweise **nicht abgedeckt**:

☐ Wir meinen, dass sich unsere Datenbearbeitung möglicherweise auf **keine der in der DSGVO vorgesehenen Rechtsgrundlagen** (vgl. Formular E.3) stützen kann bzw. wissen nicht, welche wir heranziehen könnten.

☐ Wir möchten noch Folgendes vermerken:

☐ Andere Massnahme:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

☐ Sollten wir weitermachen wie bisher.

☐ Treffen wir folgende Sofortmassnahmen:

☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

Q4

Grundsatz von Treu und Glauben I

Die Personendaten werden nach Treu und Glauben bearbeitet. Die Art und Weise, wie die Daten bearbeitet werden ist fair, die damit verfolgten Zwecke sind legitim.

Art. [5] Abs. 2 DSG, Art. 5 Abs. 1 Bst. a DSGVO

Der Grundsatz von Treu und Glauben gilt überall im Rechtsverkehr, so auch im Datenschutz. Hier bedeutet er, dass eine Datenbearbeitung den Datenschutz auch dann verletzt, wenn zwar alle sonstigen Regeln eingehalten sind, sie aber trotz allem aus irgendeinem Grund als unfair, unanständig oder sonst nicht legitim erscheint. Ob eine Datenbearbeitung gegen Treu und Glauben verstösst, wird letztlich mit dem "Bauch" entschieden werden.

Kurz und bündig:

☐ Wir sind der Meinung, dass wir uns mit dem, was wir im Rahmen der Datenbearbeitung tun, einschliesslich der Art und Weise, wie wir die Daten bearbeiten, gegenüber den betroffenen Personen fair verhalten, wir legitime Zwecke verfolgen und das tun, was von uns nach Treu und Glauben erwartet werden kann. → **hier alles OK**

☐ Das, was wir machen, könnte in der Öffentlichkeit als nicht wirklich sauber und fair gewertet werden.

Im Detail:

☐ Wir erachten diese Anforderung als **erfüllt**, denn es trifft unseres Erachtens **keiner der folgenden Fälle** zu: → **hier alles OK**

- ☐ Wenn bekannt würde, was wir machen, würden manche vermutlich der Meinung sein, dass das **nicht fair** ist und **sich nicht gehört.**
- ☐ Wir sind unabhängig vom Schutz unserer Geschäftsgeheimnisse froh, dass die Öffentlichkeit nicht genau weiss, wie wir die Daten der betroffenen Personen bearbeiten, weil das sonst zu für uns **unangenehme Diskussionen in der Öffentlichkeit und sogar Schlagzeilen** in den Medien führen würde.
- ☐ Was wir tun, hat ein "**Gschmäckle**".
- ☐ Die von uns **verfolgten Zwecke** würden von der Öffentlichkeit vermutlich als **nicht legitim** erachtet.
- ☐ Unsere Datenbearbeitung wird aus einem anderen Grund in der Wahrnehmung **problematisch** sein:

☐ Bestimmte der obigen Fälle treffen zwar zu, aber wir haben die Datenbearbeitung **bereits datenschutzrechtlich überprüfen lassen** und für **vertretbar** befunden. → **hier alles OK**

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

- ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.
- ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.
- ☐ *Soweit nur DSG anwendbar:*

  Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr. _____
- ☐ Anderer Grund:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

- ☐ Wir sollten die Datenbearbeitung anpassen, so dass die Anforderungen erfüllt wird.
- ☐ Wir sollten unsere Kommunikation anpassen, um besser zu informieren, was wir eigentlich tun und dem schlechten Eindruck entgegenzuwirken, den es geben kann.

☐ Wir möchten noch Folgendes vermerken:

☐ Andere Massnahme:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

☐ Sollten wir weitermachen wie bisher.

☐ Treffen wir folgende Sofortmassnahmen:

☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

Q5

Grundsatz der Zweckbindung I

Die Personendaten werden nur für festgelegte und eindeutige Zwecke bearbeitet. Es erfolgt keine Datensammlung "auf Vorrat" ohne definierten Zweck.

Art. [5] Abs. 3 DSG, Art. 5 Abs. 1 Bst. b DSGVO

Der Grundsatz der Zweckbindung ist im Datenschutz zentral. Personendaten dürfen nicht ohne Ziel vor Augen erhoben werden, d.h. jede Erhebung und Bearbeitung von Daten muss einen oder mehreren Zwecken dienen. Hier wird in einem ersten Schritt beurteilt, ob dem Unternehmen klar ist, für welche Zwecke die Daten im Rahmen der hier beurteilten Datenbearbeitung überhaupt bearbeitet werden. Das kann der ursprüngliche Zweck einer Datenbearbeitung sein, aber auch Zwecke, die im Laufe der Zeit dazugekommen sind.

Werden Daten an eine Dritte Person weitergegeben, die die Daten wiederum für eigene Zwecke bearbeiten darf, dann ist das in dieser Betrachtung ein Zweck für sich. Werden Adressdaten für Werbung gesammelt, so macht es also einen Unterschied, ob diese Daten nur für eigene Werbezwecke oder auch für Werbezwecke Dritter gesammelt werden. Dies sind zwei unterschiedliche Zwecke, auch wenn die Dritten lediglich Konzerngesellschaften sind.

Ob die Zwecke zulässig sind bzw. was sich daraus sonst noch ergibt, wird in den weiteren, nachfolgenden Anforderungen beurteilt.

Kurz und bündig:

☐ Die Datenbearbeitung dient einzig dem Zweck, der bereits aus ihrer Bezeichnung hervorgeht, und dieser ist klar und präzise umschrieben. → **hier alles OK**

☐ Wir wissen zwar ungefähr, was wir im Rahmen der Datenbearbeitung tun, aber wir wissen nicht wirklich, wozu die Ergebnisse unserer Arbeit dienen (oder ggf. sogar welche Dritte darauf Zugriff haben). Wir könnten, wenn gefragt, keine klare und abschliessende Aufzählung vornehmen.

Im Detail:

☐ Wir können **genau definieren**, **welche Zwecke** mit unserer Datenbearbeitung verfolgt wird, einschliesslich der darin allenfalls vorgesehenen Weitergabe von Daten innerhalb des Unternehmens oder an Dritte, nämlich: → 1. **OK**

☐ Es ist uns nicht so klar, welchen diversen **Nebenzwecken** die Datenbearbeitung in unserem Unternehmen dient (also wer z.B. auf die Daten noch zugreift, wem Daten weitergeleitet werden oder wem die Daten bzw. deren Bearbeitung sonst noch dient); wir kennen nur den **Hauptzweck**, nämlich:

☐ Die von uns definierten Zwecke sind **klar und konkret**; es besteht daher nicht viel Raum für Diskussion, was alles davon erfasst ist: → 2. **OK**

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

- ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.
- ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.
- ☐ *Soweit nur DSG anwendbar:*

  Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr. _____
- ☐ Anderer Grund:
- ☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

- ☐ Wir sollten die folgenden Zwecke, die wir mit der Datenbearbeitung verfolgen, präziser, konkreter oder enger definieren:
- ☐ Wir sollten uns überlegen, was wir mit der Datenbearbeitung alles erreichen möchten.
- ☐ Wir sollten herausfinden, wer im Unternehmen die vorliegende Datenbearbeitung auch noch für sich nutzt.

☐ Wir haben zwar wie oben angegeben Zwecke definiert, ggf. auch im Inventar so festgehalten, aber diese sind **sehr breit und wenig konkret**; unter diesen Begriffen kann man sich teilweise alle möglichen Aktivitäten vorstellen.

☐ Wir möchten noch Folgendes vermerken:

☐ Andere Massnahme:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

☐ Sollten wir weitermachen wie bisher.

☐ Treffen wir folgende Sofortmassnahmen:

☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

Q6

Grundsatz der Zweckbindung II

Daten werden nur für Zwecke beschafft, welche für die betroffenen Personen zum Zeitpunkt der Datenbeschaffung erkennbar waren, und sie dürfen nur in einer Weise verwendet werden, die mit diesen erkennbaren Zwecken datenschutzrechtlich vereinbar ist.

Art. [5] Abs. 3 DSG, Art. 5 Abs. 1 Bst. a und b DSGVO

Der Zweckbindungsgrundsatz verlangt, dass die betroffenen Personen bei der Erhebung ihrer Daten erkennen können, für welche Zwecke ihre Daten bearbeitet werden sollen. Umgekehrt bedeutet dies, dass Daten nur für jene Zwecke bearbeitet werden dürfen, die bei der Beschaffung erkennbar waren. Wer also Daten für einen bestimmten Zweck bearbeiten möchte, muss dies von Anfang an angeben und entsprechende Transparenz schaffen (z.B. im Rahmen einer Datenschutzerklärung oder einem Hinweis in einem Formular).

Erkennbarkeit setzt nicht zwingend voraus, dass da ein Text ist, der den Zweck beim Namen nennt. Er kann auch aus den Umständen hervorgehen, was vorliegend genügt.

Kurz und bündig:

☐ Wir benutzen die Daten im Rahmen dieser Datenbearbeitung nur für Zwecke, von denen die betroffenen Personen ausgehen müssen, weil wir es ihnen zum Zeitpunkt der Datenbeschaffung gesagt haben oder weil sie nach unserer Ansicht vernünftigerweise damit rechnen müssen. Auch an Dritte geben wir Daten (die diese nicht nur für uns bearbeiten) nur dann, wenn die betroffenen Personen damit rechnen müssen. → **hier alles OK**

☐ Wir tun im Rahmen der Datenbearbeitung auch Dinge, mit denen im Grunde niemand rechnen muss und die auch im Gesetz nicht vorgeschrieben werden.

Im Detail:

☐ Wir können wie in Q5 festgestellt **nicht wirklich sagen**, **wozu** die Daten im Rahmen der Datenbearbeitung benutzt werden und wissen daher auch nicht, ob wir die Zweckbindung einhalten.

☐ Für die betroffenen Personen sind alle **Zwecke, die wir mit der Datenbearbeitung verfolgen**, für die betroffenen Personen irgendwie **erkennbar** oder mit den erkennbaren Zwecken **vereinbar**. *Entweder*: → 1. **OK**

  ☐ Sind sie **in den Informationen beschrieben**, die den betroffenen Personen zum Zeitpunkt der Datenbeschaffung vorgelegen haben (z.B. im Rahmen einer Datenschutzerklärung, Vertrag, sonstigen Hinweise, mündliche Ausführungen, Hinweise durch Dritte). Das gilt für folgende Zwecke:

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

  ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.

  ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.

  ☐ *Soweit nur DSG anwendbar:*

  Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr. _____

  ☐ Anderer Grund:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

  ☐ Wir sollten abklären, wozu die Daten im Rahmen dieser Datenbearbeitung verwendet werden, da dies nicht klar ist.

    ☐ Das gilt auch für die anderen Datenbearbeitungen im Unternehmen, die auf die Daten dieser Datenbearbeitung zugreifen.

  ☐ Wir sollten unsere Informationen für die betroffenen Personen um Angaben zu folgenden Zwecken ergänzen:

  ☐ Wir sollten sicherstellen, dass auch folgende Personen direkt oder indirekt informiert werden über das, wozu wir ihre Daten bearbeiten möchten:

Es genügt sogar, dass der verfolgte Zweck zwar nicht so angegeben wurde und auch nicht aus den Umständen ersichtlich war, aber mit dem erkennbaren Zweck trotz allem als vereinbar erscheint, d.h. ihm so nahe steht, dass er als mitabgedeckt gelten muss. Das soll dann der Fall sein, wenn die betroffenen Personen auch ohne ausdrückliche Nennung mit einer Bearbeitung zu diesem Zweck rechnen mussten und dies nicht wirklich problematisch ist (im Rahmen der DSGVO muss jedoch mit → Formular E.3 geprüft werden, ob diese Zwecke gewisse zusätzliche Anforderungen erfüllen). Die Anonymisierung von Daten für die Zwecke einer statistischen Auswertung ist ein Beispiel; die Anonymisierung ist zwar für sich ein Bearbeitungsvorgang, aber unproblematisch.

Bei diesen "vereinbaren" Zwecken ist es unter der DSGVO umstritten, ob auch diese eine separate Rechtsgrundlage nach Art. 6, 9 und 10 DSGVO benötigen oder nicht. Nach der hier vertretenen Ansicht ist keine separate Rechtsgrundlage erforderlich.

In der mittleren Spalte sollte im Ergebnis beurteilt werden, ob die diversen Zwecke, welche mit der Datenbearbeitung verfolgt werden (vgl. Q5), für die betroffenen Personen in irgendeiner Person im Rahmen der Datenbeschaffung erkennbar waren oder ob die verfolgten Zwecke mindestens mit den erkennbaren Zwecken vereinbar sind.

☐ Gehen sie zwar **nicht aus einer Information** hervor, aber es musste für die betroffenen Personen auch ohne konkrete Information **aufgrund der Umstände klar** sein, dass wir ihre Daten entsprechend benutzen werden. Das gilt für folgende Zwecke:

☐ Werden die Daten werden von uns bearbeitet, weil wir **aufgrund des Schweizer Rechts dazu verpflichtet** sind, auch wenn das für die betroffenen Personen womöglich nicht erkennbar ist. Das gilt für folgende Zwecke:

☐ Oder handelt sich um **andere Zwecke**, mit denen die betroffenen Personen **vernünftigerweise rechnen müssen**, die **weder unangebracht sind noch zu beanstanden sind** (und daher mit den Zwecken, für welche wir die Daten beschafft haben, vereinbar), nämlich um folgende Zwecke:

Soweit die DSGVO anwendbar ist:

- ☐ Diese "vereinbaren" Zwecke **erfüllen** auch die Anforderungen gemäss Q5 in Abschnitt A von Formular E.3 zu DB-Nr. _____.

☐ Das gilt alles auch mit Bezug auf jene Personen, mit denen wir **nicht direkt in Kontakt sind**, wir aber aufgrund der Umstände trotzdem davon ausgehen können, dass die von uns verfolgten Zwecke für sie **erkennbar** oder mit diesen **vereinbar** sind (z.B. weil sie von unseren Vertragspartnern, Familienmitgliedern, dem Arbeitgeber etc. informiert wurden). → 2. **OK**

☐ Wir sollten folgende Bearbeitungszwecke einschränken, weil sie nicht wirklich mit den Zwecken, für welche wir die Daten beschafft haben, vereinbar sind. Dazu sollte ein Vorgehensplan ausgearbeitet und umgesetzt werden:

☐ Wir sollten auf folgende Bearbeitungszwecke verzichten, weil wir darüber nicht informiert haben und auch kein Rechtfertigungsgrund ersichtlich ist. Dazu sollte ein Vorgehensplan ausgearbeitet werden:

☐ Wir sollten sicherstellen, dass auch folgende Datenbearbeitungen, die auf die Daten dieser Datenbearbeitung zugreifen, den Zweckbindungsgrundsatz einhalten. Das ist mit den dafür zuständigen Personen zu erörtern:

Soweit das DSG anwendbar ist (nur folgende Frage):

☐ Wir sollten prüfen, ob wir allenfalls einen Rechtfertigungsgrund (wie z.B. eine Einwilligung) finden oder schaffen können.

☐ Andere Massnahme:

☐ Das gilt alles auch mit Bezug auf die **Weitergabe von Daten an Dritte**, die diese für ihre eigenen Zwecke benutzen können (also die Daten nicht nur in unserem Auftrag bearbeiten). Auch damit müssen die betroffenen Personen vernünftigerweise rechnen, soweit wir es ihnen nicht sogar sagen. → 3. **OK**

☐ Wir halten den **Zweckbindungsgrundsatz nicht** ein:

☐ Weil wir die Daten auch noch für folgende weitere, **nicht erkennbare bzw. nicht vereinbare Zwecke** benutzen:

☐ Weil die von uns verfolgten Zwecke jedenfalls für **folgende Kategorien von betroffenen Personen** womöglich **nicht erkennbar** waren:

☐ Es handelt sich allerdings um Personen, bei denen die Datenbeschaffung schon lange zurückliegt. **Inzwischen** haben wir **auch sie darüber informiert**, wozu wir die Daten nutzen, und sie haben nicht opponiert. → 1. + 2. **OK**

☐ Die Daten **gehen** aus der Datenbearbeitung **an weitere Datenbearbeitungen im Unternehmen** bzw. werden auch **anderweitig genutzt** (und die nicht auf der Ausschluss-Liste zu Beginn des Formulars stehen).

☐ **Wir wissen nicht**, ob dort der Grundsatz der Zweckbindung ebenfalls eingehalten wird.

☐ Wir wissen, dass der **Zweckbindungsgrundsatz** dort:

☐ Ebenfalls **eingehalten** wird; → 2. **OK**

☐ **Nicht eingehalten** wird, nämlich mit Bezug auf:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

☐ Sollten wir weitermachen wie bisher.

☐ Treffen wir folgende Sofortmassnahmen:

☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

☐ In allen Fällen, wo wir Daten **Dritten** (d.h. anderen Unternehmen in und ausserhalb der Firmengruppe, Behörden, Organisationen, etc.) **bekanntgeben** oder sonst für die Zwecke Dritter benutzen, haben wir **geprüft**, ob auch dies für die betroffenen Personen **erkennbar** war oder mit den **Zwecken**, für welche die Daten beschafft wurden, mindestens **vereinbar** ist; ausgenommen sind Fälle, wo Dritte die Daten lediglich für die Zwecke des Unternehmens bearbeiten (Auftragsbearbeitung).

- ☐ Diese Anforderung ist **erfüllt.** → 3. **OK**
- ☐ Diese Anforderung ist mit Bezug auf **folgende Fälle** nicht erfüllt.

- ☐ Es werden **keine Daten für Dritte genutzt** oder Dritten bekanntgegeben (auch nicht im Konzern). → 3. **OK**

☐ Wir möchten noch Folgendes vermerken:

Q7

Grundsatz der Transparenz

Die Datenerhebung erfolgt für die betroffenen Personen transparent. Ihnen wird zum Zeitpunkt der Datenbeschaffung insbesondere transparent gemacht, wer ihre Daten erhebt und wozu (und zwar alle definierten Bearbeitungszwecke; vgl. Inventar, Formular B.2), sofern dies nicht aus den Umständen ersichtlich ist.

Art. [5] Abs. 3 DSG, Art. 5 Abs. 1 Bst. a DSGVO

Der Grundsatz der Transparenz ist ebenso zentral wie der Grundsatz der Zweckbindung und mit ihm eng verwandt. Er basiert auf der Idee, dass die informationelle Selbstbestimmung, um welche es beim Datenschutz geht (jeder kann in einem gewissen Rahmen selbst bestimmen, was mit seinen Daten geschieht), voraussetzt, dass die betroffenen Personen wissen, was mit ihren Daten geschieht. Will ein Unternehmen Daten erheben und bearbeiten, muss es dies der betroffenen Person transparent machen, und zwar mit allen Aspekten, die für eine betroffene Person besonders wichtig sein wird. Der Transparenzgrundsatz ist ein Hauptgrund, warum es Datenschutzerklärungen gibt.

Weil Transparenz im Datenschutz so zentral ist, der Grundsatz der Transparenz im Rahmen der DSGVO und des revidierten DSG mit einer Informationspflicht ergänzt, die Unternehmen verpflichtet, betroffenen Personen gewisse Parameter der Datenbearbeitung zusätzlich explizit zu deklarieren. Dies wird in Q24 abgefragt. Der Grundsatz der Transparenz gilt ungeachtet dieser Informationspflicht und ist weniger scharf umrissen. Wird eine Videokamera in einem Gebäude für Sicherheitszwecke verwendet, genügt es in der Regel für die Zwecke des Grundsatzes der Transparenz, dass diese gut sichtbar und es allen klar ist, dass es um eine Sicherheitskamera geht und sich darauf einstellen können. Im Rahmen der Informationspflicht

Kurz und bündig:

☐ Wir achten darauf, dass volle Transparenz darüber besteht, wozu wir Daten bearbeiten und an wen die Daten ggf. gehen. Die betroffenen Personen können das entweder entsprechenden Hinweisen entnehmen oder aber es ist aufgrund der Umstände klar. → **hier alles OK**

☐ Wir sind jedenfalls bezüglich gewisser Dinge, die wir im Rahmen dieser Datenbearbeitung tun, nicht wirklich transparent.

Im Detail:

☐ Wir **weisen** die betroffenen Personen **darauf hin**, wer wir sind und **wozu** wir ihre Daten bearbeiten und an wen die Daten ggf. gehen: → **hier alles OK**

- ☐ Über **Hinweise** im Rahmen der Datenerhebung (z.B. Hinweise auf einem Formular);
- ☐ Über unsere **Datenschutzerklärung** auf der Website.
  - ☐ Wir weisen sie darauf hin (z.B. auf dem Formular, in den Vertragsbedingungen, auf der Website, in der App), dass die Erklärung auf der Website abgerufen werden kann.
  - ☐ Wir **gehen davon aus**, dass sie wissen, wer wir sind und wo unsere Website zu finden ist.
- ☐ Über Hinweise in einem **Vertrag** mit ihnen (auch AGB)
- ☐ Über **Schilder** und ähnliches
- ☐ Auf andere Weise:

☐ Die betroffenen Personen müssen sich aufgrund der Umstände und ihrer Erfahrung auch ohne Hinweis durch uns **bewusst sein**, dass wir über sie Daten beschaffen und wozu. → **hier alles OK**

- ☐ Weil sie uns die **Daten selbst liefern** zu den Zwecken.

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

- ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.
- ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.
- ☐ *Soweit nur DSG anwendbar:*

  Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr. _____

- ☐ Anderer Grund:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

- ☐ Wir sollten die betroffenen Personen über unsere Datenbearbeitung informieren und dazu:
  - ☐ Die Datenschutzerklärung auf der Website anpassen bzw. eine solche erstellen.
  - ☐ Unsere Formulare anpassen.
  - ☐ Unsere AGB anpassen.
  - ☐ Die von uns sonst benutzten Verträge anpassen.
  - ☐ Schilder oder ähnliches anbringen.

(Q24) muss dann noch zusätzlich über bestimmte Dinge informiert werden.

Wie Transparenz hergestellt wird, ist letztlich egal. Wesentlich ist, dass die betroffene Person erkennen kann, dass Daten über sie erhoben und bearbeitet werden.

- ☐ Weil sie **mitbekommen**, wie wir die Daten über sie **erheben** (z.B. durch eine sichtbare Kamera) und sie eins und eins zusammenzählen können.
- ☐ Weil sich aus der **allgemeinen Lebenserfahrung** bzw. dem Allgemeinwissen ergibt, dass wir bzw. Unternehmen wie wir in einer solchen Situation Daten für diese Zwecke erheben.
- ☐ Weil sie das **von früher** wissen.
- ☐ Weil sie es von **anderer Seite** erfahren haben.
- ☐ Weil es **Hinweise** darauf gibt:

- ☐ Aus anderen Gründen:

☐ Wir weisen die betroffenen Personen zwar **nicht direkt** darauf hin, aber **andere** sollten das für uns tun:
→ hier alles OK

- ☐ Weil wir es mit ihnen **vereinbart** haben;
- ☐ Weil wir **meinen, davon ausgehen zu dürfen**, dass sie das wenn nötig tun (z.B. unsere Geschäftspartner ihre Mitarbeiter informieren, unsere Arbeitnehmer ihre Familienmitglieder, unser Kunden die Leistungsempfänger, etc.).

☐ Wir meinen, dass zwar die Erhebung der Daten durch uns **transparent** ist, aber nicht, dass wir die Daten im Rahmen der Datenbearbeitung **auch** für **folgende Zwecke** bearbeiten:

- ☐ Anderes tun, nämlich:

☐ Wir haben zwar keine sinnvolle Möglichkeit zur Durchführung der erforderlichen Information, aber wir sollten mindestens die Erhebung der Daten deutlicher erkennbar machen.

☐ Wir sollten folgende Informationen anpassen und deutlicher werden, was wir tun:

☐ Wir sollten folgende Dritten dazu verpflichten oder sonst bewegen, die betroffenen Personen wenn nötig zu informieren über unsere Datenerhebung:

☐ Da wir keine zusätzliche Transparenz herstellen können, sollten wir die Datenbearbeitung wie folgt einschränken, damit wir den Anforderungen entsprechen:

☐ Die betroffenen Personen mögen zwar annehmen, dass über sie Daten erhoben werden, aber dass wir das tun, davon müssen sie **vernünftigerweise nicht ausgehen.**

☐ Die betroffenen Personen haben **keine Ahnung**, dass wir im Rahmen der Datenbearbeitung Daten über sie erheben und wozu.

☐ Wir möchten noch Folgendes vermerken:

☐ Andere Massnahme:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

☐ Sollten wir weitermachen wie bisher.

☐ Treffen wir folgende Sofortmassnahmen.

☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

Q8

Grundsatz der Verhältnismässigkeit I ("Datenminimierung")

Es werden nur Personendaten bearbeitet, die für die Erfüllung der festgelegten Bearbeitungszwecke geeignet sind.

Art. [5] Abs. 2 DSG, Art. 5 Abs. 1 Bst. c DSGVO

Der Grundsatz der Verhältnismässigkeit ist der dritte zentrale Grundsatz im Datenschutz. Er knüpft an die mit einer Datenbearbeitung verfolgten Zwecke (Q5) an und besagt, dass im Rahmen dieser Datenbearbeitung nur getan werden darf, was für die Erreichung dieser Zwecke nötig, geeignet und für die betroffene Personen zumutbar sind bzw. Zweck und Mittel in einem vernünftigen Verhältnis stehen (Verhältnismässigkeit im engeren Sinne).

Hier wird geprüft, ob wirklich nur jene Daten erhoben und bearbeitet werden, die für die Erreichung der verfolgten Zwecke tatsächlich geeignet sind. Auf alles, was nicht mindestens dafür brauchbar ist, sollte verzichtet werden. Dies ist der eine Teilaspekt der "Datenminimierung". Der andere wird in Q9 abgedeckt. Das Prinzip der Datenminimierung ist mitunter auch als Prinzip der "Datensparsamkeit" bekannt.

Kurz und bündig:

☐ Alle Kategorien von Daten, die wir einsetzen, sind für die von uns verfolgten Zwecke nützlich, mindestens aber brauchbar. → **hier alles OK**

☐ Wir haben uns nie überlegt, ob alle von uns bearbeiteten Daten wirklich zweckmässig sind.

Im Detail:

☐ Wir erachten diese Anforderung als erfüllt, denn alle Personendaten, die wir im Rahmen der Datenbearbeitung verwenden, helfen, den **Bearbeitungszweck zu erreichen** und sind daher **relevant**; diese Relevanz haben die diversen Datenkategorien trotz aller Entwicklungen der letzten Jahre nicht verloren. → **hier alles OK**

  ☐ Wir haben für diese Erhebung die einzelnen Datenkategorien **nochmals durchgesehen** und können das bestätigen.

  ☐ Diese Frage **prüfen wir standardmässig** bei der Entwicklung von Systemen bzw. Applikationen. Wir haben keinen Grund anzunehmen, dass dies hier nicht geschah.

☐ Gewisse Personendaten, die wir haben bzw. bearbeiten, **passen eigentlich nicht mehr** wirklich zu unseren heutigen Verwendungszwecken.

  ☐ Folgende:

  ☐ Einen konkreten Überblick haben wir nicht, es ist dies nur ein **Gefühl.**

☐ **Wir wissen nicht** wirklich, ob die Personendaten, die wir haben bzw. bearbeiten für unsere Verwendungszwecke überhaupt noch passen.

☐ Es sind unseres Erachtens **keine Massnahmen nötig.**

  ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.

  ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.

  ☐ *Soweit nur DSG anwendbar:*

  Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr.

  _____

  ☐ Anderer Grund:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

  ☐ Wir sollten die folgenden Datenkategorien erheben, die für unsere Verwendungszwecke keinen Sinn mehr machen, nicht mehr:

  ☐ Wir sollten auch die bestehenden Daten löschen.

  ☐ Wir sollten den Zugang zu den Daten einschränken, die für unsere Verwendungszwecke keinen Sinn mehr machen und sie ein bzw. archivieren; so beschränken wir deren Nutzung auf ein Minimum, bewahren sie aber für Archivzwecke noch auf; es sind dies folgende Daten:

☐ Wir möchten noch Folgendes vermerken:

☐ Wir sollten die einzelnen Datenkategorien durchgehen, beurteilen ihre Eignung und entscheiden, was wir mit den nicht passenden Kategorien machen:

☐ Andere Massnahme:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

☐ Sollten wir weitermachen wie bisher.

☐ Treffen wir folgende Sofortmassnahmen.

			☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen: [ ]
	Q9	**Grundsatz der Verhältnismässigkeit II ("Datenminimierung")** Es werden nur Personendaten bearbeitet, die für die Erfüllung der festgelegten Bearbeitungszwecke erforderlich sind. *Art. [5] Abs. 2 DSG, Art. 5 Abs. 1 Bst. c DSGVO* Hier wird der zweite Teilaspekt der "Datenminimierung" abgefragt (vgl. Q8), der Teil des Grundsatzes der Verhältnismässigkeit ist (dazu Q8). Hier wird geprüft, ob wirklich nur jene Daten erhoben und bearbeitet werden, die für die Erreichung der mit der Datenbearbeitung verfolgten Zwecke (Q5) tatsächlich nötig sind. Auf alles, was nicht nötig ist, sollte verzichtet werden. Umgekehrt bedeutet dies, dass das Unternehmen in der Lage sein muss, für jedes Datenelement in der Datenbearbeitung eine Begründung vorlegen zu können, warum es dieses braucht und nicht darauf verzichten kann. Diese Begründungen werden hier nicht dokumentiert; es wird nur abgefragt, ob es tatsächlich alle bearbeiteten Daten braucht. Es ist empfohlen, die Liste der Datenelemente durchzugehen und zu prüfen, ob gewisse Datenelemente gestrichen werden können.	*Kurz und bündig:* ☐ Wir sind der Meinung, dass wir im Rahmen unserer Datenbearbeitung so wenig Personendaten wie möglich erheben und bearbeiten, um die von uns verfolgten Zwecke zu erfüllen. → **hier alles OK** ☐ Wir haben uns nie überlegt, ob wir alle Daten brauchen, die wir erheben. Vermutlich würden wir auch mit weniger Daten auskommen. *Im Detail:* ☐ Ja, alle Personendaten, die wir im Rahmen der Datenbearbeitung verwenden, sind für mindestens einen der Zwecke, die wir mit der Datenbearbeitung verfolgen, **erforderlich**, d.h. wir können nicht ohne Weiteres darauf verzichten. ☐ Wir haben für diese Erhebung die einzelnen Datenkategorien **nochmals durchgesehen** und können das bestätigen. → 1. **OK** ☐ Diese Frage **prüfen wir standardmässig** bei der Entwicklung von Systemen bzw. Applikationen. Wir haben keinen Grund anzunehmen, dass dies hier nicht geschah. → 1. **OK** ☐ Wir brauchen zwar nicht alle Personendaten, die wir für die Datenbearbeitung erheben, aber bei jenen, die wir für die Zwecke dieser Datenbearbeitung nicht unbedingt brauchen, **überlassen wir es der betroffenen Person**, ob sie sie uns mitteilen will. ☐ Es wird **nichts** mit diesen Daten gemacht (und sie dienen auch nicht der betroffenen Person). Wir brauchen sie nicht.	☐ Es sind unseres Erachtens **keine Massnahmen nötig:** ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt. ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist. ☐ *Soweit nur DSG anwendbar:* Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr. _____ ☐ Anderer Grund: [ ] ☐ Es sind unseres Erachtens **folgende Massnahmen nötig:** ☐ Wir sollten die folgenden die Datenkategorien, die wir für unsere Verwendungszwecke nicht mehr brauchen, nicht mehr erheben: [ ] ☐ Wir löschen auch die bestehenden Daten.

☐ Diese Daten werden für **andere Zwecke bzw. für andere Datenbearbeitungen** benutzt bzw. **für die betroffene Person** erhoben, und die betroffene Person kennt diese Zwecke bzw. Bearbeitungen. → 1. **OK**

☐ Es würde uns **nicht genügen**, wenn wir die Personendaten **lediglich in anonymer bzw. anonymisierter Form** erheben würden, d.h. so, dass wir für uns keine Rückschlüsse auf die Identität der jeweiligen Person möglich ist. → 2. **OK**

☐ Folgende Personendaten **brauchen wir** in Anbetracht dessen, was wir mit der Datenbearbeitung erreichen wollen, eigentlich **nicht** und könnten **verzichten:**

☐ Wir können die obigen Fragen **nicht** wirklich **beantworten**, da wir keinen Überblick haben, was wir für unsere Datenbearbeitung wirklich benötigen.

☐ Wir möchten noch Folgendes vermerken:

☐ Wir sollten den Zugang zu den Daten, die für unsere Verwendungszwecke keinen Sinn mehr machen, einschränken bzw. archivieren; so beschränken wir deren Nutzung auf ein Minimum, bewahren sie aber für Archivzwecke noch auf; es sind dies folgende Daten:

☐ Wir sollten dafür sorgen, dass folgende Daten so bald wie möglich anonymisiert werden:

☐ Wir sollten der betroffenen Person bei folgenden an sich nicht zwingend benötigten Daten die Wahl selbst geben zu entscheiden, ob sie sie uns mitteilen will:

☐ Wir sollten die einzelnen Datenkategorien bezüglich ihrer Notwendigkeit beurteilen und entscheiden, was wir mit den nicht benötigten Kategorien machen.

☐ Andere Massnahme:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

			☐ **Situation unklar** Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren ☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen ☐ Sollten wir weitermachen wie bisher. ☐ Treffen wir folgende Sofortmassnahmen: ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

Q10

Grundsatz der Verhältnismässigkeit III

Die Daten werden nur auf eine Weise bearbeitet, die für die festgelegten Bearbeitungszwecke erforderlich ist. Sie werden insbesondere nur soweit für die vom Unternehmen verfolgten Zwecke nötig ausgewertet, Dritten zugänglich gemacht oder anderweitig bearbeitet.

Art. [5] Abs. 2 DSG, Art. 5 Abs. 1 Bst. b DSGVO

Der Grundsatz der Verhältnismässigkeit (vgl. Q8) sagt nicht nur, dass nur die für die verfolgten Zwecke (Q5) erforderlichen Daten erhoben werden dürfen, sondern auch, dass deren Bearbeitung nur so weit gehen darf, wie dies für diese Zwecke wirklich erforderlich ist.

Unnötige bzw. unnötig weit gehenden Analysen sind somit ebenso nicht erlaubt nach diesem Grundsatz wie eine Weitergabe oder Publikation der Daten, die für den Zweck nicht bzw. nicht mehr erforderlich ist (z.B. weil er schon erreicht wurde). Jeder Bearbeitungsschritt ist somit daraufhin zu prüfen, ob er für die verfolgten Zwecke wirklich nötig ist.

Die dazugehörige Frage, wie lange die Daten bearbeitet bzw. aufbewahrt werden, ist allerdings in Q13 abgehandelt.

Kurz und bündig:

☐ Wir tun im Rahmen der Datenbearbeitung zwar verschiedene Dinge, doch jeder solche Bearbeitungsschritt ist nötig, damit wir die von uns ursprünglich verfolgten Zwecke auch erreichen können. Wir geben Daten auch nur dann und nur so weit Dritten bekannt, als dies für diese Zwecke erforderlich ist. → **hier alles OK**

☐ Wir können nicht sagen, dass wir die Daten nur soweit bearbeiten, als dies zur Erreichung der von uns ursprünglich verfolgten Zwecke nötig ist. Wir brauchen die Daten heute auch für andere Dinge, tun teilweise mehr als nötig wäre oder geben auch Dritten mehr bekannt, als sie bräuchten.

Im Detail:

☐ Wir erfüllen die Anforderung, denn **keiner der folgenden Fälle** trifft zu: → **hier alles OK**

- ☐ Wir **gehen** bei der **Auswertung** der Daten **klar weiter**, als dies für die ursprünglich von uns verfolgten Zwecke (d.h. die bei der Beschaffung der Daten gemäss Q6 erkennbar waren) oder damit vereinbaren Zwecke (gemäss Q6) nötig wäre.

  - ☐ Im Grunde verfolgen wir auch nicht **nicht deklarierte Bearbeitungszwecke** (und verletzen damit womöglich auch den Zweckbindungsgrundsatz).

- ☐ Wir könnten die von uns ursprünglich verfolgten oder damit vereinbaren Zwecke **auch ohne bestimmte der Dinge** erreichen, die wir im Rahmen der Datenbearbeitung mit den Daten tun, nämlich:

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

- ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.
- ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.
- ☐ *Soweit nur DSG anwendbar:*

  Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr. _____
- ☐ Anderer Grund:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

- ☐ Wir sollten herausfinden, was genau im Rahmen der Datenbearbeitung mit den Daten alles geschieht, insbesondere an wen was weitergegeben werden wird und wie sie ausgewertet werden.
- ☐ Die Auswertung der Daten sollte wie folgt eingeschränkt werden:
- ☐ Die Bekanntgabe von Daten an Dritte (als Verantwortliche) sollte wie folgt eingeschränkt werden:

☐ Bei gewissen Dingen, die wir im Rahmen der Datenbearbeitung tun, haben wir uns **nicht überlegt**, ob diese für die Erreichung der von uns ursprünglich verfolgten oder vereinbaren Zwecke **erforderlich** ist:

☐ Wir geben **Dritten mehr Daten bekannt als sie** für die von uns ursprünglich verfolgten oder damit vereinbaren Zwecke **brauchen:**

☐ Wir **ziehen** im Zusammenhang mit der Datenbearbeitung **Dritte für Dinge bei**, für die wir sie für die Erreichung der von uns ursprünglich verfolgten oder damit vereinbaren Zwecke **nicht unbedingt bräuchten**, weil wir unser Ziel auch ohne diese Dritten erreichen könnten:

☐ Wir **wissen nicht wirklich**, was mit den Daten im Rahmen der Datenbearbeitung alles gemacht wird bzw. können nicht sagen, was ursprünglich verfolgt wurde oder damit vereinbar ist:

☐ Wir möchten noch Folgendes vermerken:

☐ Der Beizug Dritter (als Auftragsbearbeiter) sollte wie folgt eingeschränkt werden:

☐ Wir sollten die Liste der Bearbeitungszwecke, die wir mit der Datenbearbeitung verfolgen, aufdatieren bzw. erweitern und dies entsprechend kommunizieren:

☐ Wir sollten folgende Daten nicht mehr bearbeiten:

☐ Andere Massnahme:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

				☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen ☐ Sollten wir weitermachen wie bisher. ☐ Treffen wir folgende Sofortmassnahmen: ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:
	Q11	**Grundsatz der Verhältnismässigkeit IV** Die Personendaten werden so bearbeitet, dass dies den betroffenen Personen zugemutet werden kann, auch im Hinblick auf die (nicht datenschutzrechtlichen) Folgen, welche die Datenbearbeitung haben kann (Verhältnismässigkeit im engeren Sinn). Der von uns verfolgte Zweck steht in einem vernünftigen Verhältnis zu dem, was wir tun und welche Auswirkungen das haben kann. *Art. [5] Abs. 2 DSG, Art. 5 Abs. 1 Bst. a DSGVO* Der Grundsatz der Verhältnismässigkeit (vgl. Q8) beinhaltet nebst dem Aspekt der Eignung und Notwendigkeit für die verfolgten Zwecke (Q5) auch die Anforderung, dass sie in einem vernünftigen Verhältnis zu den dafür eingesetzten Mittel stehen. Das bedeutet im Ergebnis, dass eine Datenbearbeitung immer auch danach zu prüfen ist, ob sie in Anbe-	*Kurz und bündig:* ☐ Wir sind der Meinung, dass wir unsere Datenbearbeitung den Betroffenen zumuten können und es in einem vernünftigen Verhältnis zu den möglichen Folgen für sie steht. → **hier alles OK** ☐ Wenn die betroffenen Personen wüssten, was wir mit den Daten machen, fänden sie das wohl nicht in Ordnung und zu weitgehend. *Im Detail:* ☐ Wir erachten diese Anforderung als **erfüllt**, denn es trifft unseres Erachtens **keiner der folgenden Fälle** zu: → **hier alles OK** ☐ Was wir den betroffenen Personen zumuten mit der Bearbeitung ihrer Daten, dürfte auch für neutrale Beobachter **zu weit gehen** und daher **nicht wirklich im Verhältnis** zu dem stehen, was es uns bringt. ☐ Den betroffenen Personen drohen aufgrund dessen, was wir mit ihren Daten machen, **gewichtige negative Folgen**, mit denen sie **vernünftigerweise nicht rechnen mussten**, als wir ihre Daten beschafft haben.	☐ Es sind unseres Erachtens **keine Massnahmen nötig:** ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt. ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist. ☐ *Soweit nur DSG anwendbar:* Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr. _____ ☐ Anderer Grund: ☐ Es sind unseres Erachtens **folgende Massnahmen nötig:** ☐ Wir sollten die Datenbearbeitung so einschränken, so dass sie für die betroffenen Personen zumutbar wird.

tracht der damit verfolgten Zwecke für die betroffenen Personen zumutbar ist. Wenn die Datenbearbeitung gewichtige Folgen für die davon betroffenen Personen haben kann bzw. ein erheblicher Eingriff in die Privatsphäre darstellt, so erlaubt der Datenschutz dies nur, wenn dies für einen ebenso gewichtigen Zweck geschieht.

Ein Beispiel wäre die regelmässige und systematische Analyse aller E-Mails der Mitarbeiter, um Hinweise auf ein beliebiges Fehlverhalten der Mitarbeiter zu finden. Hingegen wäre es verhältnismässig im engeren Sinne, wenn ein Unternehmen einen automatischen Filter einsetzt, der verhindert, dass Mitarbeiter geheime Firmendokumente an externe Empfänger versendet (*Data Loss Prevention*).

Die DSGVO nennt dieses Erfordernis nicht ausdrücklich, aber es ist dort im Gebot der Bearbeitung nach Treu und Glauben enthalten. Darum wird es hier auch im Falle einer Anwendbarkeit der DSGVO geprüft.

☐ Unsere Datenbearbeitung könnte **aus einem anderen Grund** als für die betroffenen Personen **nicht zumutbar** qualifiziert werden:

☐ Wir möchten noch Folgendes vermerken:

☐ Wir sollten zusätzliche Massnahmen treffen, um die negativen Folgen für die betroffenen Personen abzufedern oder sogar zu verhindern.

☐ Wir sollten die betroffenen Personen entscheiden lassen, ob sie der Datenbearbeitung widersprechen möchten.

☐ Andere Massnahme:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

				☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen ☐ Sollten wir weitermachen wie bisher. ☐ Treffen wir folgende Sofortmassnahmen: ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:
	Q12	**Grundsatz der Verhältnismässigkeit V** Auf die Daten haben nur jeweils jene Personen Zugriff, die diesen für die festgelegten Bearbeitungszwecke benötigen. *Art. [5] Abs. 2 DSG, Art. 5 Abs. 1 Bst. a, b, e und f DSGVO, Art. 32 DSGVO* Auch hinsichtlich der Personen, die Zugriff auf die bearbeiteten Personendaten haben, sollte der Grundsatz der Verhältnismässigkeit (vgl. Q8) beachtet werden: Zugriff sollte auch innerhalb des Unternehmens nur haben, wer diesen für die Erfüllung der mit der Datenbearbeitung verfolgten Zwecke benötigt. Die DSGVO nennt dieses Erfordernis nicht ausdrücklich, aber es ist dort im Gebot der Bearbeitung nach Treu und Glauben, der Zweckbindung und der Speicherbegrenzung enthalten. Darum wird es hier auch im Falle einer Anwendbarkeit der DSGVO geprüft. Die Zugriffsbeschränkung ergibt sich ferner aus dem Gebot der Datensicherheit.	*Kurz und bündig:* ☐ Bei allen Daten der Datenbearbeitung haben wir ein Konzept erarbeitet, wer worauf zugreifen können muss und wie lange. Es beschränkt die Zugriffe auf das, was nötig ist. Diese Zugriffsregelung haben wir in den Systemen entsprechend umgesetzt. → **hier alles OK** ☐ Zugriff hat bei uns zwar nicht jeder, aber die Zugriffsrechte könnte ohne Einbussen bei der Zielerreichung wesentlich eingeschränkt werden. Wir haben entweder gar kein Zugriffskonzept oder aber ein Konzept, das deutlich optimiert werden könnte. *Im Detail:* ☐ Der **betriebsinterne Zugriff** auf die Daten dieser Datenbearbeitung ist bei uns: ☐ Für (fast) **jeden** im Betrieb möglich: ☐ Weil unser System **keine** sinnvolle **Zugangsbeschränkung** ermöglicht. ☐ Weil die so zugänglichen Daten sowieso **öffentlich** sind. → 1. **OK**	☐ Es sind unseres Erachtens **keine Massnahmen nötig:** ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt. ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist. ☐ *Soweit nur DSG anwendbar:* Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr. _____ ☐ Anderer Grund: ☐ Es sind unseres Erachtens **folgende Massnahmen nötig:** ☐ Wir sollten ein Konzept erstellen, das die Zugriffsberechtigungen gesetzeskonform regelt.

☐ Weil alle diesen **Zugriff brauchen**, wenngleich einige öfters und andere weniger oft. → 1. **OK**

☐ Weil wir uns um das Thema bisher **nicht gekümmert** haben.

☐ Aus einem anderen Grund:

☐ Nur für **bestimmte Personen** möglich, wobei:

☐ Im Falle von Daten, die aus Sicht der betroffenen Person **sensitiv** sind**,** wir noch genauer darauf achten, dass nur jene, die dies **wirklich benötigen**, Zugriff haben. → 1. **OK**

☐ Der Zugriff auf Daten generell auf jene Personen beschränkt, welche ihn **wirklich benötigen.** → 1. **OK**

☐ Wir im Falle von Daten, die aus Sicht der betroffenen Personen **sensitiv** sind, darauf achten, dass nur Personen Zugriff haben, die ihn **wirklich benötigen.** Bei allen **anderen Daten** achten wir darauf, dass wir nur Personen Zugriff geben, bei denen wir davon ausgehen, dass sie sie **nicht zweckentfremden** bzw. **missbrauchen.** → 1. **OK**

☐ Bei uns ist es anders:

☐ Wir **wissen gar nicht wirklich**, wer Zugriff hat.

☐ Bei uns ist es anders:

☐ Wir sollten unser bestehendes Konzept, das die Zugriffsberechtigungen regelt, überarbeiten und an die gesetzlichen Anforderungen anpassen.

☐ Wir sollten nur noch folgenden Personen Zugriff auf die Daten dieser Datenbearbeitung geben.

☐ Wir sollten die Zugriffsberechtigungen für folgende Personen einschränken oder entfernen:

☐ Wir sollten unsere Weisungen für den Zugriff auf die Datenbearbeitung anpassen:

☐ Wir sollten folgende zusätzlichen Sicherheitsmassnahmen (wie z.B. Protokollierung der Zugriffe) einführen:

☐ Wir sollten erheben, wer überhaupt Zugriff hat.

☐ Weil die Daten aus Sicht der betroffenen Personen besonders sensitiv sind, sollten wir zusätzliche Vorkehrungen einführen um zu überprüfen, ob wirklich nur die Personen Zugriff erhalten, die ihn brauchen.

☐ Wir sollten mit dem Anbieter unseres Systems prüfen, welche Zugangsberechtigungen möglich sind.

☐ Die **betriebsinterne Beschränkung** des Zugriffs wird bei uns:

- ☐ **Technisch** sichergestellt (z.B. Login, Protokollierung). → 2. **OK**
- ☐ **Organisatorisch** sichergestellt (z.B. Weisung, Überwachung). → 2. **OK**
- ☐ **Nicht genügend** sichergestellt, weil das von uns für die Datenbearbeitung benutzte System dies nicht unterstützt, obwohl wir meinen, es wäre erforderlich, dies sicherzustellen.
- ☐ Nicht sichergestellt, da **nicht erforderlich,** → 2. **OK**

☐ Wir haben uns zur Frage, wer im Betrieb Zugriff auf die Daten dieser Datenbearbeitung haben und wie dieser aussehen sollte **keine Gedanken** gemacht.

☐ Wir möchten noch Folgendes vermerken:

☐ Wir sollten unser System wechseln (oder anpassen), da es in der heutigen Form nicht mehr die erforderlichen Möglichkeiten zur Zugangskontrolle bietet.

☐ Andere Massnahme:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

- ☐ Weitere Abklärungen sind nötig
- ☐ Experte konsultieren

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

- ☐ Sollten wir weitermachen wie bisher.
- ☐ Treffen wir folgende Sofortmassnahmen:
- ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

Q13

Grundsatz der Verhältnismässigkeit VI ("Speicherbegrenzung")

Die Daten werden anonymisiert oder gelöscht, wenn sie für die festgelegten Bearbeitungszwecke nicht mehr benötigt werden. Werden sie nicht mehr für alle verfolgten Zwecke benötigt, ist der Zugriff entsprechend einzuschränken.

Art. [5] Abs. 2 DSG, Art. 5 Abs. 1 Bst. e DSGVO

Der Grundsatz der Verhältnismässigkeit (vgl. Q8) verlangt schliesslich, dass Daten nur so lange (in personenbezogener Form) bearbeitet werden, wie dies für die verfolgten Zwecke (Q5) erforderlich ist. Werden sie nicht mehr gebraucht, sollte das Unternehmen sie entweder löschen bzw. die Datenträger vernichten oder aber die Personendaten anonymisieren, d.h. sie so anpassen, dass eine Re-Identifizierung nicht mehr möglich ist.

Die DSGVO hält ferner fest, dass Personendaten darüber hinaus weiter verwendet werden dürfen, wenn dies öffentlichen Archivinteressen, wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken dient. Allerdings sind dann gewisse Massnahmen wie z.B. die Pseudonymisierung zu treffen (vgl. dazu Art. 89 DSGVO). Diese Ausnahmefälle sind hier nicht abgedeckt.

In der Praxis ist die Speicherbegrenzung einer der Anforderungen des Datenschutzes, die am wenigsten befolgt wird, da viele Unternehmen ihre Daten länger als erforderlich aufbewahren bzw. nie löschen oder dies auch gar nicht können. Ist es nicht möglich Daten zu löschen, obwohl dies erforderlich wäre, sollte immerhin versucht werden, den Zugriff so stark einzuschränken, dass sie im operativen Geschäft nicht mehr gebraucht werden (*Put Beyond Use*).

Kurz und bündig:

☐ Wir löschen (oder anonymisieren) die von uns bearbeiteten Daten (und zwar auch aus Backups und Archivkopien), sobald wir sie nicht mehr brauchen bzw. aufbewahren müssen, und haben dazu auch Fristen definiert. Werden die Daten nicht mehr von allen gebraucht, wird auch der Zugriff eingeschränkt. → **hier alles OK**

☐ Wir löschen unsere Daten grundsätzlich nicht, oder nur *ad-hoc*. Ein klares Konzept, wie lange die diversen Kategorien von Daten aufbewahrt werden sollen, haben wir nicht bzw. nicht umgesetzt.

Im Detail:

☐ Wir **löschen** die Personendaten dieser Datenbearbeitung **nie**, oder höchstens, wenn wir keinen Speicherplatz mehr haben oder in Sonderfällen (aber ohne Konzept),

  ☐ Wir könnten sie **mit der Zeit sicher löschen** (oder anonymisieren), müssten uns dazu aber ausserhalb dieses Self-Assessments vertieft Gedanken machen bzw. Abklärungen treffen.

☐ Wir haben **Fristen** definiert, **wie lange** wir die einzelnen Kategorien von Personendaten im Rahmen unserer Datenbearbeitung **aufbewahren**.

  ☐ Die Fristen gibt es für alle Daten,

  ☐ Die Fristen sind nur für folgende Daten bestimmt, für andere gibt es keine:

  ☐ Die Fristen sind angemessen, da die Fristen jeweils danach bestimmt wurden, wie lange wir meinen, die Daten aufgrund gesetzlicher Pflichten und unserer geschäftlichen Interessen (z.B. Beweiszwecke, historische Interessen, Vorlagen, Langzeitstatistiken) zu brauchen. → 1. **OK**

  ☐ Wir haben die Fristen nicht oder nicht alle danach geprüft, ob sie angemessen sind. Womöglich sind sie zu lang.

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

  ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.

  ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.

  ☐ *Soweit nur DSG anwendbar:*

  Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr.

  _____

  ☐ Anderer Grund:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig;**

  ☐ Wir sollten auf folgende Datenkategorien verzichten, da wir uns dann um die Aufbewahrungsfristen keine Gedanken mehr machen müssen;

  ☐ Wir sollten die Fristen für die Aufbewahrung für die folgenden Daten:

  wie folgt festlegen (danach Löschung/Anonymisierung):

☐ Wir haben **nicht definiert**, wie lange wir die Daten im Rahmen unserer Datenbearbeitung aufbewahren,

- ☐ Weil wir **nicht wissen**, wie lange wir die Daten wirklich brauchen,
  - ☐ Das gilt für **alle Daten,**
  - ☐ Das gilt für folgende Daten:

    [ ]
- ☐ Aber **wir wissen** eigentlich, wie lange wir die Daten normalerweise brauchen. Wir müssten es lediglich festhalten.

☐ Wir **löschen** oder **anonymisieren** die Personendaten unserer Datenbearbeitung normalerweise:

- ☐ **Nach Ablauf** der definierten **Aufbewahrungsfristen.**
  - ☐ Wir löschen **alle Daten.** → 2. **OK**
  - ☐ Wir löschen nur für die folgenden Daten:

    [ ]
    - ☐ Alle anderen Daten löschen wir **nie.**
    - ☐ Alle anderen Daten löschen wir wie folgt:

      [ ]
      - ☐ Wir löschen gar nicht, weil wir die Daten brauchen, **solange das Unternehmen existiert.** → 2. **OK**
  - ☐ Das geschieht **automatisch.** → 3. **OK**
  - ☐ Das geschieht **manuell.**
    - ☐ Wir machen das auch wirklich. → 3. **OK**

☐ Wir sollten festlegen, dass die folgenden Daten:

[ ]

nach folgender Frist mit eingeschränktem Zugriff archiviert bzw. versorgt werden können:

[ ]

☐ Wir sind noch nicht in der Lage, die fehlenden Fristen festzulegen, sollten aber als Massnahme schon jetzt festlegen, dass wir für folgende Datenkategorien:

[ ]

die Fristen definieren, nach welchen diese Daten:

- ☐ Mit eingeschränktem Zugriff archiviert bzw. versorgt werden können.
- ☐ Gelöscht oder anonymisiert werden können.

☐ Wir sollten dafür sorgen, dass die folgenden Daten:

[ ]

künftig fristgemäss

- ☐ gelöscht werden.
- ☐ anonymisiert werden.
- ☐ anderes behandelt werden, nämlich:

  [ ]

☐ **Nach anderen Kriterien**, nämlich:

☐ Wir **löschen** oder **anonymisieren** die Personendaten unserer Datenbearbeitung normalerweise **gar nicht.**

☐ Weil wir **alle** Daten brauchen **solange das Unternehmen existiert** (d.h. z.B. gesellschaftsrechtliche Dokumente). → 1.+2.+3.+4. **OK**

☐ Wenn wir von **löschen** bzw. **anonymisieren** sprechen:

☐ Dann meinen wir hier **löschen**, d.h. die Datensätze sind auf unseren Systemen grundsätzlich **nicht mehr vorhanden** (von Backups abgesehen). → 3. **OK**

☐ Dann meinen wir hier **anonymisieren**, d.h. wir passen die Daten so an, dass es unseres Erachtens vernünftigerweise **nicht mehr möglich ist** (jedenfalls für uns und jene, die Zugang zu den Daten haben) auf die **Identität der betroffenen Person zu schliessen.** → 3. **OK**

☐ Dann **sperren** wir hier die Daten, d.h. sie sind für die hier relevante Datenbearbeitung normalerweise nicht mehr nutzbar, aber:

☐ Wir **haben sie noch** im Unternehmen, weil sie für andere Datenbearbeitungen noch gebraucht werden; → 3. **OK**

☐ Sie sind weiterhin **auf dem System**, weil es technisch nicht möglich ist, sie zu löschen, → 3. **OK**

☐ Falls wir die Daten zwar **noch brauchen**, aber nicht mehr im täglichen Betrieb oder wir die Daten nur noch für besondere Zwecke brauchen (falls keins von beiden: → 4. **OK**), dann:

☐ **Schränken wir den Zugriff** darauf ein, so dass darauf grundsätzlich nur jene zugreifen können, die die Daten wirklich noch brauchen. → 4. **OK**

☐ Die Daten kommen in ein **Archiv** oder anderes System mit beschränktem Zugriff.

☐ Wir sollten dafür sorgen, dass die folgenden Daten mit eingeschränktem Zugriff archiviert bzw. versorgt werden, sobald sie im täglichen Betrieb nicht mehr gebraucht werden:

☐ Wir sollten ein Konzept erarbeiten, dass für die nötigen Löschfreigaben nach Ablauf der Aufbewahrungsfristen sorgt.

☐ Wir sollten folgende Systeme so anpassen, dass sie die Daten nach Ablauf der definierten Aufbewahrungsfristen tatsächlich löschen bzw. anonymisieren:

☐ Es handelt sich um eine Standardlösung. Daher sollten wir den Hersteller um Anpassung bitten.

☐ Wir sollten bei folgenden internen Stellen die fristgerechte Löschung unserer Daten sicherstellen:

☐ Archiv

☐ Wir sollten bei folgenden Auftragsbearbeitern die fristgerechte Löschung unserer Daten sicherstellen:

☐ Ob die Daten im Archiv je **gelöscht** werden, wissen wir nicht:

☐ Obwohl wir dafür zuständig wären.

☐ Doch ist dafür jemand anderer zuständig.

☐ Die **Zugriffsrechte** werden **eingeschränkt.**

☐ **Schränken wir** dennoch **nicht** oder nicht überall den Zugriff ein.

☐ Tun wir Folgendes:

☐ Die von uns bearbeiteten Daten werden auch **von anderen, internen Anwendungen übernommen** (abgesehen von den gemäss diesem Formular ausgeschlossenen Anwendungen), so dass wir nicht mehr kontrollieren können, ob diese fristgerecht gelöscht werden (falls nicht: → 5. **OK**).

☐ Für diese anderen Anwendungen sind **andere Stellen** zuständig, die auch für die Löschung verantwortlich sind. → 5. **OK**

☐ **Wir wissen nicht**, ob jemand sich um die fristgerechte Löschung kümmert.

☐ Für die fristgerechte Löschung sind **weiterhin wir zuständig** und wir haben das:

☐ Im Griff; → 5. **OK**

☐ Nicht im Griff,

☐ Wir setzen folgende **Auftragsbearbeiter** ein, die ebenfalls Daten von uns haben, die gelöscht werden müssen (falls nicht: → 6. **OK**):

☐ Wir sollten bei unseren folgenden Auftragsbearbeitern ermitteln, wann und wie sie Daten löschen bzw. anonymisieren und mit ihnen die nötigen Massnahmen zur Einhaltung der Fristen erarbeiten:

☐ Wir können jetzt noch keine konkrete Massnahme festlegen, aber sollten separat ein Konzept zur fristgerechten Löschung bzw. Anonymisierung der nicht mehr benötigten Daten erarbeiten.

☐ Andere Massnahme:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

☐ **Wir wissen nicht**, ob und wann unsere Daten gelöscht werden, weil sich darum die Auftragsbearbeiter kümmern.

☐ Unsere Auftragsbearbeiter sind **verpflichtet,** die bei sich gespeicherten Daten (ebenfalls) in den angegebenen Fristen **zu löschen.** → 6. **OK**

☐ Bei uns ist es anders:

☐ Wir löschen bzw. anonymisieren **nicht fristgerecht:**

☐ Weil unsere Systeme das **nicht können.**

☐ Weil wir **kein Verfahren zur Löschfreigabe** haben; es ist nicht bestimmt bzw. klar, wer die Löschung anweisen kann und muss.

☐ Weil eine Anpassung der Systeme und Abläufe **zu kostspielig** oder **zeitraubend** ist.

☐ Weil wir uns das **noch nie überlegt haben.**

☐ Weil wir uns **nicht sicher** sind, wann wir löschen können.

☐ Aus einem anderen Grund:

☐ Wir möchten noch Folgendes vermerken:

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

☐ Sollten wir weitermachen wie bisher.

☐ Treffen wir folgende Sofortmassnahmen:

☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

Q14

Grundsatz der Datenrichtigkeit

Es sind Vorkehrungen getroffen um sicherzustellen, dass die Personendaten im Hinblick auf ihren Zweck richtig und auf dem neusten Stand sind und bleiben. Unrichtige, veraltete bzw. unvollständige Daten werden korrigiert, aufdatiert, komplettiert oder gelöscht bzw. anonymisiert.

Art. [5] Abs. 5 DSG, Art. 5 Abs. 1 Bst. d DSGVO

Dass die Bearbeitung falscher (oder auch unvollständiger oder nicht mehr aktueller) Daten für die betroffene Person negative Konsequenzen haben kann, liegt auf der Hand. Aus diesem Grund verlangt der Datenschutz, dass Anstrengungen unternommen werden, um korrekte Daten zu beschaffen und sie auch in korrektem Zustand zu halten. Welches Mass an Richtigkeit verlangt wird, ergibt sich aus dem Zweck der verfolgt wird. Befindet sich in einer Datenbank für den Versand von Werbung eine veraltete Adresse, so ist dies in der Regel nicht problematisch für die betroffene Person. Ist die Adresse in der Datenbank der Kreditauskunftei falsch, kann dies dazu führend, dass die betroffene Person nicht gefunden oder verwechselt wird und eine für sie nachteilige Kreditauskunft erfolgt.

Der Verantwortliche muss einerseits selbst dafür sorgen, dass die von ihm bearbeiteten Daten über eine hinreichende Qualität aufweisen und behalten, dass er sie für seine Zwecke problemlos verwenden kann, und andererseits wird er auf Korrekturwünsche der betroffenen Personen eingehen müssen, was sich aus einer separaten Bestimmung ergibt (Q15), aber damit zusammenhängt.

Kann die Richtigkeit von Daten nicht mehr gewährleistet werden, müssen die Daten ggf. gelöscht (oder anonymisiert) werden. Daraus ergibt sich auch, dass Daten, die zu alt sind, um noch sinnvoll verwendet werden zu können, ebenfalls gelöscht werden müssen.

Kurz und bündig:

☐ Wir achten in dieser Datenbearbeitung laufend darauf, dass die Daten korrekt und aktuell sind, soweit das für unsere Zwecke relevant ist. Sind sie das nicht, wird i.d.R. korrigiert/aktualisiert, geht das nicht, gelöscht oder anonymisiert. → **hier alles OK**

☐ Die Qualität der Daten ist bei dieser Datenbearbeitung ungenügend.

Im Detail:

☐ **Wir wissen nicht**, ob die von uns bearbeiteten Daten **richtig** oder **vollständig** sind.

☐ Angesichts des Zwecks der Datenbearbeitung spielt es für die betroffene Person eigentlich **keine Rolle**, ob ihre Daten bei uns richtig und vollständig sind (z.B. ob ihre E-Mail-Adresse in unserem Newsletter-Verteiler noch gültig ist); es hat auf sie normalerweise **keine Auswirkungen**. → 1.+2. **OK**

☐ Um **sicherzustellen**, dass wir richtige und vollständige Daten erheben:

- ☐ Lassen wir die betroffenen Personen die Daten **selbst erfassen** bzw. übernehmen sie direkt von ihr (z.B. Website, Formular, App, Automat, Mail).
  - ☐ Wobei sie die Daten vor dem Abschluss des Vorgangs **nochmals überprüfen kann** (z.B. via Bestätigungsseite oder zweimalige Eingabe der E-Mail-Adresse). → 1. **OK**
  - ☐ Wir machen das nicht, aber wir meinen auch, dass das in Anbetracht der Umstände **nicht nötig** ist, weil es kaum zu relevanten Fehlern kommt. → 1. **OK**
  - ☐ Sie füllt sie **auf Papier** aus, und wir stellen sicher, dass die Formulare **korrekt erfasst** werden, → 1. **OK**
  - ☐ Es ist anders, aber **Fehler** bzw. unvollständige Daten **kommen nicht oft vor** oder werden von uns **bereinigt,** → 1. **OK**

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

- ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.
- ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.
- ☐ *Soweit nur DSG anwendbar:*

  Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr. _____
- ☐ Anderer Grund:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

- ☐ Wir sollten im Rahmen der Datenbeschaffung (zusätzliche) Vorkehrungen zur Sicherstellung der Datenqualität treffen:
  - ☐ Anpassung der Anforderungen an unsere Datenquellen.
  - ☐ Die betroffenen Personen stärker einbinden.
  - ☐ Zusätzliche Datenprüfungen vorsehen.
  - ☐ Andere:

- ☐ Wir haben **Probleme** mit fehlerhaften und unvollständigen Daten; die Situation ist **unbefriedigend,**

  [ ]

- ☐ Teilt uns die Person die Daten selbst **mündlich** mit.
  - ☐ Wir können **sicherstellen**, dass wir die Daten **korrekt erfassen**; nach unseren Erfahrungen ist die Datenqualität hinreichend gut. → 1. **OK**
- ☐ Verlassen wir uns auf unseren **Datenlieferanten**.
  - ☐ Er ist **vertraglich verpflichtet**, korrekte Daten zu liefern und wir haben keinen Grund zur Annahme, dass er dies nicht befolgt. → 1. **OK**
  - ☐ Nach unseren Erfahrungen ist die **Datenqualität hinreichend gut.** → 1. **OK**
- ☐ **Überprüfen** wir die Daten (z.B. auf Plausibilität) und meinen so, eine hinreichende Datenqualität sicherzustellen. → 1. **OK**
- ☐ Haben wir andere Vorkehrungen getroffen: → 1. **OK**

  [ ]

- ☐ **Unternehmen** wir **nichts Besonderes**, aber wir haben hinsichtlich der Datenqualität keine schlechten Erfahrungen gemacht, und die **Fehler**, die vorkommen, haben normalerweise **keine negativen Folgen** für die betroffenen Personen. → 1. **OK**

☐ Die von uns geführten Daten können **über Zeit veralten**, **nicht mehr richtig** oder **nicht mehr vollständig** sein.

- ☐ Das Nachführen der Daten **klappt** normalerweise **gut**, weil: → 2. **OK**
  - ☐ Es die betroffenen Personen **selbst machen** (z.B. über eine Online-Schnittstelle) oder uns mitteilen.
  - ☐ Wir von unseren Datenquellen **Updates** erhalten.

- ☐ Wir sollten (zusätzliche) Vorkehrungen treffen, um die Qualität der bei uns bereits vorhandenen Daten periodisch zu überprüfen und die Daten wenn nötig nachzuführen:
  - ☐ Häufigere Updates aus Drittquellen.
  - ☐ Den betroffenen Personen online die Möglichkeit zum Nachführen ihre Daten geben.
  - ☐ Die betroffenen Personen sonst stärker einbinden.
  - ☐ Zusätzliche Datenprüfungen vorsehen.
  - ☐ Andere:

    [ ]

- ☐ Wir sollten unsere Systeme anpassen, damit wir künftig auch die folgenden Daten korrigieren bzw. ergänzen können, wenn das nötig werden sollte:

  [ ]

- ☐ Wir sollten die folgenden Daten löschen bzw. anonymisieren, weil wir ihre Richtigkeit und Vollständigkeit nicht mehr gewährleisten können:

  [ ]

- ☐ Die Datenqualität ist nicht so, wie sie sein sollte. Weil sich das nicht kurzfristig verbessern lässt, sollten wir nicht mehr wie bisher auf diese Daten abstellen; wir müssen ein Konzept ausarbeiten, wie damit umzugehen ist.

☐ Wir die Daten **regelmässig** von uns aus **überprüfen.**

☐ Wir andere Vorkehrungen getroffen haben:

☐ Das Nachführen der Daten klappt **nicht zufriedenstellend**, wäre aber sinnvollerweise **nötig:**

☐ Wir haben dafür noch **keine Lösung**.

☐ Wir **löschen** bzw. **anonymisieren** die Daten daher nach einer gewissen Zeit, was das Problem mehr oder weniger löst. → 2. **OK**

☐ Wir haben eine andere Lösung gefunden: → 2. **OK**

☐ Das spielt letztlich **keine Rolle**, weil in unserer speziellen Situation die mangelhafte Qualität der Daten für die betroffenen Personen normalerweise **keine negativen Folgen.** → 2. **OK**

☐ In unserem speziellen Fall **veralten die Daten nicht** und werden daher auch **nicht falsch; sie sind, was sie sind** (z.B. chronologische Aufzeichnungen von Fakten). → 2. **OK**

☐ Wir möchten noch Folgendes vermerken:

☐ Andere Massnahme:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

☐ Sollten wir weitermachen wie bisher.

☐ Treffen wir folgende Sofortmassnahmen.

☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

Q15

Anspruch auf Berichtigung

Wenn eine betroffene Person es verlangt, werden unrichtige Personendaten korrigiert. Das Unternehmen hat die nötigen Vorkehrungen getroffen, um dies sicherzustellen.

Falls die DSGVO gilt:

Die Korrekturwünsche werden auch Dritten mitgeteilt, denen die (falschen) Daten zuvor mitgeteilt worden sind. Die Betroffenen können erfahren, wer diese Dritten sind, um ihre Ansprüche auch direkt geltend zu machen.

Art. [28] Abs. 1 DSG, Art. 16 DSGVO

Eine betroffene Person kann vom Verantwortlichen verlangen, dass ihre Daten berichtigt werden. Dies ist im Datenschutzrecht ausdrücklich so vorgesehen, ergibt sich aber auch aus dem Grundsatz der Datenrichtigkeit (Q14).

Unter der DSGVO kann sogar verlangt werden, dass der Verantwortliche die Korrekturwünsche auch an die Dritten weitergibt, die die (falschen) Daten erhalten haben, oder dass sie der betroffenen Person wenigstens genannt werden. Dazu muss das Unternehmen natürlich protokollieren, wem es welche Daten weitergibt.

In der Praxis kommen Berichtigungsgesuche nicht sehr häufig vor. Die meisten Unternehmen sind gut beraten, wenn sie intern die Zuständigkeit für die Bearbeitung solcher Gesuche festlegen, damit klar ist, wer sich darum kümmert, und diese Person weiss, was zu tun ist. Wichtig ist natürlich auch, dass die Daten sich technisch überhaupt berichtigen lassen, d.h. die Systeme eine nachträglich Anpassung bzw. Ergänzung der Personendaten überhaupt zulassen.

Kurz und bündig:

- ☐ Wenn eine betroffene Person die Korrektur ihrer Personendaten verlangt, so passen wir das in der Regel an. Es ist geregelt, wer dafür zuständig und die Systeme lassen solche Anpassungen auch zu. Soweit die DSGVO gilt, informieren wir auch Dritte, die die Daten von uns erhalten haben, über die Korrekturwünsche und auf Wunsch die betroffene Person, wer diese Dritten sind. → **hier alles OK**
- ☐ Wir sind bei dieser Datenbearbeitung auf etwaige Berichtigungsgesuche nicht wirklich vorbereitet.

Im Detail:

- ☐ Wenn eine betroffene Person von uns die **Korrektur** ihrer Daten verlangt:
  - ☐ Haben wir einen **definierten Prozess** mit Verantwortlichkeiten, wie mit solchen Anfragen umzugehen ist. → 1. **OK**
  - ☐ Haben wir **jemanden**, der sich darum kümmern wird und diese Person weiss, was sie zu tun hat oder wird sich kundig machen. → 1. **OK**
  - ☐ Ist uns **nicht wirklich klar**, wie wir mit solchen Anfragen in organisatorischer Hinsicht umgehen würden.
- ☐ Wenn betroffene Personen im Rahmen der vorliegenden Datenbearbeitung ihre Daten korrigiert haben wollen, **verfahren wir wie folgt:**
  - ☐ Wir **erfüllen** solche Wünsche normalerweise **vorbehaltlos** und dies mit Bezug auf **alle Daten.**
    - ☐ Wir **stellen dabei sicher**, dass es sich wirklich um die **betroffene Person** handelt. → 2. **OK**
  - ☐ Wir **erfüllen** diesen Wunsch in folgenden Fällen **nicht:**
    - ☐ Die Korrektur gewisser Daten macht **im Hinblick auf den Zweck** der Daten **keinen Sinn** (z.B. weil die Daten etwas dokumentieren, was in der Vergangenheit geschehen ist oder weil die Daten nicht mehr benutzt werden); dort ändern wir nichts.
    - ☐ Die Korrektur oder Vervollständigung gewisser Daten ist uns **gesetzlich verboten**; dort ändern wir nichts.

- ☐ Es sind unseres Erachtens **keine Massnahmen nötig:**
  - ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.
  - ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.
  - ☐ Anderer Grund:

- ☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**
  - ☐ Wir sollten einen Prozess zur Behandlung von Berichtigungsgesuchen definieren und einführen.
  - ☐ Wir sollten festlegen, wer intern für die Behandlung von Berichtigungsgesuchen verantwortlich ist und sicherstellen, dass die zuständige Person weiss, was zu tun ist (oder dies bei Bedarf herausfinden kann).
  - ☐ Wir sollten unsere Systeme anpassen, damit wir künftig auch die folgenden Daten korrigieren bzw. ergänzen können, wenn das nötig werden sollte:
  - ☐ Wir sollten unsere Systeme so anpassen, damit wir künftig dort, wo wir die Daten nicht korrigieren wollen, mindestens einen Bestreitungsvermerk angeben können.
  - ☐ Wir sollten aufzeichnen, wem wir unsere Daten zur eigenen Benutzung zur Verfügung stellen, damit wir diese Dritten im Falle eines Korrekturwunsches informieren können bzw. der betroffenen Person die Namen mitteilen können.

- ☐ Gewisse Daten werden **zu Archivzwecken im öffentlichen Interesse** bearbeitet; dort ändern wir nichts.
- ☐ Wenn der Wunsch jenseits von Gut und Böse ist, nur dazu dient uns zu **schikanieren**.
- ☐ Wenn uns nicht klar, ob es sich wirklich um die betroffene Person handelt, weisen wir den Wunsch zurück, bis die Person ihre **Identität belegt.**
- ☐ Wenn wir der Meinung sind, dass die gewünschte Korrektur **inhaltlich unbegründet**, d.h. nicht belegt ist, dass die Daten falsch sind (würde die Person klagen, könnte sie immerhin vermerken lassen, dass die Richtigkeit der Daten bestritten ist).
- ☐ Wenn die Person die Änderungen **selbst vornehmen könnte** (z.B. über ein Online-Konto) und es keine guten Gründe gibt, warum sie dies nicht auch selbst tut.
- ☐ Wir meinen **nicht**, dass wir den Wunsch aus anderen Gründen als vorstehend angegeben **zurückweisen** würden. → 2. **OK**

☐ Obwohl dies vermutlich nicht zulässig wäre, kann es sein, dass wir Korrekturwünsche auch **in folgenden Fällen zurückweisen:**

- ☐ Gewisse Daten können in unseren Systemen nicht nachträglich geändert werden und es ist auch **nicht möglich**, solche Änderungen oder Ergänzungen anders zu vermerken:

- ☐ Eine **Änderung** der Daten würde in diesen Fällen allerdings auch **keinen Sinn machen**, weil sie lediglich **objektiv wiedergeben, was geschehen ist** (z.B. Videoaufzeichnungen, Zugriffsprotokolle). → 2. **OK**

- ☐ Andere Massnahme:
- ☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

- ☐ Weitere Abklärungen sind nötig
- ☐ Experte konsultieren

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

- ☐ Sollten wir weitermachen wie bisher.
- ☐ Treffen wir folgende Sofortmassnahmen.
- ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

☐ Weil es für uns **zu aufwändig** wäre.

☐ Aus anderen Gründen:

☐ Wir könnten **alle diese Wünsche**, mit denen wir realistischerweise rechnen müssen, mit unseren Systemen mit vertretbarem Aufwand **erfüllen**, wenn wir müssten. → 2. **OK**

Soweit nur DSGVO anwendbar (nur nächster Punkt):

☐ Wir machen unsere Daten auch **Dritten für deren eigene Nutzung zugänglich**. (wenn nein: → 3. + 4. **OK**).

☐ Wir **informieren diese Dritten** über den Korrekturwunsch, soweit dies für uns möglich ist und keinen unverhältnismässigen Aufwand mit sich bringt. Dazu stellen wir sicher, dass wir wissen, wen wir bei einem Korrekturwunsch informieren müssen. → 3. **OK**

☐ Wir **informieren** die betroffenen Personen, die das wissen wollen, darüber, **wer diese Dritten sind.** Dazu stellen wir sicher, dass wir wissen, wer diese Dritten sind, sollten wir mit einer solchen Anfrage konfrontiert werden. → 4. **OK**

☐ Wir möchten noch Folgendes vermerken:

Q16

Bekanntgabe ins Ausland

Es werden Daten in der Schweiz einer Person oder Stelle ausserhalb der Schweiz nur dann übermittelt (ob durch aktive Mitteilung oder Zugreifenlassen), wenn ein angemessener Datenschutz sichergestellt oder eine der gesetzlich vorgesehenen Ausnahme gegeben ist, wie z.B. das Vorliegen einer Einwilligung, die Abwicklung eines Vertrags oder die Vorlage von Beweismitteln für ausländische Prozesse. Dasselbe gilt für Übermittlungen von Daten von der EU bzw. dem EWR in ein Land, welches nicht zur EU bzw. dem EWR gehört.

Art. [13] f. DSG, Art. 44–49 DSGVO

Werden Daten in ein Land ohne angemessenen gesetzlichen Datenschutz übermittelt, ist dies nur zulässig, wenn der angemessene Datenschutz entweder auf andere Weise (insbesondere mittels Vertrag) sichergestellt wird, oder aber eine der Ausnahmegründe (wie z.B. die Durchführung eines Gerichts- oder Behördenverfahrens im Ausland) gegeben ist. Ob ein Land über einen angemessenen Datenschutz verfügt und somit ein sicheres Drittland ist, bestimmt in der EU die Europäische Kommission und in der Schweiz unter dem revidierten DSG der Bundesrat, wobei er in der Regel die Entscheide der EU übernimmt.

Kurz und bündig:

☐ Es gehen keine Daten ins Ausland, und es gibt auch keinen Fernzugriff. → **hier alles OK**

☐ Wenn wir hier Daten mit Personen ausserhalb Europas zugänglich machen, dann nur, wenn diese entweder (i) in einem sicheren Drittland sind, (ii) als US-Unternehmen "Privacy Shield"-zertifiziert sind, (iii) einen Datenschutzvertrag abgeschlossen haben oder (iv) eine der gesetzlichen Ausnahmen greift (z.B. Prozess im Ausland, Vertragsabwicklung, Einwilligung). → **hier alles OK**

Im Detail:

☐ Im Rahmen dieser Datenbearbeitung fliessen **keine Daten ins Ausland**, auch nicht per Fernzugriff. → **hier alles OK**

☐ Im Rahmen dieser Datenbearbeitung kommt die Übermittlung von Daten ins Ausland einzig **an die betroffene Person selbst** vor. → **hier alles OK**

☐ Daten dieser Datenbearbeitung **fliessen aus der Schweiz ins Ausland** (falls nicht: → 1. **OK**; falls Daten aus der EU/dem EWR fliessen s. unten), doch sind alle folgenden **Anforderungen**, soweit anwendbar, vollständig **erfüllt** oder aber sie sind für gewisse Übermittlungen erfüllt (Ausnahmen unten).

  ☐ Daten gehen in andere Länder **Europas** oder in einen **anderen Staat**, der über ein **angemessenes gesetzliches Datenschutzniveau** verfügt (die Liste der Staaten ist hier abrufbar): Keine weiteren Anforderungen: → 1. **OK**

  ☐ Daten gehen an ein **US-Unternehmen**, das für die betreffenden Daten gemäss dem "**US-CH-Privacy Shield Framework**" zertifiziert ist (die Liste der Unternehmen ist hier abrufbar): Keine weiteren Anforderungen: → 1. **OK**

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

  ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.

  ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.

  ☐ Anderer Grund:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

  ☐ Wir sollten für folgende Übermittlungen von Personendaten ins Ausland mit den Empfängern Verträge abschliessen, um einen angemessenen Datenschutz zu gewährleisten:

    ☐ Dazu verwenden wir die EU-Musterklauseln, da diese allgemein akzeptiert sind.

  ☐ Wir sollten für folgende Übermittlung von Personendaten ins Ausland prüfen, ob wir uns auf eine der Ausnahmen (oder anderen Garantien) abstützen können:

    ☐ In Frage kommt insbesondere eine ausdrückliche Einwilligung.

    ☐ In Frage kommt insbesondere der Rechtfertigungsgrund der Vertragsanbahnung und -abwicklung.

    ☐ In Frage kommt insbesondere der Rechtfertigungsgrund der Durchsetzung etc. von Rechtsansprüchen.

Innerhalb von Europa (einschliesslich Schweiz) ist die grenzüberschreitende Bekanntgabe von Personendaten keinen weiteren Einschränkungen unterworfen. Die Schweiz gilt aus Sicht der EU bzw. des EWR als sicherer Drittstaat und umgekehrt ebenfalls. Bei der Beurteilung der Datenbearbeitung ist trotz allem auf die Differenzierung zwischen dem DSG und der DSGVO zu achten: Unter der DSGVO gilt die Übermittlung innerhalb der EU (und des EWR) nicht als Übermittlung in ein Drittland (die EU gilt insgesamt als Binnenmarkt), während aus Sicht der DSG auch die Übermittlung aus der Schweiz in die EU eine grenzüberschreitende Bekanntgabe im Sinne des Gesetzes darstellt.

Die Regelungen für grenzüberschreitende Bekanntgaben sind weitgehend gleich. Werden Daten in ein unsicheres Drittland übermittelt, werden in der Praxis vor allem die Musterverträge der Europäischen Kommission verwendet; sie können ohne Notifikation der Behörden und ohne weitere Genehmigung eingesetzt werden. Da die Regeln für die grenzüberschreitende Bekanntgabe auch innerhalb von Unternehmensgruppen gilt, schliessen solche meistens multilaterale Datenübermittlungsverträge (ein sog. *Intra Group Data Transfer Agreement, IGDTA*), welche den Datenfluss zwischen den Gruppengesellschaften gemäss den Vorgaben des DSG und der DSGVO regeln. Alternativ können auch sog. Binding Corporate Rules vereinbart werden, die ähnlich funktionieren, aber nicht strikte den vorab genehmigten Musterklauseln der Europäischen Kommission folgen, damit flexibler sind, aber auch separat und einzeln genehmigt werden müssen.

Für die Datenbearbeitung bedeutet dies, dass typischerweise zwischen gruppeninternen und gruppenexternen Übermittlungen ins Ausland unterschieden werden muss (wobei als Übermittlung auch jeder Fernzugriff zählt), weil diese in der Praxis meist unterschiedlich geregelt sind. Idealerweise besteht in einer Unternehmensgruppe ein IGDTA, das alle gruppeninterne Bekanntgaben mit einem Schlag regelt, während Übermittlungen an Dritte, ob Auftragsbearbeiter oder Verantwortliche, typischerweise bilateral geregelt werden müssen.

☐ In allen **anderen Fällen**:

Es ist einer der folgenden Fälle gegeben: → 1. **OK**

- ☐ Mit dem Empfänger im Ausland wurden die **EU-Musterklauseln** für die grenzüberschreitende Bekanntgabe von Personendaten (oder andere, vom EDÖB anerkannte bzw. genehmigte Standardvertragsklauseln, hier abrufbar) **vereinbart.**
  - ☐ Es geht um einen **Gruppen-internen Datenfluss**. Dieser ist durch einen **multilateralen Datentransfer-Vertrag** (IGDTA oder ähnlich) auf Basis der EU-Musterklauseln geregelt.
- ☐ Mit dem Empfänger im Ausland wurde ein **anderer Vertrag vereinbart**, der diese zur Einhaltung eines angemessenen Datenschutzes verpflichtet und vom EDÖB genehmigt wurde bzw. wird oder der dem EDÖB mitgeteilt wurde.
- ☐ Es geht um einen **Unternehmens- oder Gruppen-internen Datenfluss**, und eine für alle beteiligten Personen und Stellen **verbindliche Regelung** (z.B. Vertrag) stellt sicher, dass ein angemessener Datenschutz eingehalten wird (sog. ***Binding Corporate Rules***). Diese Regelung ist vom EDÖB oder einer anderen, von ihm anerkannten Stelle genehmigt oder wird es.
- ☐ Ein **völkerrechtlicher Vertrag** stellt den angemessenen Datenschutz sicher.
- ☐ Wir übermitteln die Daten in der Eigenschaft als **Bundesorgan** und haben zur Sicherstellung des Datenschutzes im Ausland entsprechende Garantien ausgehandelt bzw. vorgesehen und diese dem EDÖB mitgeteilt

- ☐ Wir sollten prüfen, ob wir bei der Lieferung von Daten für ausländische Gerichts- und Behördenverfahren jeweils die nötigen Schutzvorkehrungen treffen (Protective Orders, Schwärzung von Kunden- und Mitarbeiternamen, Vorabinformation, etc.).
- ☐ Die grenzüberschreitenden Datenflüsse innerhalb der Unternehmensgruppe sind nicht geregelt. Wir sollten ein *Intra-Group Data Transfer Agreement* (IGDTA) abschliessen, d.h. einen multilateralen Datentransfer-Vertrag auf Basis der EU-Musterklauseln.
- ☐ Ein IGDTA bietet uns zu wenig Flexibilität. Wir sollten daher den Abschluss von Binding Corporate Rules prüfen, auch wenn dies einen grösseren Aufwand und eine Genehmigung durch die Datenschutzbehörden erfordert.
- ☐ Wir sollten die Übermittlung von Personendaten ins Ausland in den folgenden Fällen einschränken oder beenden, weil wir die gesetzlichen Anforderungen nicht erfüllen:
- ☐ Andere Massnahme:
- ☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

	Für die USA gilt eine spezielle Regel: Hat sich ein Unternehmen in den USA unter dem "privacy shield"-Programm selbstzertifiziert (was für die EU und die Schweiz möglich ist), gelten Übermittlungen an dieses Unternehmen als Übermittlung in einen sicheren Drittstaat. Ansonsten hat die USA nicht den Status eines sicheren Drittstaates. Für die vorliegende Datenbearbeitung ist somit in einem ersten Schritt zu überprüfen, ob und wohin ins Ausland Daten übermittelt werden (einschliesslich durch die Möglichkeit von Fernzugriffen) und in einem zweiten Schritt, wie die der Datenschutz am Ort des Empfängers geschützt sind oder ob ggf. eine der Ausnahmebestimmungen greift. In der überwiegenden Zahl der Fälle werden Übermittlungen in unsere Drittstaaten heute auf vertraglicher Basis abgesichert.	☐ Wir können uns in den nachfolgend beschriebenen Übermittlungen ins Ausland auf eine der folgenden **Ausnahmen** berufen: ☐ Die Daten gehen **an die betroffene Person selbst**, die sich im Ausland befindet (gilt als Fall der Einwilligung). ☐ Es liegt uns eine ausdrückliche Einwilligung der betroffenen Personen vor, und diese ist nicht zurückgezogen. Sie wurden darüber informiert, dass ihre Daten ins Ausland gehen und dort nicht mehr einem Datenschutz wie in der Schweiz unterliegen. Darüber hinaus erfüllen die Einwilligungen die Anforderungen an eine **gültige, ausdrückliche Einwilligung** gemäss Q1 in Abschnitt A von Formular E.4.: ☐ Die Übermittlung der Daten ins Ausland steht in **unmittelbarem Zusammenhang** mit dem **Abschluss oder der Abwicklung eines Vertrags**, welchen die betroffene Person selbst abgeschlossen hat oder abschliessen will oder der in ihrem Interesse von einem Dritten abgeschlossen wurde oder werden soll: ☐ Wir **dokumentieren** diese Fälle, damit wir den EDÖB auf Anfrage informieren können.	☐ **Situation unklar** Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren ☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen ☐ Sollten wir weitermachen wie bisher. ☐ Treffen wir folgende Sofortmassnahmen: ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

☐ Die Übermittlung der Daten ins Ausland ist **nötig** zur **Wahrung eines öffentlichen Interesses**, und dieses öffentliche Interesse **überwiegt die Risiken**, welcher die betroffene Person aufgrund eines fehlenden gesetzlichen Datenschutzes gemäss europäischen Vorbild ausgesetzt ist:

☐ Wir **dokumentieren** diese Fälle, damit wir den EDÖB auf Anfrage informieren können.

☐ Die Übermittlung der Daten ins Ausland ist nötig für die **Feststellung**, **Ausübung** oder **Durchsetzung** von **Rechtsansprüchen** vor einem Gericht oder einer anderen zuständigen ausländischen Behörde; dies umfasst u.a. die Datenlieferung im Rahmen einer Pre-Trial-Discovery, die Mitwirkung an ausländischen Behördenuntersuchungen und die Mitwirkung in Verfahren ausländischer Aufsichtsbehörden:

☐ Im Falle von Datenlieferung für **US-Gerichtsverfahren** zielen wir auf den Abschluss von sog. *Protective Orders* zum Schutz der Personendaten vor Offenlegung und Verwendung der Daten ausserhalb des Verfahrens und prüfen etwaige Schwärzungen zum Schutz der Mitarbeiter und Dritter.

☐ Im Falle von Datenlieferungen für **US-Behörden** prüfen wir jeweils, ob wir Namen von Kunden, Mitarbeitern und Dritten schwärzen oder diese vorgängig informieren müssen.

☐ Wir **merken** uns diese Fälle, damit wir den EDÖB auf Anfrage informieren können.

☐ Die Bekanntgabe der Daten ins Ausland ist **nötig**, um **Leib oder Leben zu schützen** und es bleibt jeweils keine Zeit zum Einholen einer Einwilligung:

☐ Wir **dokumentieren** diese Fälle, damit wir den EDÖB auf Anfrage informieren können.

☐ Es werden Daten ins Ausland übermittelt, die aus einem **öffentlich zugänglichen Register** stammen; soweit für die Einsichtnahme ins Register ein **Interessennachweis** erforderlich ist, ist dieser auch für die Übermittlung ins Ausland nötig.

☐ Daten dieser Datenbearbeitung **fliessen aus der Schweiz ins Ausland**, doch wir **erfüllen** die obigen **Anforderungen** bei folgenden Übermittlungen **nicht:**

☐ In allen anderen Fällen hingegen schon, es kommen folgende **Garantien** bzw. **Ausnahmen** zur Anwendung:

☐ Wie im vorangehenden Punkt vermerkt.

☐ Soweit Daten **von einem Verantwortlichen oder Auftragsbearbeiter in der EU** bzw. dem **EWR in ein Land fliessen, das nicht der EU bzw. dem EWR angehört** (falls nicht: → 2. **OK**):

☐ Sind **keine besonderen Vorkehrungen nötig**, wenn die Daten lediglich in die Schweiz oder ein anderes Land fliessen, das **von der EU als Land mit angemessenem Datenschutz anerkannt** ist (die Liste ist hier abrufbar). → 2. **OK**

- ☐ Sind ansonsten **besondere Vorkehrungen** analog der obigen Anforderungen zu treffen, sofern keine Ausnahme analog der obigen Ausnahmen gegeben ist nach DSGVO.
  - ☐ Wir haben das geprüft und die Anforderungen sind **erfüllt.** → 2. **OK**
  - ☐ Wir haben das geprüft und die Anforderungen sind **nicht erfüllt.**
  - ☐ Wir haben das **nicht geprüft.**
- ☐ Wir möchten noch Folgendes vermerken:

Q17

Grundsatz der Datensicherheit

Es sind Massnahmen getroffen worden um eine angemessene Datensicherheit zu gewährleisten, d.h. sicherzustellen, dass die bearbeiteten Daten nicht unbeabsichtigt oder unbefugt zugänglich, geändert oder vernichtet werden oder verloren gehen. Die Massnahmen haben dem Risiko entsprechend zu erfolgen, d.h. hängen davon ab, wie wahrscheinlich ein Vorfall ist und wie gewichtig seine Konsequenzen sein können.

Art. [7] DSG, Art. 5 Abs. 1 Bst. f DSGVO, Art. 32 DSGVO

Datensicherheit ist nicht gleich Datenschutz, sondern nur ein Aspekt des Datenschutzes. Datensicherheit 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 der Datensicherheit sind z.B. die Verschlüsselung bzw. Pseudonymisierung, Zugang nur mit persönlichem Login, Firewalls, Protokolle. Organisatorische Massnahmen sind Weisungen, Schulungen, Audits, Kontrollen.

In den meisten Unternehmen ist eine eigene Stelle für die Gewährleistung der Datensicherheit zuständig. Daher wird hier nicht näher auf die Datensicherheit eingegangen, mit welcher die Datenbearbeitung geschützt wird. Es wird lediglich abgefragt, ob eine hinreichende Datensicherheit (auch) bezüglich der hier diskutieren Datenbearbeitung besteht.

Kurz und bündig:

☐ Die Datensicherheit ist bei uns gewährleistet. Darum kümmert sich eine eigene Stelle. → **hier alles OK**

☐ Um die Datensicherheit haben wir uns bei dieser Datenbearbeitung bis jetzt nicht gekümmert.

Im Detail:

☐ Die Datensicherheit dieser Datenbearbeitung ist **bereits beurteilt** und für **angemessen** befunden worden. Wir behandeln sie hier daher nicht weiter. → **hier alles OK**

  ☐ Sie ist **übergreifend** (d.h. nicht bezogen auf diese Datenbearbeitung) **geregelt** und in → Formular F.2 zu DB-Nr. _____ dokumentiert.

☐ Die Datensicherheit aller von dieser Datenbearbeitung betroffenen Systeme wurde nach ISO 27001 oder einem vergleichbaren Standard **erfolgreich zertifiziert** und etwaige festgestellte nennenswerte Defizite behoben. → **hier alles OK**

☐ Wir haben **Massnahmen zur Datensicherheit** getroffen, wie in → Formular F.2 zu DB-Nr. _____ dokumentiert.

  ☐ Wir kommen darin zum Schluss, dass diese Massnahmen dem Risiko entsprechend **angemessen** sind. → **hier alles OK**

  ☐ Wir kommen darin zum Schluss, dass diese Massnahmen **dem Risiko gut** sind, aber noch verbessert werden müssen.

  ☐ Wir kommen darin zum Schluss, dass diese Massnahmen **dem Risiko noch völlig ungenügend** sind.

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

  ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.

  ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.

  ☐ *Soweit nur DSG anwendbar:*

  Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr. _____

  ☐ Anderer Grund:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

  ☐ Wir sollten die Risiken einer Verletzung der Datensicherheit näher beurteilen, da wir nicht sicher sind, ob sie angemessen adressiert sind. Sorgen bereitet uns insbesondere:

  ☐ Wir sollten die für die Datensicherheit bei uns zuständigen Stellen um eine Einschätzung der Angemessenheit der Datensicherheit bitten.

  ☐ Wir sollten folgende zusätzlichen Massnahmen zur Datensicherheit treffen:

    ☐ Vorzeitige Pseudonymisierung oder Verschlüsselung der Daten, um das Risiko bei unerwünschten Zugriffen weiter zu reduzieren.

☐ Wir haben **keine Massnahmen** zur Datensicherheit getroffen.

☐ Alle Daten, die wir bearbeiten, sind **öffentlich**, wenn wir sie ganz oder teilweise verlieren macht das nichts, ebenso nichts, wenn sie manipuliert werden. → **hier alles OK**

☐ Wir möchten noch Folgendes vermerken:

☐ Andere Massnahme:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

☐ Sollten wir weitermachen wie bisher.

☐ Treffen wir folgende Sofortmassnahmen:

☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

Q18

Grundsatz des "Privacy by Design"

Es wurden Vorkehrungen getroffen, um sicherzustellen, dass die Bearbeitungsgrundsätze (Transparenz, Zweckbindung, Datensparsamkeit, Datenrichtigkeit, Speicherbegrenzung) eingehalten werden. Insbesondere wurden die Systeme datenschutzfreundlich ausgestaltet und die Mitarbeiter entsprechend instruiert.

Art. [6] Abs. 1 und 2 DSG, Art. 25 Abs. 1 DSGVO

Der Grundsatz des *Privacy by Design* ergänzt die Datensicherheit dahingehend, dass er technische und organisatorische Massnahmen verlangt, die ergänzend zur Gewährleistung der Datensicherheit (Q17) die Einhaltung der diversen Bearbeitungsgrundsätze und sonst des Datenschutzes sicherstellen. Der Hinweis "by Design" will sagen, dass diese Massnahmen schon in der Konzeption einer Datenbearbeitung bedacht werden müssen, damit die Grundsätze von Anfang eingehalten werden.

Hintergrund ist dabei die Überlegung, dass die zur Datenbearbeitung benutzte Systeme (z.B. Softwareanwendungen) bereits so ausgestaltet und einschränkt sind, dass eine datenschutzwidrige Nutzung möglichst schon durch diese technischen Massnahmen verhindert wird. Werden die Daten z.B. automatisch nach einer bestimmten Zeit gelöscht, kommt es nicht mehr darauf an, dass sich ein Mensch daran erinnert, dies zu tun. Wer die Einhaltung der Zweckbindung sicherstellen will, wird wiederum nur denjenigen Mitarbeitern Zugang zu einer Datenbearbeitung geben, die diesen für ihre Arbeit (bzw. die verfolgten Zwecke) benötigen. Wer die Datenrichtigkeit sicherstellen will, baut im Rahmen der Datenerfassung Plausibilisierungskontrollen ein und lässt die betroffene Person die Daten vor der Speicherung

Kurz und bündig:

☐ Wir haben versucht, die Vorgaben des Datenschutzes in der Ausgestaltung und Konfiguration unserer Systeme bereits zu berücksichtigen und schulen unsere Mitarbeiter ebenfalls im Datenschutz. → **hier alles OK**

Im Detail:

☐ Die für die Datenbearbeitung benutzten **Systeme** sind – soweit mit vertretbarem Aufwand möglich – so ausgestaltet, dass: → 1. **OK**

- ☐ Dort, wo betroffene Personen mit ihnen in Kontakt kommen, für sie **möglichst transparent** gemacht wird, was mit ihren Daten geschieht ("**Transparenz**").
- ☐ Die Daten möglichst **nur für die vordefinierten Zwecke** und nicht anders genutzt werden können ("**Zweckbindung**").
- ☐ Die **Erhebung** von Daten und deren **Gebrauch** auf ein **Minimum** beschränkt wird ("**Datensparsamkeit**").
- ☐ Die Daten **möglichst richtig** und auf dem neusten Stand sind und bleiben, und ansonsten korrigiert oder gelöscht werden ("**Datenrichtigkeit**"), und.
- ☐ Die Daten **nicht länger als nötig behalten** werden, d.h. so bald wie möglich pseudonymisiert werden und so bald wie möglich gelöscht oder anonymisiert werden ("**Speicherbegrenzung**").
- ☐ Die betroffenen Personen soweit in Anbetracht des Verwendungszwecks **möglich selbst über die Bearbeitung ihrer Daten bestimmen können** ("**informationelle Selbstbestimmung**").

☐ Die **Mitarbeiter** wurden im Rahmen der Datenbearbeitung angewiesen bzw. sind **instruiert** und soweit nötig geschult: → 2. **OK**

- ☐ Was sie mit den Daten **wie machen dürfen** bzw. wie und **wozu** die Daten benutzt werden dürfen.
- ☐ Was die **Bearbeitungsgrundsätze** bedeuten und wie sie sie einhalten müssen (Transparenz, Zweckbindung, Datensparsamkeit, Datenrichtigkeit, Speicherbegrenzung).

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

- ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.
- ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.
- ☐ *Soweit nur DSG anwendbar:*

  Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr.

  _____
- ☐ Anderer Grund:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

- ☐ Wir sollten unser für die Datenbearbeitung benutztes System:

  im Hinblick auf folgende Aspekte datenschutzfreundlicher ausgestalten:

  - ☐ Transparenz
  - ☐ Zweckbindung
  - ☐ Datensparsamkeit
  - ☐ Datenrichtigkeit
  - ☐ Speicherbegrenzung
  - ☐ Informationelle Selbstbestimmung

überprüfen. Auch die Pseudonymisierung von Daten ist eine oft zitierte Massnahme, weil sie das Risiko eines Missbrauchs der Daten reduzieren kann.

Als Massnahmen kommen auch solche organisatorischer Natur in Frage. Wichtig sind hier Weisungen, Schulungen und Kontrollen.

Vorliegend ist zu prüfen, ob im Rahmen der Datenbearbeitung besondere Massnahmen zur Einhaltung der Bearbeitungsgrundsätze getroffen wurden, insbesondere technischer Natur (d.h. Programmierung und Konfiguration der Anwendungen). Die Erfahrung zeigt, dass die meisten Unternehmen Schwierigkeiten haben, diese Anforderung zu fassen bzw. sich vorstellen zu können, welche Massnahmen in ihrem Fall hier gemeint sein könnten bzw. zu treffen sind. In diesem Fall lohnt es sich, die Bearbeitungsgrundsätze Punkt für Punkt durchzugehen und zu prüfen, ob und was an Massnahmen ergriffen wurde bzw. wird, um die Einhaltung sicherzustellen.

Wie weit dabei gegangen werden muss, hängt letztlich vom Risiko negativer Folgen für die betroffene Person und der Schwere des Eingriffs in ihre Privatsphäre ab.

- ☐ Dass sie es **den betroffenen Personen** soweit in Anbetracht des Verwendungszwecks möglich **erlauben**, **selbst über die Bearbeitung ihrer Daten bestimmen** zu können ("informationelle Selbstbestimmung").

☐ Die Mitarbeiter wurden in diesen Dingen zwar **nicht unterwiesen**, aber wir gehen davon aus, dass ihnen dies aufgrund ihres Fach- bzw. Branchenwissens bzw. ihrer Erfahrung **klar** ist. → 2. **OK**

☐ Wir können **davon ausgehen**, dass sie sich **an diese Dinge halten.** → 3. **OK**

- ☐ Weil wir das immer wieder **überprüfen.**
- ☐ Weil das unsere **bisherige Erfahrung** zeigt.
- ☐ Weil sie über **entsprechendes Know-how verfügen** und aus unserer Sicht **zuverlässig** sind.

☐ Die vorstehenden Anforderungen betr. Mitarbeiter sind auch mit Bezug auf **andere beigezogene Dritte** erfüllt. → 4. **OK**

☐ Wir ziehen **keine Dritten** bei. → 4. **OK**

☐ Wir möchten noch Folgendes vermerken:

☐ Wir sollten den Lieferanten unseres Systems zu einer datenschutzfreundlicheren Gestaltung drängen, insbesondere bei Software, für welche wir einen Wartungsvertrag haben:

☐ Wir sollten mit Bezug auf die Mitarbeiter speziell für die Datenbearbeitung eigene:

- ☐ Datenschutz-Weisungen erstellen.
- ☐ Datenschutz-Schulungen durchführen.
- ☐ Umsetzungskontrollen durchführen.

☐ Wir sollten mit Bezug auf beigezogene Dritte speziell für die Datenbearbeitung eigene:

- ☐ Datenschutz-Weisungen erstellen bzw. die Verträge entsprechend anpassen.
- ☐ Datenschutz-Schulungen durchführen.
- ☐ Umsetzungskontrollen durchführen.

☐ Wir sollten die folgenden Weisungen anpassen:

☐ Andere Massnahme:

			☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern: ☐ **Situation unklar** Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren ☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen ☐ Sollten wir weitermachen wie bisher. ☐ Treffen wir folgende Sofortmassnahmen: ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

Q19

Grundsatz des "Privacy by Default"

Nur, wenn ein Service angeboten wird, bei welchem die betroffene Person Datenschutzeinstellungen vornehmen kann:

Die Person wird zu Beginn gefragt, welche Einstellungen sie haben möchte, oder aber sie sind standardmässig so, dass möglichst nichts mit den Daten geschieht.

Art. [6] Abs. 3 DSG, Art. 25 Abs. 2 DSGVO

Das Gebot *Privacy by Default* wurde mit Blick auf Online-Dienste wie Facebook entwickelt. Es soll sicherstellen, dass wenn ein solcher verschiedene Einstellungen zum Datenschutz erlaubt, jene Einstellungen voreingestellt sein sollen, bei welchen die Daten des Nutzers am wenigsten intensiv bzw. weitgehend genutzt werden. Will der Benutzer, dass mit seinen Daten mehr gemacht wird, muss er sich dafür aktiv entscheiden und die entsprechenden Einstellungen anpassen. Die Bestimmung will mit anderen Worten sicherstellen, dass er sich der Nutzung seiner Daten durch einen Online-Dienst bewusster wird. Allerdings gilt Privacy by Default nicht nur für Anbieter wie Facebook, sondern überall, wo ein System dem Benutzer es erlaubt, die Nutzung seiner Daten selbst zu konfigurieren.

Kein Fall von *Privacy by Default* ist die Situation, in welcher der Benutzer gefragt wird, wie er einen Dienst konfigurieren will und sich bei der Ersteinrichtung seines Kontos für oder gegen eine bestimmte Nutzung seiner Daten entscheiden muss (unter dem DSG darf dabei das Kästchen für die Datennutzung sogar schon angekreuzt sein, unter der DSGVO nicht). Wird er jedoch beim Aufsetzen seines Kontos zunächst nicht gefragt, ihm aber jederzeit die Möglichkeit zur Anpassung geboten, greift das Gebot von *Privacy by Default*.

Kurz und bündig:

☐ Soweit wir Datenschutzeinstellungen für unsere Services nicht direkt bei der betroffenen Person abfragen, sind sie standardmässig auf ein Minimum reduziert. → **hier alles OK**

☐ Wir sehen im Rahmen der Datenbearbeitung gar keine Datenschutzeinstellungen vor. → **hier alles OK**

Im Detail:

☐ Wir **sprechen uns mit der Person nicht darüber ab** bzw. lassen sie nicht wählen, **wie weit** wir bei der Bearbeitung ihrer Daten gehen. → **hier alles OK**

☐ Wir holen von der betroffenen Person zwar **gewisse Einwilligungen** ab und sehen auch vor, dass sie diese widerrufen kann, aber **darüber hinaus kann sie nicht wählen**, wie weit ihre Daten bearbeitet werden bzw. was damit geschieht. → **hier alles OK**

☐ Wir geben der betroffenen Person im Rahmen der Datenbearbeitung (z.B. ein Online-Service) **mehrere Optionen**, wie weit wir bei der Bearbeitung ihrer Daten gehen; diese Optionen kann sie selbst ein- und ausschalten (z.B. in Form von Datenschutzeinstellungen).

  ☐ Die betroffene Person muss **vorgängig angeben**, wie ihre Daten bearbeitet werden (z.B. auf einer Anmeldeseite oder vor der Installation eines Apps) und kann dabei wählen, welche Datenschutzeinstellungen sie möchte.

  Soweit das DSG anwendbar ist:

  ☐ Bei dieser Wahlmöglichkeit möchten wir die **für uns beste Option vorangekreuzt** haben. → **hier alles OK**

  Soweit die DSGVO anwendbar ist:

  ☐ Bei dieser Wahlmöglichkeit ist die für uns **beste Option vorangekreuzt.**

  ☐ Bei dieser Wahlmöglichkeit ist **keine Option angekreuzt** (d.h. die Person muss aktiv werden). → **hier alles OK**

  ☐ Bei dieser Wahlmöglichkeit ist die **datenschutzfreundlichste Option angekreuzt.** → **hier alles OK**

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

  ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.

  ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.

  ☐ *Soweit nur DSG anwendbar:*

  Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr.

  _____

  ☐ Anderer Grund:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

  ☐ Wir sollten folgende Datenschutzeinstellungen anpassen, damit sie standardmässig auf das Minimum eingestellt sind:

  ☐ Wir sollten die betroffene Person gleich zu Beginn "zwingen", zwischen den verschiedenen Einstellungen entscheiden zu müssen. So gehen wir dem Problem aus dem Weg.

  ☐ Wir müssen sicherstellen, dass bei der Wahl der gewünschten Einstellungen entweder keine oder aber die datenschutzfreundlichste Einstellung vorangekreuzt ist; sonst ist das unter der DSGVO keine zulässige Einwilligung.

  ☐ Andere Massnahme:

☐ Gewisse **Datenschutzeinstellungen** sind **standardmässig** gesetzt, ohne dass wir die betroffene Person dazu befragen, bevor wir mit der Bearbeitung ihrer Daten beginnen; die Person kann sie aber **nachträglich jederzeit ändern.**

- ☐ Die Standardeinstellungen sind so, dass möglichst nichts mit den Daten geschieht, d.h. wenn die betroffene Person die von ihr gewünschten Optionen (in der Software, im Online-Service, etc.) nicht anpasst, mache wir mit den Daten nur das **Minimum** (z.B. keine Freischaltung für die Öffentlichkeit, falls diese im Rahmen eines Online-Services optional ist). → **hier alles OK**
- ☐ Die Standardeinstellungen sind **nicht** in der "**datenschutzfreundlichsten**" **Einstellung** (sondern z.B. so, wie sie am häufigsten eingestellt werden oder wie möglichst viel herausgeholt wird aus dem Dienst).

☐ Die Datenbearbeitung **sieht** solche **Wahlmöglichkeiten** für die betroffene **Person gar nicht** vor bzw. hat **keine Datenschutzeinstellungen**, wo zwischen einer mehr oder weniger weitgehenden Datenbearbeitung gewählt werden kann. → **hier alles OK**

☐ Wir möchten noch Folgendes vermerken:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

- ☐ Weitere Abklärungen sind nötig
- ☐ Experte konsultieren

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

- ☐ Sollten wir weitermachen wie bisher.
- ☐ Treffen wir folgende Sofortmassnahmen.
- ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

Q20

Korrekte Auftragsbearbeitung

Soweit Dritte beigezogen werden, welche die Daten im Auftrag für die Unternehmen bearbeiten, erfüllen diese Beauftragung die Anforderungen an eine korrekte Auftragsbearbeitung.

Art. [8] DSG, Art. 28 f. DSGVO

Es ist im Datenschutz grundsätzlich auch ohne Zustimmung der betroffenen Personen erlaubt, Dritte zur Bearbeitung der eigenen Daten beizuziehen, sofern gewisse Voraussetzungen erfüllt sind. Wesentlich ist, dass diese sog. Auftragsbearbeiter die Daten nur nach Weisung des Auftraggebers (d.h. dem für die Datenbearbeitung Verantwortlichen) bearbeiten und dafür sorgen, dass die Daten bei ihnen sicher sind. Dies wird in der Praxis primär durch den Abschluss eines entsprechenden Vertrags sichergestellt (in Deutschland ist oft von einem "ADV" bzw. einem Vertrag zur Auftragsdatenverarbeitung die Rede). Dieser regelt die beiden genannten und diverse weitere Punkte, die insbesondere die DSGVO explizit vorschreibt. Da diese etwas umfangreicher sind, wurde dafür das → Formular F.1 geschaffen, auf das in der mittleren Spalte verwiesen wird.

Abgrenzungsschwierigkeiten bereitet in der Praxis oft die Frage, wann überhaupt eine Auftragsbearbeitung vorliegt. Oft wird pauschal angenommen, dass jeder, der im Rahmen der Erbringung seiner Dienstleistung für ein Unternehmen (auch) dessen Daten bearbeitet, ein Auftragsbearbeiter ist. Das ist nicht richtig. Eine Auftragsbearbeitung liegt nur vor, wenn dem Dienstleister eine eigene Datenbearbeitung delegiert wird, dies also Teil des Auftrags ist. Bindet ein Online-Shop einen Zahlungsdienstleister in sein Angebot ein, so bearbeitet dieser zwar auch Daten der Käufer (sie müssen ja ihre Kreditkartendaten erfassen und der Dienstleister erhält Informationen zum Betrag, den er einkassieren muss), aber diese Daten bearbeitet der Zahlungsdienstleister in

Kurz und bündig:

☐ Die Verträge mit den diversen Unternehmen (auch im Konzern), die zwecks Beschaffung, Analyse, Versand, Systembetrieb, Aufbewahrung oder sonstiger Bearbeitung unserer Daten für uns tätig sind, entsprechen den Vorgaben der DSGVO bzw. des revidierten DSG. → **hier alles OK**

☐ Wir setzen im Rahmen der Datenbearbeitung gar keine Auftragsbearbeiter ein. → **hier alles OK**

Im Detail:

☐ Wir haben die Bearbeitung unserer Personendaten (oder Vorgänge, bei welchen diese bearbeitet werden) weder an einen Outsourcing-Provider, noch an eine andere Konzerngesellschaft noch an sonstige Dritte ausgelagert, sondern **machen alles selbst** einschliesslich Beschaffung, Analyse, Versand, Systembetrieb und Aufbewahrung. → **hier alles OK**

☐ Wir haben im Zusammenhang mit der Datenbearbeitung solche **Auslagerungen**, und zwar an folgende Unternehmen für folgende Bereiche:

☐ Datenbeschaffung	☐ Datenanalyse
☐ Versand	☐ Systembetrieb
☐ Aufbewahrung	☐ andere

☐ Wir haben **für jede Auftragsbearbeitung** die **Einhaltung der gesetzlichen Anforderungen geprüft** → dokumentiert in den folgenden Formularen des Typs F.1:

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

- ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.
- ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.
- ☐ *Soweit nur DSG anwendbar:*

  Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr.

  _____
- ☐ Anderer Grund:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

- ☐ Wir sollten die Verträge mit folgenden Auftragsbearbeitern auf ihre Konformität mit dem Gesetz überprüfen und ggf. anpassen:
  - ☐ Obwohl die Datenbearbeitung nicht unter die DSGVO fällt, sollten die Verträge den Anforderungen der DSGVO genügen.
  - ☐ Da es sich um Anbieter von Standard-Services handelt, sollten wir sie um einen Vorschlag für eine DSGVO-konforme Lösung bitten.
- ☐ Wir sollten bei den zuständigen Stellen intern rückfragen bzw. sicherstellen, dass diese die Verträge mit unseren Auftragsbearbeitern auch tatsächlich überprüfen.

eigener Verantwortung, d.h. er bestimmt, welche Daten er wie bearbeitet, damit er seine Dienstleistung erbringen kann. Die Datenbearbeitung ist Folge und nicht Inhalt seines Auftrags. Es kommen folglich nicht die Regeln der Auftragsbearbeitung zur Anwendung.

Liegt keine Auftragsbearbeitung vor, muss geprüft werden, ob der Zweck der Bearbeitung die Weitergabe der Daten an den beigezogenen Dienstleister abdeckt (vgl. Q6 und Q10). Ist dies der Fall, ist datenschutzrechtlich grundsätzlich keine spezielle Vereinbarung erforderlich (vorbehältlich des Falls, dass sich der Dienstleister in einem unsicheren Drittstaat befindet, vgl. Q16).

☐ Wir **meinen**, dass alle diese Auftragsbearbeitungen die gesetzlichen Anforderungen **grundsätzlich erfüllen:** → **hier alles OK**

☐ Folgende Auftragsbearbeitungen **erfüllen** die gesetzlichen Anforderungen womöglich **nicht** oder aber **wir können es nicht beurteilen:**

☐ Wir haben die Einhaltung der gesetzlichen Anforderungen im Rahmen unserer Auftragsbearbeitungen **nicht geprüft**.

☐ Das tun folgende **andere Stellen** im Unternehmen; wir gehen daher davon aus, die Auftragsbearbeitung wird gesetzeskonform sein: → **hier alles OK**

☐ Wir arbeiten **mit Dritten** zusammen, bei denen wir nicht sicher sind, ob sie **tatsächlich als Auftragsbearbeiter** betrachtet werden müssen oder können. Das wäre näher zu prüfen:

☐ Zahlungsdienstleister, Banken betr. ihre Bankdienstleistungen, Versicherungen betr. ihrer Versicherungen (keine Auftragsbearbeiter) → **hier alles OK**

☐ Post- und Fernmeldedienstanbieter, Logistikdienstleister (keine Auftragsbearbeiter) → **hier alles OK**

☐ Wir sollten mit den folgenden Auftragsbearbeitern die festgestellten Defizite bereinigen:

☐ Wir sollten überprüfen, ob folgende Dritte tatsächlich als Auftragsbearbeiter gelten, und die entsprechenden Massnahmen vorkehren:

☐ Andere Massnahme:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

			☐ Wir möchten noch Folgendes vermerken: ☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen ☐ Sollten wir weitermachen wie bisher. ☐ Treffen wir folgende Sofortmassnahmen. ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:
	Q21	**Lösch- und Sperrbegehren der betroffenen Person** Wenn eine betroffene Person nicht oder nicht mehr will, dass ihre Daten in einer bestimmten Art und Weise bearbeitet oder deren Sperrung oder Löschung verlangt, dann befolgt das Unternehmen diesen Wunsch, soweit keine der gesetzlichen Ausnahmefälle bzw. Rechtfertigungsgründe vorgesehen ist. Das Unternehmen hat die nötigen Vorkehrungen getroffen, um dies sicherzustellen. *Art. [26] Abs. 2 Bst. b DSG, Art. 17, 18, 21. DSGVO* Sowohl das DSG wie auch die DSGVO sehen vor, dass eine betroffene Person ihre Daten nicht nur berichtigen kann, sondern auch verlangen kann, dass ihre Daten nicht oder nicht mehr in einer bestimmten Weise bearbeitet werden. Im DSG ist das sehr generisch festgehalten, während die DSGVO zwischen einem Löschrecht, einem Anspruch auf Einschränkung und einem Recht auf Widerspruch unterscheidet. In der DSGVO ist das	*Kurz und bündig:* ☐ Wenn eine betroffene Person die Löschung oder Sperrung der sie betreffenden Daten in der Datenbearbeitung verlangt, so leisten wir dem soweit möglich Folge (z.B. keine Nutzung mehr von Daten zu Marketingzwecken). Es ist geregelt, wer dafür zuständig ist und die Systeme lassen solche Löschungen und Sperrungen auch zu. Soweit die DSGVO gilt, informieren wir auch Dritte, die die Daten von uns erhalten haben, über die Lösch- und Sperrwünsche und auf Wunsch die betroffene Person, wer diese Dritten sind.→ **hier alles OK** ☐ Wir sind bei dieser Datenbearbeitung auf etwaige Lösch- und Sperrgesuche nicht wirklich vorbereitet. *Im Detail:* ☐ Wenn eine betroffene Person die Löschung oder Sperrung von Daten **verlangt**: ☐ Haben wir einen **definierten Prozess** mit Verantwortlichkeiten, wie mit solchen Anfragen umzugehen ist. → 1. **OK** ☐ Haben wir **jemanden**, der sich darum kümmern wird und diese Person weiss, was sie zu tun hat oder wird sich kundig machen. → 1. **OK** ☐ Ist uns **nicht wirklich klar**, wie mit solchen Anfragen in organisatorischer Hinsicht umgehen würden.	☐ Es sind unseres Erachtens **keine Massnahmen nötig.** ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt. ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist. ☐ *Soweit nur DSG anwendbar:* Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr. _____ ☐ *Soweit nur DSGVO anwendbar:* Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.5 zu DB-Nr. _____ ☐ Anderer Grund:

von Relevanz, weil die Ausnahmen je nach Art des Anspruchs unterschiedlich ausgestaltet sind.

Für die vorliegenden Zwecke ist wichtig, ob die Datenbearbeitung bzw. die dafür benutzten Systeme so ausgestaltet sind, dass sich die Bearbeitung der Daten einer Person bei Bedarf entweder ganz gelöscht werden können oder aber die weitere Benutzung verhindert werden kann. Das Schulbeispiel ist die Streichung von der Versandliste für den firmeneigenen Newsletter, aber der Anspruch auf Widerspruch, Löschung und Einschränkung gilt natürlich universell, auch wenn es natürlich ebenso zahlreiche Gründe geben kann, warum ein Unternehmen einen solchen Wunsch nicht nachkommen wird.

In der Praxis werden solche Wünsche nicht häufig vorkommen. Es ist daher meistens ratsam, sich auf jene Fälle zu beschränken, die am wahrscheinlichsten sind und für diese zu prüfen, ob eine Löschung oder Sperrung der Daten tatsächlich möglich ist. Ist eine Löschung und Sperrung nicht möglich, sind aber Anfragen wahrscheinlich, sollte eine Anpassung der Systeme ins Auge gefasst werden.

Wichtig ist weiter, dass das Unternehmen die internen Verantwortlichkeiten festgelegt hat, damit klar ist, was mit einem entsprechenden Gesuch zu tun ist.

☐ Wir sind bei der Bearbeitung der Daten einer betroffenen Person im Rahmen dieser Datenbearbeitung **völlig flexibel**. Wenn eine Person nicht will, was oder wie wir mit ihren Daten tun, dann können wir sie aus dem System löschen (von Backups abgesehen). → 2. **OK**

☐ Wir müssen **realistischerweise damit rechnen**, dass folgende **Kategorien** von **betroffene Personen:**

[ ]

von uns im Rahmen der Datenbearbeitung **verlangen**, dass:

- ☐ Wir ihre Daten in unseren Systemen **ganz** oder **teilweise löschen**.
- ☐ Wir soweit möglich auch jene **über den Löschwunsch informieren**, die die Daten über eine **Publikation** von uns bezogen haben.
- ☐ Wir ihre Daten **nicht mehr weiter benutzen** (z.B. weil sie nach ihrer Meinung nicht korrekt sind, sie ihre Einwilligung widerrufen haben, sie bestreiten, dass unser berechtigtes Interesse überwiege, oder unsere Bearbeitung illegal ist).
- ☐ Wir ihre Daten nicht mehr weiter benutzen und sie **zusätzlich einfrieren**, d.h. selbst gar nicht mehr löschen dürfen (z.B. weil sie sie für einen Prozess sichern wollen).
- ☐ Wir ihre Daten **nicht mehr für Direktwerbung benutzen.**
- ☐ Wir ihre Daten **nicht mehr für wissenschaftliche, historische oder statistische Zwecke einsetzen.**
- ☐ Wir etwas anderes tun bzw. nicht mehr tun:

  [ ]

- ☐ Wir rechnen mit **keinen solchen Wünschen** von betroffenen Personen.

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

- ☐ Wir sollten einen Prozess zur Behandlung von Lösch- und Sperrbegehren definieren und einführen.
- ☐ Wir sollten festlegen, wer intern für die Behandlung von Lösch- und Sperrbegehren verantwortlich ist und sicherstellen, dass die zuständige Person weiss, was zu tun ist (oder dies bei Bedarf herausfinden kann).
- ☐ Wir sollten sicherstellen, dass wir die Daten einer bestimmten Person im Zusammenhang mit der vorliegenden Datenbearbeitung:
  - ☐ Von unseren Systemen löschen (oder sie anonymisieren)
  - ☐ "Einfrieren" (d.h. die Löschung verhindern)
  - ☐ Generell sperren (d.h. eine weitere Benutzung mindestens für eine gewisse Zeit blockieren)
  - ☐ Für Direktwerbung blockieren
  - ☐ Für wissenschaftliche, historische und statistische Zwecke blockieren

  können, wenn die betroffene Person dies von uns berechtigterweise verlangt.

			☐ Wir könnten **alle diese Wünsche**, mit denen wir realistischerweise rechnen müssen, mit unseren Systemen mit vertretbarem Aufwand **erfüllen**, wenn wir müssten. → 2. **OK** *Soweit nur DSGVO anwendbar (nur nächster Punkt):* ☐ Wir haben die Daten, die wir löschen bzw. sperren sollen, zuvor schon **Dritten für deren eigene Nutzung** weitergegeben bzw. zugänglich gemacht (wenn nein: → 3. + 4. **OK**). ☐ Wir **informieren diese Dritten** über das Lösch- und Sperrbegehren, soweit dies für uns möglich ist und keinen unverhältnismässigen Aufwand mit sich bringt. → 3. **OK** ☐ Wir **informieren** die betroffenen Personen, die das wissen wollen, darüber, **wer diese Dritten sind.** → 4. **OK** ☐ Wir möchten noch Folgendes vermerken: [ ]	
	Q22	**Grundsatz, dass Dritte keine besonders schützenswerte Personendaten erhalten (nur DSG)** Das Unternehmen gibt Dritten (im Konzern oder ausserhalb) ohne Rechtfertigungsgrund keine besonders schützenswerten Personendaten (→ Glossar) bekannt, soweit diese die Daten für ihre eigenen oder fremden Zwecke bearbeiten. *Art. [26] Abs. 2 Bst. c DSG* Für die Erhebung und weitere Bearbeitung von besonders schützenswerten Personendaten braucht es unter dem DSG weder eine Einwilligung noch sonst einen Rechtsfertigungsgrund, auch wenn dies teilweise anders vertreten wird. Das Gesetz ist in dieser Hinsicht klar: Einen Rechtfertigungsgrund braucht bloss die Weitergabe solcher Daten an ei-	*Kurz und bündig:* ☐ Wir geben (ohne Rechtfertigungsgrund) Dritten weder innerhalb noch ausserhalb des Konzerns besonders schützenswerte Personendaten bekannt. → **hier alles OK** *Im Detail:* ☐ **Wir geben Dritten** (auch Konzerngesellschaften) **keine** besonders schützenswerten Personendaten (→ Glossar) bekannt, **es sei denn**, sie **bearbeiten diese lediglich für uns**, aber nicht für eigene Zwecke (d.h. im Rahmen einer Auftragsbearbeitung). → **hier alles OK** ☐ Doch, **wir tun dies**, und zwar in folgenden Fällen: [ ]	☐ Es sind unseres Erachtens **keine Massnahmen nötig:** ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt. ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist. ☐ Die Anforderung ist zwar möglicherweise nicht erfüllt, aber wir meinen, dass wir einen Rechtfertigungsgrund haben → dokumentiert in Formular E.4 zu DB-Nr. _____ ☐ Anderer Grund: [ ] ☐ Es sind unseres Erachtens **folgende Massnahmen nötig:** ☐ Wir sollten prüfen, ob wir auf die Bekanntgabe dieser Daten verzichten können.

			nen Dritten (Verantwortlichen). Ist dies in der vorliegenden Datenbearbeitung der Fall, ist mit einem separaten Formular zu prüfen, ob hierfür ein genügender Rechtfertigungsgrund vorliegt. Hingegen erfordert das Profiling keine Rechtfertigung. Unter dem alten Recht war die Weitergabe von Persönlichkeitsprofilen noch gleich wie besonders schützenswerte Personendaten behandelt worden. Das Persönlichkeitsprofil als Spezialbegriff wurde aber abgeschafft.	☐ Wir möchten noch Folgendes vermerken: [ ]	☐ Wir sollten prüfen, ob wir dem Dritten vorschreiben können, dass er die Daten nur für unsere Zwecke verwendet (im Sinne einer Auftragsbearbeitung). ☐ Wir sollten prüfen, ob es möglich wäre, wenn wir die Daten vor der Bekanntgabe so codieren, dass die Empfänger und etwaige Dritte keine Rückschlüsse mehr auf die Identität der betroffenen Personen ziehen könnten. ☐ Wir sollten prüfen, ob sich für die Bekanntgabe nicht ein Rechtfertigungsgrund wie z.B. eine Einwilligung finden lässt. ☐ Wir sollten mit den folgenden Auftragsbearbeitern die festgestellten Defizite bereinigen: [ ] ☐ Andere Massnahme: [ ] ☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern: [ ] ☐ **Situation unklar** Grund: [ ] ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren

					☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen ☐ Sollten wir weitermachen wie bisher. ☐ Treffen wir folgende Sofortmassnahmen. ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:
		Q23	**Auskunftsrecht der betroffenen Person** Das Unternehmen ist in der Lage, alle Daten jeder betroffenen Person auf deren Wunsch zu lokalisieren, zu exportieren und ihr mitzuteilen, soweit dem keine gesetzlichen Ausnahmen entgegenstehen. Dies ist innert 30 Tagen möglich, wobei diese Frist vor Ablauf noch um bis zu zwei weitere Monate verlängert werden kann. Das Unternehmen hat die nötigen Vorkehrungen getroffen, um dies sicherzustellen. *Art. [23] ff. DSG, Art. 15 DSGVO* Das Auskunftsrecht ist das vermutlich in der Praxis wichtigste und am häufigsten ausgeübte Recht der betroffenen Personen. Es erlaubt ihnen, Einblick in die über sie bearbeiteten Personendaten zu nehmen, dies mit dem Sinn und Zweck, die betroffenen Personen selbst prüfen zu lassen, ob ihre Daten datenschutzkonform bearbeitet werden..	*Kurz und bündig:* ☐ Die Frage des Auskunftsrechts wird nicht für diese Datenbearbeitung nicht isoliert beurteilt, sondern zentral durch eine andere Stelle. → **hier alles OK** ☐ Wenn eine betroffene Person Auskunft über die sie betreffenden Daten in der Datenbearbeitung verlangt, so erteilen wir diese in der Regel, solange dies nicht Dritte oder unsere eigenen Geschäftsgeheimnisse tangiert. Es ist geregelt, wer dafür zuständig ist und die Systeme lassen die Extraktion der nötigen Daten auch zu. → **hier alles OK** ☐ Wir sind bei dieser Datenbearbeitung auf etwaige Auskunftsgesuche nicht wirklich vorbereitet. *Im Detail:* ☐ Wenn eine betroffene Person von uns Auskunft über ihre Daten **verlangt:** ☐ Haben wir einen **definierten Prozess** mit Verantwortlichkeiten, wie mit solchen Anfragen umzugehen ist → 1. **OK** ☐ Haben wir **jemanden**, der sich darum kümmern wird und diese Person weiss, was sie zu tun hat oder wird sich kundig machen.	☐ Die Frage der Einhaltung des Auskunftsrechts **wird gesondert auf höherer Stufe behandelt**. ☐ Es sind unseres Erachtens **keine Massnahmen nötig:** ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt. ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist. ☐ Anderer Grund: ☐ Es sind unseres Erachtens **folgende Massnahmen nötig:** ☐ Wir sollten einen Prozess zur Behandlung von Auskunftsbegehren definieren und einführen. ☐ Wir sollten festlegen, wer intern für die Behandlung von Auskunftsbegehren verantwortlich ist und sicherstellen, dass die zuständige Person weiss, was zu tun ist (oder dies bei Bedarf herausfinden kann).

Sowohl das DSG als auch die DSGVO definiert hierzu einen Katalog an Informationen, die dem Gesuchsteller im Rahmen des Auskunftsrechts mitgeteilt werden müssen, soweit er es verlangt (und nur dann). Will das Unternehmen mit entsprechenden Anfrage korrekt umgehen können, sollte es sich vergewissern, dass es all diese gesetzlich vorgesehenen Angaben bei Bedarf liefern kann und weiss, wie sie rasch und effizient zusammengetragen werden können (also z.B. wo sich im Rahmen einer Datenbearbeitung bzw. im Betrieb überall Daten einer bestimmten Person befinden und von diesen eine Kopie erhalten werden kann). Das ist in manchen Unternehmen teilweise aufwändiger als es den Anschein haben mag.

Das Unternehmen sollte sichergestellt haben, dass mindestens die Verantwortlichkeiten klar sind. Ist mit nur wenigen Auskunftsbegehren zu rechnen, ist es in der Regel ausreichend, wenn darauf ad hoc reagiert wird, da in der Regel genügend Zeit für eine Antwort besteht (ein Monat, verlängerbar).

Bei häufigeren Anfragen derselben Art kann es sinnvoll sein, eine Standardantwort vorzubereiten und einen entsprechenden Prozess zu definieren. Dieser Prozess sollte auch die Identifikation der betroffenen Person vorsehen, was beispielsweise über eine Ausweiskopie, aber auch auf andere geeignete Weise erfolgen kann (geht es z.B. über die in einem Online-Konto gespeicherten Angaben, genügt die Identifikation via Login in das betreffende Konto; in diesem Fall ist es oft am einfachsten, den Abruf der gespeicherten Informationen durch die Person selbst zu ermöglichen).

Wünscht jemand "alle Daten" zu sehen, die das Unternehmen über die Person überhaupt bearbeitet, kann es sinnvoll sein, der Person zunächst nur die typischerweise bearbeiteten Daten mitzuteilen und von ihr zu verlangen, nähere Angaben darüber zu machen, was sie spezifisch interessiert (d.h. sie zur Mitwirkung anzuhalten). Es sollte jedoch nach Möglichkeit keine Vollständigkeitserklärung abgegeben werden d.h. erklärt werden, dass ihr nun alle Angaben geliefert worden sind. Stellt sich das nämlich als falsch heraus, kann dies Sanktionen zur Folge

- ☐ Wir **meinen** in Anbetracht der bisherigen Erfahrungen mit solchen Anfragen, dass **das genügen wird.** → 1. **OK**
- ☐ Ist **uns nicht wirklich klar**, wie mit solchen Anfragen in organisatorischer Hinsicht umgehen würden.

☐ Wenn eine betroffene Person von uns Auskunft über ihre Daten **verlangt**:

- ☐ **Meinen wir zu wissen**, **wo** überall wir im Rahmen mit der Datenbearbeitung über diese Person Daten aufbewahren oder sonstwie bearbeiten und meinen in der Lage, diese mit vernünftigem Aufwand aus diesen Systemen zu **extrahieren.** → 2. **OK**
  - ☐ Wir haben für gewisse, **häufige Auskunftsersuchen** sogar eigene Abfragen eingerichtet bzw. dokumentiert, wie die Daten zusammenzutragen sind.
- ☐ Hätten wir vermutlich **Mühe** herauszufinden, wo überall im Rahmen der Datenbearbeitung Daten über die betroffene Person gespeichert oder sonst bearbeitet werden, oder diese **aus den Systemen zu ziehen.**
- ☐ Sollten wir **in der Lage** sein, die so **extrahierten Daten in einer Form aufzubereiten**, die wir der betroffenen Person mindestens auf **Papier** zur Verfügung stellen können. → 3. **OK**
- ☐ Stellen wir der betroffenen Person all ihre Daten online zur Verfügung, wo sie sie **über ihr Online-Konto selbst einsehen kann;** wer eine schriftliche Auskunft will, bekommt sie aber trotzdem. → 3. **OK**
- ☐ Meinen wir auch alle **gesetzlich vorgeschriebenen Zusatzinformationen** zur vorliegenden Datenbearbeitung **verfügbar** zu haben. → 4. **OK**
- ☐ **Liegen uns** die folgenden, gesetzlich vorgeschriebenen Zusatzinformation bisher **nicht** oder nicht vollständig **vor:**
  - ☐ **Identität** und **Kontaktangaben** des Verantwortlichen *(nur soweit DSG anwendbar).*
  - ☐ **Bearbeitungszwecke.**

- ☐ Wir sollten Richtlinien definieren, wie Auskunftsgesuche beantwortet werden können, einschliesslich der Fälle, in denen die Auskunft eingeschränkt bzw. verweigert werden kann oder sogar muss.
- ☐ Wir sollten Standardschreiben bzw. Templates für die Beantwortung von Auskunftsgesuchen definieren.
- ☐ Wir sollten festhalten, wo welche Informationen im Falle eines Auskunftsersuchens gefunden bzw. extrahiert werden können.
- ☐ Wir sollten einen Prozess zum Schwärzen von Dokumenten vorsehen, falls wir bei einem Ersuchen Daten Dritter bzw. Geschäftsgeheimnisse abdecken müssen.
- ☐ Wir sollten unsere Mitarbeiter besser darauf aufmerksam machen, keine Dinge aufzuschreiben, die nicht auch der betroffenen Person offengelegt werden könnten.
- ☐ Wir sollten den betroffenen Personen online eine Möglichkeit geben, ihre Daten selbst einzusehen, vor allem, wenn sie bei uns schon ein Online-Konto haben und dabei identifiziert sind.
- ☐ Wir sollten folgende Anpassungen an unseren Systemen oder Prozessen vornehmen, damit wir etwaige Auskunftsersuchen erfüllen bzw. besser erfüllen können:

  ☐ Programmieren eines Standardreports zur einfacheren Beantwortung von Auskunftsersuchen, weil wir mit regelmässigen Auskunftsgesuchen rechnen und dies unsere Arbeit daher erheblich erleichtern wird:

haben, da Unternehmen bzw. die Personen, die sich um die Auskunft kümmern, zur korrekten Antwort verpflichtet sind.

Das Auskunftsrecht verlangt allerdings auch nicht, dass in einem Unternehmen jeder Stein umgedreht wird, um jedes mögliche personenbezogene Datum der betroffenen Person zu finden. Exzessive oder schikanöse Anfragen können zurückgewiesen werden. Darüber hinaus sieht das Recht auch weitere Rückweisungsgründe, wie z.B. eigene Geschäftsgeheimnisse oder Interessen Dritter vor, indem Namen von anderen Personen in den herauszugebenden Daten geschwärzt werden.

- ☐ **Kategorien** der bearbeiteten Daten (soweit nicht offensichtlich).
- ☐ Kategorien von **Empfängern** der Daten.
- ☐ **Wie lange** das Unternehmen die Daten üblicherweise **aufbewahrt** bzw. Kriterien, wie es diese Frist bestimmt.
- ☐ Bestehen der diversen **Lösch-, Sperr- und Beschwerderechte.**
- ☐ **Herkunft** der Daten (soweit die Daten nicht bei der betroffenen Person selbst erhoben werden und Herkunftsangaben verfügbar sind).
- ☐ Bestehen etwaiger **automatisierter Einzelentscheide**, inklusive Angaben über die Entscheidlogik, die Tragweite der Entscheide und wozu die Entscheide dienen.
- ☐ **Länder**, in welche die Daten ggf. **übermittelt** werden *(nur soweit DSG anwendbar).*
- ☐ **Verträge** und **BCR** (→ Glossar), mit welchen das Unternehmen bei einem Export ins Ausland ein angemessenes Datenschutzniveau sicherstellt.
- ☐ **Ausnahmen**, auf die sich das Unternehmen bei der Übermittlung in Länder ohne angemessenen Datenschutz ggf. abstützt, wenn es keine Datenschutzverträge und dergleichen verwendet *(nur soweit DSG anwendbar).*
- ☐ Alle **weiteren Informationen**, die nötig sind, damit die betroffene Person ihre Rechte gemäss DSG geltend machen kann *(nur soweit DSG anwendbar).*
- ☐ Bemerkungen:

- ☐ Andere Massnahme:
- ☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

- ☐ Weitere Abklärungen sind nötig
- ☐ Experte konsultieren

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

- ☐ Sollten wir weitermachen wie bisher.
- ☐ Treffen wir folgende Sofortmassnahmen.
- ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

☐ Wir erwarten bei der Aufbereitung der Antwort auf das Auskunftsgesuch folgende weiteren **Probleme:**

☐ Wir meinen, **Auskunftsgesuche** im Zusammenhang mit dieser Datenbearbeitung:

- ☐ Innert **30 Tagen** → 5. **OK**
- ☐ Innert 30 Tagen (plus einer **Fristverlängerung** von maximal zwei Monaten, allerdings nur, wenn das aufgrund der Anfrage wirklich nötig ist und sich begründen lässt) → 5. **OK**
- ☐ **Nicht innert dieser Frist** beantworten zu können.

☐ Bevor die Antwort auf ein Auskunftsgesuch an die betroffene Person geht, **stellen** wir alle **folgende Dinge sicher.** → 6. **OK**

- ☐ Bei der auskunftsersuchenden Person **handelt es sich wirklich um die betroffene Person**, d.h. sie hat sich mittels Ausweiskopie ausgewiesen, wir kennen sie oder es ergibt sich aus anderen Umständen, dass es sich um die Person handelt, deren Daten wir herausgeben (z.B. Online-Login mit Bezug auf zum Online-Konto gespeicherten Daten).
- ☐ Es sind **keine Daten von Dritten enthalten**, die wir der betroffenen Person nicht offenlegen dürften (weil sie sie schon kennen, die Dritten zugestimmt oder kein überwiegendes Interesse haben); ggf. schwärzen wir die Angaben dieser Dritten (z.B. Mitarbeiternamen, andere Kunden).
- ☐ Es sind keine Geheimnisse oder andere Informationen enthalten, bei denen uns unser **Berufsgeheimnis** oder das **Schweizer Recht** sonst **verbietet**, sie mitzuteilen.

☐ **Gebühren** verlangen wir lediglich in den gesetzlich uns gestatteten Fällen; normalerweise ist das Auskunftsrecht bei uns kostenlos. → 7. **OK**

☐ Wir **weisen Auskunftsgesuche ab** oder **schränken** sie **ein**:

☐ Nur, wenn einer der nachfolgenden **gesetzlich vorgesehenen Fälle** erfüllt ist, nämlich, wenn: → 8. **OK**

☐ Ein Auskunftsersuchen jenseits von Gut und Böse ist, nur dazu dient, uns zu **schikanieren** oder sonst augenscheinlich nichts mit Datenschutzanliegen zu tun hat.

Soweit DSG anwendbar:

☐ Wir ein **überwiegendes eigenes Interesse** (→ Glossar) daran haben, keine oder keine vollständige Auskunft zu erteilen (unsere Daten aber nicht mit Dritten teilen und wir auch nicht als Bundesorgan die Daten bearbeiten).

☐ Eigene **Geschäftsgeheimnisse**

☐ **Aufwand** wäre zu gross

☐ Andere überwiegende eigene Interessen:

☐ Weil wir uns auf das **Medienprivileg** berufen können. (→ Glossar)

☐ Wir die Daten als **Bundesorgan** bearbeiten und die Auskunft eine **Ermittlung**, **Untersuchung** oder anderes Verfahren gefährden würde.

☐ Wir die Daten als Bundesorgan bearbeiten und die Wahrung der **inneren Sicherheit** oder sonst ein überwiegendes öffentliches Interesse dies gebietet.

Soweit DSGVO anwendbar:

☐ Wenn dies sonst eine Offenlegung unserer **Geschäftsgeheimnisse** zur Folge hätte, an denen die betroffene Person kein überwiegendes Interesse haben dürfte.

			☐ In den vorstehenden Fällen, aber auch in folgenden Fällen: ☐ Wo uns der **Aufwand** einfach **zu hoch** ist, weil wir nicht wirklich dafür eingerichtet sind. ☐ Wo die von uns bearbeiteten Daten (z.B. Kommentare in einem CRM) für uns **peinlich** wären. ☐ Wir möchten noch Folgendes vermerken:	
	Q24	**Informationspflicht** Alle Personen, über die wir Daten beschaffen, werden zum Zeitpunkt der Datenbeschaffung oder, wenn nicht bei ihnen direkt beschafft, spätestens nach einem Monat über folgende Punkte informiert: 1. Name und Adresse des Unternehmens 2. *Falls die Daten nicht bei der Person direkt beschafft werden:* Kategorien der Personendaten 3. Alle Bearbeitungszwecke	*Kurz und bündig:* ☐ Wir haben eine Datenschutzerklärung verfasst, die alle nach DSGVO bzw. revidiertem DSG vorgeschriebenen Angaben zur vorliegenden Datenbearbeitung enthalten und weisen die betroffenen Personen darauf hin (z.B. über Verträge, Websites, etc.). → **hier alles OK** ☐ Wir wissen, dass wir diese Anforderung nicht erfüllen und eine solche Datenschutzerklärung noch erstellen müssen. *Im Detail:* ☐ Wir wissen, dass wir diese Informationspflichten (noch) **nicht erfüllen** und unsere Datenschutzerklärung grundsätzlich überarbeiten müssen. ☐ Ja, die betroffenen Personen werden über die erforderlichen Punkte **informiert.** → 1. **OK**	☐ Es sind unseres Erachtens **keine Massnahmen nötig:** ☐ Wir meinen, dass wir die betroffenen Personen grundsätzlich wie erforderlich informieren. ☐ Wir meinen, dass die die betroffenen Personen jedenfalls in den in der Praxis wichtigsten Fällen wie erforderlich informieren. ☐ Wo wir nicht in der vorgesehenen Weise informieren, ist dies unserer Ansicht nach nicht erforderlich: ☐ Weil die betroffenen Personen schon über die Information verfügen, da:

4. Etwaige Dritte, welche Daten erhalten (inkl. Auftragsbearbeiter); es kann auch mit Kategorien gearbeitet werden
5. Länder, in welchen die Daten zugänglich sein können und diesbezügliche Rechtsgrundlagen
6. Alle weiteren Aspekte der Bearbeitung der Daten, mit denen die Personen nicht rechnen müssen

Gemäss DSGVO sind zusätzlich folgende Angaben erforderlich:

7. Name und Adresse des Repräsentanten nach Art. 27 DSGVO (wo vorhanden → Formular A.1/D.1)
8. Name und Adresse des Datenschutzbeauftragten gemäss Art. 37 DSGVO (wo vorhanden → Formular A.1/D.1)
9. Rechtsgrundlage(n) der Datenbearbeitung, inkl. Darlegung etwaiger berechtigter Interessen und Möglichkeit des Widerrufs einer Einwilligung, falls eine solche benutzt wird (→ Formular E.4)
10. Dauer, für welche die personenbezogenen Daten gespeichert werden oder die Kriterien für die Festlegung dieser Dauer
11. *Falls die Daten nicht bei der betroffenen Person direkt beschafft werden:*

☐ Nein, sie werden informiert, **aber noch nicht vollständig** über alle verlangten Informationen. Informationen fehlen zu den Punkten (Angabe der Ziffern genügt):

☐ Ja, sie werden von uns **direkt informiert**, indem wir:

- ☐ Die verlangten Informationen den betroffenen Personen per E-Mail, per Post oder auf andere Weise **zusenden.** → 2. **OK**
- ☐ Mit den betroffenen Personen **reden.** → 2. **OK**
- ☐ Unsere **Vertragsbedingungen** die Informationen enthalten oder auf eine Datenschutzerklärung mit den Informationen verweisen. → 2. **OK**
- ☐ Eine **Datenschutzerklärung** mit den Informationen auf unserer **Website** bereithalten:
  - ☐ Wir **gehen davon aus**, dass die betroffenen Personen **wissen**, dass wir Daten über sie beschaffen und rasch unsere Website finden, falls sie sich für die Informationen interessieren. → 2. **OK**

☐ Wir beschaffen Daten auch **indirekt**, d.h. nicht (nur) von den betroffenen Personen selbst (falls nicht: → 3. **OK**).

- ☐ Ja, die betroffenen Personen **erhalten die Information trotzdem innert Monatsfrist** (oder falls wir mit ihr verkehren oder die Daten Dritten mitteilen entsprechend früher). → 3. **OK**
- ☐ Ja, die **Quellen**, von welchen wir die Daten erhalten, **haben sich verpflichtet**, die betroffenen Personen zu informieren bzw. auf unsere Website mit der Datenschutzerklärung hinzuweisen (z.B. andere Familienmitglieder, eigene Mitarbeiter). → 3. **OK**

- ☐ Weil wir sonst das Geheimnis eines anderen preisgeben müssten, zu dessen Wahrung wir gesetzlich verpflichtet sind, da:
- ☐ Aus anderen Gründen:

Soweit Daten nicht direkt beschafft werden:

- ☐ Weil die Information unmöglich wäre oder einen unverhältnismässigen Aufwand verursachen würde, da:

Soweit DSG anwendbar:

- ☐ Weil die von uns betriebene Datenbearbeitung gesetzlich so vorgesehen ist.
- ☐ Weil der Information überwiegende Interessen Dritter (→ Glossar) entgegenstehen.
- ☐ Weil die Information den Zweck der Datenbearbeitung vereiteln würde.
- ☐ Weil wir ein überwiegendes eigenes Interesse (→ Glossar) daran haben, nicht wie vorgeschrieben zu informieren (unsere Daten aber nicht mit Dritten teilen):
  - ☐ Eigene Geschäftsgeheimnisse
  - ☐ Aufwand wäre zu gross

Quelle(n), aus welchen die Daten beschafft werden, und – *im Rahmen der DSGVO* – ob es sich um öffentlich zugängliche Quellen handelt

12. Bestehen des Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung und Widerspruch
13. Bestehen des Rechts, sich bei einer zuständigen Datenschutzbehörde über die Datenbearbeitung des Unternehmens zu beschweren
14. *Falls die Daten bei der betroffenen Person direkt beschafft werden:*

    Ob sie gesetzlich oder vertraglich verpflichtet oder es für die Abwicklung des Vertrags nötig ist, dem Unternehmen die verlangten Daten zu geben und was die Folgen sind, wenn sie es nicht tut
15. *Falls im Unternehmen der Computer aufgrund von Daten einer Person vollständig alleine Entscheide betreffend eine der angesprochenen Personen trifft, die sonst im Ermessen eines Menschen liegen würden und diese Entscheide rechtliche oder nachteilige Konsequenzen haben:*

    Angaben zu diesem automatisierten Einzelentscheid, dessen Logik, seine Tragweite und Auswirkungen

☐ Ja, wir erreichen zwar nicht alle Personen, **gehen aber davon aus**, dass sie bei Interesse den Weg auf unsere **Website finden werden**. Dort informieren wir. → 3. **OK**

Soweit DSGVO anwendbar (nur nächste Frage):

☐ Es kann sein, dass wir die Daten nach der Beschaffung für **weitere** als die ursprünglich angegebenen **Zwecke** nutzen wollen. In diesem Fall werden wir die betroffenen Personen **nachinformieren:**

☐ Durch **Anpassung** unserer **Datenschutzerklärung** und, wo möglich, die betroffenen Personen darauf hinweisen → 4. **OK**

☐ Durch eine **Mitteilung** an die betroffenen Personen. → 4. **OK**

☐ Und zwar auf eine andere Weise: → 4. **OK**

☐ Wir **erreichen** mit unseren Informationen folgende relevante Gruppe von betroffenen Personen **nicht:**

☐ Wir **informieren** die betroffenen Personen **nicht.**

☐ Es ist bei uns so:

☐ Wir möchten noch Folgendes vermerken:

☐ Andere überwiegende eigene Interessen:

☐ weil wir uns aufs Medienprivileg berufen können (→ Glossar)

Soweit DSGVO anwendbar:

☐ Weil es sich um eigene Geschäftsgeheimnisse handelt, an denen die betroffene Person kein überwiegendes Interesse haben dürfte.

☐ Anderer Grund:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

☐ Es fehlen uns zu folgenden Punkten die nötigen Angaben für die Information. Sie sollten intern entsprechend beschafft bzw. festgelegt werden:

Art. [17] f. DSG, Art. 13 f. DSGVO

Während der Grundsatz der Transparenz verlangt, dass für die betroffene Person im Groben erkennbar ist, dass und wozu ihre Daten erhoben werden, dient die Informationspflicht dazu, sie mit bestimmten, vom Gesetzgeber vordefinierten Informationen zu versorgen. Diese sind oben aufgeführt. Es können und sollen selbstverständlich mehr Informationen geliefert werden, wenn dies der Transparenz dient. In der Praxis beschränken sich Unternehmen jedoch typischerweise auf die genannten Pflichtinformationen.

Es gibt keine Formvorschriften, wie diese Informationen der betroffenen Person mitgeteilt werden müssen, aber in aller Regel wird dies mittels einer Datenschutzerklärung getan. Diese wird auf der Website des Unternehmens aufgeschaltet (ggf. auch gedruckt abgegeben) und es wird darauf auch in Verträgen, Kundeninformationen, Rechnungen oder an anderen Orten verwiesen. Wesentlich ist, dass die betroffenen Personen die Informationen vorgelegt bekommen, wenn von ihnen Daten erhoben werden (oder spätestens in einem Monat), wenn die Daten aus Drittquellen beschafft werden. Sie müssen den Erhalt der Informationen weder bestätigen, noch Einwilligen, aber sie muss ihnen einfach zugänglich sein (in Apps gilt z.B. die Faustregel, dass die Datenschutzerklärung nicht mehr als zwei Klicks entfernt sein darf).

Datenschutzerklärungen sind typischerweise sehr schematisch aufgebaut. Nicht zwingend, aber empfehlenswert ist es, in einem ersten Teil in Prosa darzulegen, was mit den Daten der betroffenen Personen normalerweise geschieht. Es kann dabei auf die wichtigsten Elemente fokussiert werden. In einem zweiten Teil können dann die "Pflichtinformationen" aufgeführt werden, was in der Praxis durchaus schematisch geschieht (hier das Beispiel einer Schweizer Grossbank: https://goo.gl/uZWEXt).

☐ Für folgende Bearbeitungstätigkeiten den Anforderungen sollten wir entsprechende Informationsschreiben/Erklärungen erstellen und Bereitstellung organisieren:

☐ Folgende Informationsschreiben/Erklärungen sind zwar eine gute Basis, sollten aber an die neuen Anforderungen angepasst werden:

☐ An folgenden Stellen sollten wir Verweise auf Informationsschreiben/Erklärungen vorsehen, damit betroffene Personen wissen, wo sie sich informieren können.

☐ Allgemeine Vertragsbedingungen:

☐ Die Stellen, von denen wir Daten erhalten, sollten wir verpflichten, die betroffenen Personen auch für uns zu informieren.

☐ Wir sollten einen Prozess zur Nachinformation der betroffenen Personen schaffen, für den Fall, dass wir die Daten für weitere Zwecke bearbeiten wollen, die nicht angegeben waren.

☐ Andere Massnahme:

	Da die Anforderungen an Datenschutzerklärungen sowohl unter dem revidierten DSG als auch der DSGVO zugenommen haben, werden die unter dem alten Recht erstellten Datenschutzerklärungen den Anforderungen nie genügen, d.h. sie werden für jede Datenbearbeitung überarbeitet werden müssen. In der Praxis wird nicht für jede Datenbearbeitung eine separate Datenschutzerklärung erstellt, sondern es werden kombinierte Erklärungen gemacht. Häufig wird eine Datenschutzerklärung für die eigenen Mitarbeiter gemacht (worin dargelegt wird, wie ihre Daten bearbeitet werden), eine für die Kunden (d.h. Privatkunden, Konsumenten und den Personen in deren Umkreis wie z.B. Familienangehörige, Begünstigte), eine für die Benutzer der Website und Apps des Unternehmens (die Kunden sein können aber auch andere Personen; sie wird mitunter kombiniert mit der Erklärung für Kunden) und ggf. eine, die alle anderen abdeckt (z.B. Lieferanten, Geschäftskunden, etc. und deren Mitarbeiter). Die Datenschutzerklärung muss in jenen Sprachen abgefasst sein, welche die betroffenen Personen verstehen und in welcher mit ihnen kommuniziert wird.		☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern: ☐ **Situation unklar** Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren ☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen ☐ Sollten wir weitermachen wie bisher. ☐ Treffen wir folgende Sofortmassnahmen. ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

Q25

Autom. Einzelfallentscheide (nur DSG)

Falls relevante automatisierte Einzellfallentscheide vorkommen:

Die betroffene Person kann, wenn der Entscheid nicht wie von ihr gewünscht ausgefallen ist, mit einem entscheidbefugten Menschen darüber sprechen, ausser, sie hat ausdrücklich verzichtet. Sie wird in diesem Fall darüber vor oder mit dem Entscheid informiert.

Ein nach DSG relevanter automatisierter Einzelfallentscheid liegt vor, wenn (i) im Rahmen der Datenbearbeitung der Computer anhand von Daten einer Person vollständig alleine Entscheide betreffend diese einzelne Person trifft, (ii) es eine Art von Entscheiden ist, bei denen das Ergebnis je nach Unternehmen unterschiedlich sein dürfte, und (iii) diese Entscheide für die betroffene Person rechtliche oder nachteilige Konsequenzen haben können

Art. [19] DSG

Die Bestimmung über automatisierte Einzelentscheide regelt eine Informationspflicht, hat jedoch eine eigenständige Bedeutung. Hintergrund ist ein Misstrauen gegenüber Entscheidungen, die ein Computer alleine trifft, dabei möglicherweise nicht alle relevanten Faktoren berücksichtigt und so zu ungerechten Ergebnissen kommt. Die Regel geht von der Vorstellung aus, durch Menschen getroffene Entscheide seien gerechter, weil auch Sonderfälle berücksichtigt werden könnten und es eine Möglichkeit geben muss, um auf falsche oder unvollständige Daten hinzuweisen.

Kurz und bündig:

☐ Wir haben im Rahmen unserer Datenbearbeitung Fälle, in welchen es zu automatisierten Einzelentscheiden *(siehe Definition in der linken Spalte)* kommt, bieten den betroffenen Personen aber an, dass sie sich dazu äussern können, ein Mensch den Entscheid daraufhin prüft und nötigenfalls anpasst. → **hier alles OK**

☐ Wir nutzen automatisierte Einzelentscheide, die Folgen für betroffene Personen haben können und ihnen ggf. nicht gefallen, informieren aber nicht oder sehen nicht die Möglichkeit einer Wiedererwägung durch einen Menschen vor, sollte jemand dies verlangen.

☐ Wir haben im Rahmen der Datenbearbeitung keine hier relevanten automatisierten Einzelentscheide. → **hier alles OK**

Im Detail:

☐ Im Rahmen unserer Datenbearbeitung treffen in folgenden Fällen von A bis Z **alleine unsere Computer** gestützt auf Daten von betroffenen Personen **Entscheide** (d.h. Computer bereiten diese nicht bloss vor), die sich jeweils auf einzelne Personen beziehen. Die Art und Weise, wie die Computer entscheiden sind, sind unternehmensspezifisch, d.h. bei jedem Unternehmen dürften andere Entscheide herauskommen:

☐ Kreditgewährung ☐ Rechnungsprüfung

☐ Betrugsprüfung ☐ Individualisierte Preise

☐ Individualisiertes Marketing

☐ Wir lassen Entscheide betreffend einzelner Personen im Rahmen der Datenbearbeitung **nicht alleine vom Computer treffen**. → **hier alles OK**

☐ Es gibt zwar voll automatisierte Entscheide betreffend einzelner Personen bei uns, aber sie haben **weder rechtliche noch nachteilige Folgen** für diese Personen. → **hier alles OK**

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.

☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.

☐ Anderer Grund:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

☐ Wir sollten prüfen lassen, ob die von uns identifizierten automatisierten Einzelentscheide wirklich solche im Sinne des Gesetzes sind.

☐ Wir sollten prüfen, ob wirklich gültige Einwilligungen in die automatisierten Einzelentscheide vorliegen.

☐ Wir sollten vorsehen, dass wir die betroffenen Personen über die automatisierten Einzelentscheide informieren.

☐ Wir sollten vorsehen, dass die betroffenen Personen sich an einen Menschen wenden können, der ihren Fall nochmals überprüft.

☐ Wir sollten die Mitarbeiter schulen, mit Anfragen betr. solche automatisierten Einzelentscheide umzugehen.

☐ Wir sollten die nicht beurteilten Fälle genauer ansehen im Hinblick auf die Anforderungen.

☐ Wir sollten den Einsatz der folgenden automatisierten Einzelentscheide überdenken, oder von der vollständigen Automatisierung wieder etwas wegkommen, damit wir nicht unter die neuen Regelungen fallen.

Es ist weder ein Verbot vorgesehen, noch ein Anspruch der betroffenen Person, nicht einer automatisierten Einzelentscheidung zu unterliegen. Es wird stattdessen verlangt, dass eine betroffene Person grundsätzlich über eine solche automatisierte Einzelentscheidung informiert und ihr die Möglichkeit gegeben werden muss, sich mit einem Menschen über den Entscheid zu unterhalten. Dieser muss den vom Computer getroffenen Entscheid zwar umstossen können. Tun muss er es jedoch nicht. Es ist dies mit anderen Worten ein Anspruch auf "menschliches Gehör".

Hat die betroffene Person darin ausdrücklich eingewilligt, dass der Entscheid in einer bestimmten Angelegenheit vom Computer definitiv beschlossen wird, dann kann auf das menschliche Gehör verzichtet werden. Ebenso, wenn ein automatisierter Einzelentscheid im Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und die betroffene Person bekommen hat, was sie wollte.

In der Praxis wird nicht immer einfach zu entscheiden sein, wann ein automatisierter Einzelentscheid vorliegt. Dazu müssen folgende Kriterien erfüllt sein:

- Erforderlich ist zunächst ein Einzelentscheid über eine betroffene Person. Wenn also beispielsweise eine Fluggesellschaft von einem Computer bestimmen lässt, wie hoch die Preise für bestimmte Sitzplätze an eine bestimmte Destination zu einem bestimmten Zeitpunkt am besten sind, so ist das kein Einzelentscheid. Es wird keine Entscheidung über eine einzelne Person gefällt. Wird hingegen der Computer so programmiert, dass er auf einen bestimmten Kunden individualisierte Preise berechnet, so liegt ein Einzelentscheid vor.
- Der Einzelentscheid muss aufgrund der Bearbeitung von Personendaten der betroffenen Person erfolgen. Wer also den Computer Einzelentscheide über anonyme Besucher einer Website treffen lässt, ist nicht erfasst.

☐ Die Entscheide können für die betroffenen Personen **rechtliche Folgen** haben (ob ein Vertrag zustande kommt, zu welchen Konditionen, ob eine Leistung erfolgt, ob Kredit gewährt wird, etc.) oder **erhebliche Beeinträchtigungen** mit sich bringen.

- ☐ Diese Entscheide stehen in unmittelbarem Zusammenhang mit dem **Abschluss oder der Abwicklung eines Vertrags** mit der betroffenen Person und der Vertrag kommt so zustande bzw. wird so abgewickelt, wie von der Person **gewünscht.** → **hier alles OK**
- ☐ Die betroffene Person hat ausdrücklich **eingewilligt**, dass ein Computer bezüglich ihrer Belange entscheidet; im Rahmen der Einwilligung wurde die Person informiert, worüber der Computer entscheidet und wann, und die Einwilligung erfüllt alle Anforderungen gemäss Q1 von → Formular E.4. → **hier alles OK**
- ☐ Es ist in unserem Fall zwar **keiner** der beiden vorstehenden Fälle gegeben, aber:
  - ☐ Wir **informieren** die betroffene Person über diesen automatisierten Entscheid und sie kann:
    - ☐ Von uns als **privates Unternehmen** verlangen, dass ein Mitarbeiter den **Entscheid überprüft** und sie ihm dazu ihren Standpunkt darlegen kann, oder → **hier alles OK**
    - ☐ Soweit wir als **Bundesorgan** agieren, ein **Rechtsmittel** gegen den Entscheid einlegen. → **hier alles OK**
  - ☐ Wir **informieren** die betroffene Person **nicht**, dass ein automatisierter Entscheid erfolgt.
  - ☐ Wir sehen **nicht** vor, dass ein Mensch den **Entscheid überprüfen** kann, wenn die betroffene Person dies verlangt.

☐ Andere Massnahme:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

☐ Sollten wir weitermachen wie bisher.

☐ Treffen wir folgende Sofortmassnahmen.

☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

			• Der Einzelentscheid muss vollständig von einer Maschine getroffen werden. Bereitet der Computer Entscheide nur vor, und prüft bzw. segnet ein Mensch sie inhaltlich ab, bevor sie der betroffenen Person kommuniziert werden, liegt kein automatisierter Einzelentscheid vor. Ob die Entscheidregeln von Menschenhand stammen, spielt keine Rolle, wesentlich ist, dass die Subsumption des konkreten Sachverhalts im Einzelfall maschinell erfolgt und diese bis zur Fällung des definitiven Entscheids nicht mehr von einem Menschen überprüft wird. • Die maschinelle Subsumption bzw. Entscheidung muss eine gewisse Komplexität aufweisen, d.h. es muss um eine inhaltliche Beurteilung bzw. Bewertung und nicht eine reine "wenn-dann-Entscheidung" gehen. Ist letzteres der Fall, so liegt gar kein Entscheid im engeren Sinn vor, weil in der Sache kein Spielraum besteht, zu welchem Ergebnis der Vorgang richtigerweise kommen kann. In diesem Sinne fällt ein elektronisches Türschloss keinen Entscheid über den Zutritt zum Gebäude: Ist der Code richtig, hat es zu öffnen. Anders ist hingegen der Kreditentscheid. Er kann von seiner Natur aus so oder so ausfallen. • Der Entscheid muss für die betroffene Person mit einer Rechtsfolge verbunden sein oder aber sie erheblich beeinträchtigen. Jede Rechtsfolge genügt, sei es ein Vertragsabschluss, die Ausübung eines vertraglichen Rechts und theoretisch auch eine Erfüllungshandlung unter dem Vertrag (also z.B. die Lieferung der Ware). Eine "erhebliche Beeinträchtigung" soll allerdings blosse Belästigungen nicht erfassen.	☐ Die vorstehenden Ausführungen gelten **nur** für die folgende(n), besonders wichtige(n) Datenbearbeitung(en): ☐ Für die anderen ist eine **separate Beurteilung** erforderlich ☐ Die anderen erscheinen **nicht problematisch** ☐ Wir möchten noch Folgendes vermerken:	

Q26

Autom. Einzelfallentscheide (nur DSGVO)

Falls relevante automatisierte Einzellfallentscheide vorkommen:

Die betroffene Person wird darüber informiert und sie kann verlangen, dass ihr Fall stattdessen von einem Menschen beurteilt wird. Hat sie in die automatisierte Entscheidfindung vorgängig ausdrücklich eingewilligt, ist sie gesetzlich vorgesehen oder dient sie dem Abschluss oder der Abwicklung eines Vertrags, ist es zulässig, den Entscheid automatisiert vorzunehmen, sofern die betroffene Person ihn nachträglich unter Darlegung ihres Standpunkts bei einem Menschen anfechten kann. Wenn es um besondere Kategorien von Personendaten (→ Glossar) geht, kann die Person auch dort, wo es um den Abschluss oder die Abwicklung eines Vertrags geht, verlangen, dass der Entscheid von vornherein von einem Menschen getroffen wird.

Ein nach DSGVO relevanter automatisierter Einzelfallentscheid liegt vor, wenn (i) im Rahmen der Datenbearbeitung anhand der Daten einer Person ausschliesslich von einem Computer oder basierend auf einem Profiling (→ Glossar) ein Entscheid nur betreffend diese einzelne Person getroffen wird und (ii) er für sie rechtliche oder nachteilige Konsequenzen haben können.

Kurz und bündig:

☐ Wir haben im Rahmen unserer Datenbearbeitung Fälle, in welchen es zu automatisierten Einzelentscheiden von Relevanz *(siehe Definition in linker Spalte)* kommt, doch haben die betroffenen Personen darin vorab ausdrücklich eingewilligt oder es dient dem Abschluss oder der Abwicklung eines Vertrags (in diesem Fall kommen keine besonderen Kategorien von Personendaten vor). Die betroffenen Personen erhalten ferner die Möglichkeit, den Entscheid vor einem Menschen unter Vorlage weiterer Argumente anzufechten. → **hier alles OK**

☐ Wir nutzen automatisierte Einzelentscheide, die Folgen für betroffene Personen haben können, informieren diese aber nicht oder sehen nicht vor, dass auf Verlangen ein Mensch sich den Fall im Hinblick auf den definitiven Entscheid anschaut.

☐ Wir haben im Rahmen der Datenbearbeitung keine hier relevanten automatisierten Einzelentscheide. → **hier alles OK**

Im Detail:

☐ Im Rahmen unserer Datenbearbeitung treffen wir in folgenden Fällen **gestützt auf ein automatisiertes Profiling** oder sonst **alleine durch unsere Computer** Entscheide zu einzelnen betroffenen Personen anhand deren Daten:

☐ Kreditgewährung ☐ Rechnungsprüfung

☐ Betrugsprüfung ☐ Individualisierte Preise

☐ Individualisiertes Marketing

☐ Wir haben **keine automatisierten Einzelentscheide** und auch keine Entscheide betreffend einzelner Personen, die sich auf ein **Profiling** abstützen. → **hier alles OK**

☐ Es gibt zwar von A bis Z automatisierte Entscheide bei uns, aber sie haben **weder rechtliche noch nachteilige Folgen** für die betroffenen Personen. → **hier alles OK**

☐ Es sind unseres Erachtens **keine Massnahmen nötig:**

☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt.

☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist.

☐ Anderer Grund:

☐ Es sind unseres Erachtens **folgende Massnahmen nötig:**

☐ Wir sollten prüfen lassen, ob die von uns identifizierten automatisierten Einzelentscheide bzw. Einzelentscheide basierend auf einem Profiling wirklich solche im Sinne des Gesetzes sind.

☐ Wir sollten prüfen, ob wirklich gültige Einwilligungen in die automatisierten Einzelentscheide vorliegen.

☐ Wir sollten vorsehen, dass wir die betroffenen Personen über die automatisierten Einzelentscheide informieren.

☐ Wir sollten vorsehen, dass die betroffenen Personen sich an einen Menschen wenden können, der ihren Fall nochmals überprüft.

☐ Wir sollten die Mitarbeiter schulen, mit Anfragen betr. solche automatisierten Einzelentscheide umzugehen.

☐ Wir sollten die nicht beurteilten Fälle genauer ansehen im Hinblick auf die Anforderungen.

☐ Wir sollten den Einsatz der folgenden automatisierten Einzelentscheide überdenken, oder von der vollständigen Automatisierung wieder etwas wegkommen, damit wir nicht unter die neuen Regelungen fallen.

Art. 22 DSGVO

Der Bestimmung liegt derselbe Gedanke zugrunde wie der gleichgelagerten Bestimmung des DSG (vgl. Q25). Sie ist vergleichbar, weicht vor allem in folgenden Punkten davon ab:

Die Definition, was ein automatisierter Einzelentscheid ist, ist in der EU vergleichbar wie unter dem DSG. Der Entscheid muss allerdings nicht zwingend von einem Computer getroffen worden sein. Ein Einzelentscheid, der auf der Basis eines Profilings im Sinne der DSGVO erfolgt, ist ebenfalls erfasst. In der Schweiz ist dabei der Begriff des Profilings etwas anders definiert als in der EU: In der Schweiz muss ein Profiling immer durchgängig automatisiert sein, damit es ein solches ist, in der EU ist dies nicht der Fall. Daher ist die Regel der DSGVO, dass ein automatisierter Einzelentscheid auch auf Basis eines Profilings entstehen kann, von Relevanz.

In der EU ist derzeit umstritten, ob die Bestimmung zu automatisierten Einzelentscheiden ein Verbot solcher Entscheide beinhaltet, oder lediglich das Recht einer betroffenen Person, eine solche in ihrem Fall zu verbieten. Nicht verboten ist ein solcher automatisierter Einzelentscheid in drei Fällen: Wenn er im Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags erfolgt, auf Basis einer ausdrücklichen Einwilligung der betroffenen Person oder wo er im Recht der EU (bzw. des EWR) gesetzlich vorgesehen ist.

Ist er nicht verboten, so muss trotz allem das menschliche Gehör gewährt werden. Anders als im DSG wird für Fälle, in denen ein Kunde vom Computer bekommt, was er verlangt hat, unter der DSGVO keine Ausnahme gemacht: Auch hier muss der betroffenen Person mindestens das Recht auf menschliches Gehör gewährt werden.

☐ Diese Entscheide können für die betroffenen Personen **rechtliche Folgen** haben (ob ein Vertrag zustande kommt, zu welchen Konditionen, ob eine Leistung erfolgt, ob Kredit gewährt wird, etc.) oder **erhebliche Beeinträchtigungen** mit sich bringen.

- ☐ Diese Entscheide sind **gesetzlich vorgesehen** oder vom jeweils anwendbaren EU- oder EWR-Recht für zulässig erklärt worden. → 1. + 2. **OK**
- ☐ Wir bieten betroffenen Personen an, dass wir ihren Fall **nicht einem automatisierten Einzelentscheid unterziehen**, wenn sie dies verlangen. Sie werden darüber **informiert**, dass es solche Entscheide gibt und wie sie vorgehen müssen, wenn sie von vornherein die Beurteilung durch einen Menschen möchten. → 1. + 2. **OK**
- ☐ Die betroffene Person hat **ausdrücklich** darin **eingewilligt**, dass ein Computer bzw. ein Profiling bezüglich ihrer Belange entscheidet; im Rahmen der Einwilligung wurde die Person informiert, worüber der Computer entscheidet und wann und die Einwilligung erfüllt alle Anforderungen gemäss Q1 von → Formular E.3. → 1. **OK**
- ☐ Diese Entscheide stehen in unmittelbarem Zusammenhang mit dem **Abschluss oder der Abwicklung eines Vertrags** mit der betroffenen Person.
  - ☐ Es geht nicht um besondere Kategorien von Personendaten. → 1. **OK**
  - ☐ Es geht um besondere Kategorien von Personendaten.
- ☐ Diese betroffene Person wird darüber **informiert**, dass es solche Entscheide gibt und es wird ihr die Möglichkeit geboten, den Entscheid **nachträglich bei einem Menschen anzufechten** und diesem hierzu den eigenen Standpunkt dazulegen. → 2. **OK**

☐ Andere Massnahme:

☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen

☐ Sollten wir weitermachen wie bisher.

☐ Treffen wir folgende Sofortmassnahmen:

☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

			☐ Die vorstehenden Ausführungen gelten **nur** für die folgende(n), besonders wichtige(n) Datenbearbeitung(en): ☐ Für die anderen ist eine **separate Beurteilung** erforderlich. ☐ Die anderen erscheinen **nicht problematisch.** ☐ Wir möchten noch Folgendes vermerken:	
	Q27	**Anspruch auf Datenübertragbarkeit (nur DSGVO)** *Falls das Unternehmen auf Basis einer Einwilligung oder vertraglichen Grundlage für sich Daten über die betroffene Person von ihr direkt erhält und bei sich IT-mässig verarbeitet:* Die betroffene Person kann die Herausgabe der Daten in einem strukturierten, gängigen und maschinenlesbaren Format erhalten oder die direkte Übermittlung an ein anderes Unternehmen (insbesondere einem Mitbewerber des Unternehmens) verlangen. *Art. 20 DSGVO* Der Anspruch auf Datenübertragbarkeit, zuweilen auch als Recht auf Datenkopie oder Datenportabilität bezeichnet, will erreichen, dass betroffene Personen die Daten, die Unternehmen über sie anlegen, in elektronischer Form herausverlangen können, damit sie einfacher zu einem Mitbewerber verschoben werden können. Dies hat im engeren	*Kurz und bündig:* ☐ Wenn wir von einer Person für uns Daten erhalten, die wir mit unseren Computern im Rahmen eines Vertrags mit der Person oder auf Basis einer Einwilligung von ihr bearbeiten, können wir ihr diese Daten jederzeit auf deren Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zurückgeben bzw. geben diese direkt dem Konkurrenten weiter, den die Person uns angibt, sofern dies möglich ist. Wir informieren die betroffenen Personen auch über dieses Recht. → **hier alles OK** ☐ Wir sind nicht in der Lage, einer betroffenen Person die von ihr stammenden Daten, die wir für uns selbst erheben, ihr in einem strukturierten, gängigen und maschinenlesbaren Format zurückzugeben. ☐ Wir erhalten von den betroffenen Personen direkt keine Daten. → **hier alles OK** ☐ Wenn eine betroffene Person von uns die Herausgabe ihrer Daten in einem **elektronischen Format verlangt:** ☐ Haben wir einen **definierten Prozess** mit Verantwortlichkeiten, wie mit solchen Anfragen umzugehen ist. → 1. **OK**	☐ Es sind unseres Erachtens **keine Massnahmen nötig:** ☐ Wir meinen, die Anforderung ist grundsätzlich erfüllt. ☐ Wir meinen, dass die Anforderung jedenfalls in den in der Praxis wichtigsten Fällen erfüllt ist. ☐ Anderer Grund: ☐ Es sind unseres Erachtens **folgende Massnahmen nötig:** ☐ Wir sollten prüfen lassen, wir tatsächlich dem Anspruch auf Datenportabilität unterliegen. ☐ Wir sollten die betroffenen Personen über ihren Anspruch auf Datenportabilität informieren. ☐ Wir sollten einen Prozess zur Behandlung von Ansprüchen auf Datenportabilität definieren und einführen.

Sinne nichts mit Datenschutz zu tun, ist aber aus politischen Gründen in der DSGVO aufgenommen worden.

Das Recht auf Datenkopie gilt nur für Fälle, in denen die betroffene Person sich auf die DSGVO berufen kann. Es gilt auch nur für Daten, die das Unternehmen als Verantwortlicher bearbeitet. Alle Daten, die ihm als Auftragsbearbeiter übertragen wurden, sind nicht erfasst.

Voraussetzung ist weiter, dass es sich um Daten handeln muss, die das Unternehmen aufgrund eines Vertrags oder einer Einwilligung der betroffenen Person bearbeitet, und es dies mit Hilfe von Computern tut. Ist das der Fall, so kann die betroffene Person entweder verlangen, dass diese Daten an den von ihr ausgewählten Konkurrenten des Unternehmens übermittelt wird, oder aber in einem standardisierten, maschinenlesbaren Format herausgegeben werden.

Gedacht wurde dabei an Online-Dienste wie etwa ein Musik-Streaming-Dienst, von dem die Benutzer nunmehr verlangen können, dass die Liste der von ihnen gespielten Titel oder ihre persönlichen Wiedergabelisten ihnen auf Verlangen kostenlos in einem elektronischen Datenformat zwecks Wiederverwendung an anderer Stelle herausgegeben wird. Das Recht auf Datenkopie gilt allerdings universell, nicht nur für Online-Dienste. Es wird sich zeigen müssen, wo es in der Praxis tatsächlich eine Rolle spielt und was die Folgen sein werden. Dies ist noch völlig unklar.

- ☐ Haben wir **jemanden**, der sich darum kümmern wird und diese Person weiss, was sie zu tun hat oder wird sich kundig machen.
  - ☐ Wir **meinen** in Anbetracht der bisherigen Erfahrungen mit solchen Anfragen, dass **das genügen wird.** → 1. **OK**
- ☐ Wir meinen, vernünftigerweise **keine solchen Anfragen** zu erhalten. Wir haben daher auch keinen Prozess dafür und würden **ad-hoc** reagieren, sollte es trotzdem einmal eine Anfrage geben. → 1. **OK**
- ☐ Ist **uns nicht wirklich klar**, wie mit solchen Anfragen in organisatorischer Hinsicht umgehen würden.

☐ Wir haben von betroffenen Personen Daten **für unsere eigenen Zwecke erhalten**, bearbeiten diese **mit unseren Computern** (falls eines der beiden Dinge nicht zutrifft: → 2. + 3. + 4. **OK**) und wird tun dies auf einer der beiden folgenden Rechtsgrundlagen:

- ☐ Weil **für den Abschluss** oder **die Abwicklung eines Vertrags** mit der betroffenen Person nötig. → 2. **OK**
- ☐ Weil wir dafür eine **Einwilligung** der betroffenen Person eingeholt haben. → 2. **OK**

☐ Wir sind in der Lage, ihre so bearbeiteten Daten auf Wunsch der betroffenen Person **aus unseren Systemen zu extrahieren** und ihr oder einem von ihr bezeichneten Dritten (z.B. Konkurrent) in einem strukturierten, gängigen und **maschinenlesbaren Format** zu geben (solange Dritte darin in ihren Rechten nicht tangiert sind).

- ☐ Wir können dabei sicherstellen, dass **Dritte** in ihren Rechten dadurch **nicht verletzt** werden. → 3. **OK**

☐ Wir **informieren** die betroffenen Personen **über dieses Recht**, soweit es besteht (falls nein: → 4. **OK**). → 4. **OK**

☐ Wir haben so bearbeitete Daten, sind aber **nicht in der Lage**, der betroffenen Person diese Daten **herauszugeben**, so dass sie sie für sich weiterbenutzen kann.

- ☐ Wir sollten festlegen, wer intern für die Behandlung von Datenportabilitätsansprüchen verantwortlich ist und sicherstellen, dass die zuständige Person weiss, was zu tun ist (oder dies bei Bedarf herausfinden kann).
- ☐ Wir sollten Richtlinien definieren, wie Anfragen auf Herausgabe der eigenen Daten beantwortet werden können.
- ☐ Wir sollten Standardschreiben bzw. Templates für die Beantwortung von Auskunftsgesuchen definieren.
- ☐ Wir sollten festhalten, wo welche Informationen im Falle eines Auskunftsersuchens gefunden bzw. extrahiert werden können.
- ☐ Wir sollten einen Prozess zum Abdecken oder Entfernen von Drittinformationen vorsehen, falls solche geschützt werden müssen.
- ☐ Wir sollten unsere Systeme so programmieren, dass wir die verlangten Daten einfach herausziehen und wie erforderlich aufbereiten können.
- ☐ Wir sollten mit Mitbewerbern diskutieren, ob und wie sie solche herausverlangten Daten übernehmen können, und umgekehrt.
- ☐ Wir sollten die Mitarbeiter schulen, mit Anfragen betr. Datenportabilität umzugehen.
- ☐ Andere Massnahme:

- ☐ Folgende Person kann intern die für die Umsetzung der Massnahmen nötigen Informationen liefern:

		☐ Wir möchten noch Folgendes vermerken:	☐ **Situation unklar** Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren ☐ Bis zur ☐ Klärung bzw. ☐ Umsetzung der Massnahmen ☐ Sollten wir weitermachen wie bisher. ☐ Treffen wir folgende Sofortmassnahmen: ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

Weitere Bemerkungen:

Risikobeurteilung

Prozessowner	Datenschutzstelle
Wir sind zur Ansicht gekommen, dass die oben beurteilte Datenbearbeitung (ohne die ausgeschlossenen Teile) grundsätzlich datenschutzkonform ist: ☐ Ja ☐ Nein Wir sehen folgende Risiken hinsichtlich des Datenschutzes: Wir schlagen folgende Massnahmen vor, um die Risiken zu minimieren: ☐ Die Datenbearbeitung sollte ins Risikoinventar aufgenommen werden	Wir teilen die Ansicht des Prozessowners ☐ Ja ☐ Nein Die Datenbearbeitung (ohne die ausgeschlossenen Teile) ist unserer Beurteilung nach grundsätzlich datenschutzkonform ☐ Ja ☐ Nein Begründung: Wir schlagen folgende Massnahmen vor, um die Risiken zu minimieren: ☐ Die Datenbearbeitung wird ins Risikoinventar aufgenommen

Stellungnahme des Prozessowners zur Beurteilung der Datenschutzstelle:

Diese Risiken (soweit vorhanden) werden vom Prozessowner akzeptiert: ☐ Ja ☐ Nein Datum, Name: _____