Compliance Check III – Auftragsbearbeitung

Formular F.1

Unternehmenseinheit: _____ Ausgefüllt von: _____ Stand vom: _____

☐ Das Unternehmen bearbeitet die Daten in der Rolle des Verantwortlichen (falls in der Rolle des Auftragsbearbeiters → Formular E.2 ausfüllen)

Dieses Formular wird für folgenden Auftragsbearbeiter ausgefüllt: _____

Er ist an den folgenden Datenbearbeitung(en) beteiligt: _____ **DB-Nr:** _____

_____ **DB-Nr:** _____

_____ **DB-Nr:** _____

☐ Es besteht noch kein Vertrag. Dieses Formular dient der **Vorabüberprüfung** zwecks Freigabe des Vertragsschlusses.

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

☐ FINMA RS 2018|3 "Outsourcing" (→ Q11)

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

☐ Ich
☐ Folgende Personen (Name, Kontakt, Thema): _____

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

☐ Ich
☐ Folgende Personen (Name, Kontakt, Thema): _____

Arbeitsanweisung:

- Dieses Formular dient dazu, die Konformität einer Auftragsbearbeitung zu beurteilen. Es funktioniert nach dem Prinzip der **Selbst-Deklaration**. Wer dieses Formular ausfüllt, muss selbst entscheiden, welchen Anspruch er hat, ist aber auch selbst für seine Deklaration und Einschätzung **verantwortlich**. Das Formular erlaubt dabei auch pragmatische Einschätzungen.

- Für **jeden Auftragsbearbeiter** und **jeden Vertrag** mit diesem ist in der Regel ein **separates Formular** auszufüllen; dient seine Leistung mehreren Datenbearbeitungen (z.B. Betrieb eines Systems, das für verschiedene Bearbeitungen genutzt wird), kann dies auf dem Deckblatt vermerkt werden.

- Das Formular kann entweder zur **Vorabprüfung** einer Auftragsbearbeitung oder zur Prüfung einer **bestehenden Auftragsbearbeitung** benutzt werden. Beurteilt wird, ob sie die Vorgaben des revidierten DSG und der DSGVO einhält. Ist dies nicht der Fall, können Massnahmen zur Behebung des Defizits empfohlen werden.

- Für jede Anforderung ist in der **mittleren Spalte** anzugeben, wie es sich *im Moment* verhält mit Bezug auf die Auftragsbearbeitung, 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. Ob sie in jedem Fall gelten, wird mit diesem Formular nicht geprüft.

- Die Aussagen **"Kurz und bündig"** und **"Im Detail"** sind gleichwertig. Wer sich jedoch nicht sicher ist oder die Situation sich etwas differenzierter darstellt, sollte die Aussagen "Im Detail" wählen, die den Sachverhalt etwas differenzierter und auf verschiedene Teilaspekte aufgebrochen darlegt. Wer überhaupt nicht weiterkommt, gibt dies in der rechten Spalte (**"Situation unklar"**) an und muss dies eskalieren (z.B. mit dem internen Datenschutzverantwortlichen oder Rechtsdienst besprechen). Für gewisse, weit verbreitete Auftragsbearbeiter mit standardisierten Verträgen wurden **Standardantworten** vorbereitet. Diese sollen ausgebaut werden.

- Darüber hinaus dient die **rechte Spalte** der Selbst-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 Auftragsbearbeitung **trotzdem konform** sein, bedarf aber einer besonderen Beurteilung (vom internen Datenschutzverantwortlichen, dem Rechtsdienst oder einem externen Experten).

		Anforderung	Anforderung erfüllt?	Was zu tun ist
	Q1	**Auftragsbearbeiter** Es ist der Auftragsbearbeiter (d.h. die rechtliche Einheit, die Vertragspartner ist) zu dokumentieren und die Kontaktpersonen sind festzuhalten, insbesondere für die datenschutzrechtlichen Belange. Im Falle einer Auftragsbearbeitung muss der Verantwortliche wissen, an wen er sich bei entsprechenden Vorkommnissen wenden kann. Kann der Auftragsbearbeiter keine für den Datenschutz zuständigen Personen nennen, deutet dies darauf hin, dass er sich mit dieser Frage nicht hinreichend auseinandergesetzt hat.	*Kurz und bündig:* ☐ Microsoft (für Azure, O365 in Europa): Microsoft Ireland Operations, Ltd., One Microsoft Place, South County Industrial Park, Leopardstown, Dublin 18, D18 P521, Irland; Datenschutzbeauftragter: Selbe Adresse, "Attn: Data protection" und online erreichbar unter Online erreichbar unter http://go.microsoft.com/?linkid=9846224. Technischer und administrativer Kontakt: https://support.microsoft.com/de-ch/contactus/, https://support.microsoft.com/de-ch/contactus/. *Im Detail:* **Name**: ☐ Es handelt sich um eine konzerninterne Auslagerung **Adresse**: **Technischer Kontakt:** **Administrativer Kontakt**:	☐ **Folgende Massnahmen** sollten ergriffen werden, damit die Anforderung erfüllt ist: ☐ Es sollte ein Kontakt für Anliegen zur Datensicherheit festgehalten werden. ☐ Es sollte ein Kontakt für Anliegen zum Datenschutz (exkl. Datensicherheit) festgehalten werden. ☐ Es sollten noch folgende Informationen beschafft werden: ☐ Andere: ☐ 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:

			Datenschutzbeauftragter nach Art. 37 DSGVO: ☐ Keiner **EU-Vertreter** nach Art. 27 DSGVO: ☐ Keiner Ansprechpartner für **Datenschutzfragen**: ☐ Wie technischer Kontakt Ansprechpartner für **Datensicherheit**: ☐ Wie technischer Kontakt	☐ Sollten wir die Auftragsbearbeitung wie folgt einschränken/stoppen:
	Q2	**Standorte der Datenbearbeitung** Der Verantwortliche muss wissen, wo seine Daten bearbeitet werden, auch wenn sie in den Händen des Auftragsbearbeiters sind. Diese Information braucht der Verantwortliche einerseits für die Beurteilung der Risiken, die mit der Bearbeitung seiner Daten in unterschiedlichen Länder verbunden sind (und den dazu ergreifenden Gegenmassnahmen), andererseits, weil er die Länder, in welchen seine Daten bearbeitet werden, im Inventar bzw. in den betreffenden Datenschutzerklärungen aufführen muss.	*Kurz und bündig:* ☐ Microsoft Azure/O365, mit Europa-Option: Lagerung der Daten in Irland und den Niederlanden (im Verlaufe des Jahres 2019 auch in der Schweiz), Zugriff jedoch aus allen Ländern der Welt möglich. Link: https://www.microsoft.com/de-de/trustcenter/privacy/where-your-data-is-located, https://azure.microsoft.com/en-us/global-infrastructure/regions#services.	☐ Der Auftragsbearbeiter **bearbeitet die Daten mindestens teilweise in der EU** (bzw. des EWR). Daher findet die DSGVO auf ihn Anwendung (und *er* muss einen Vertrag gemäss Art. 28 DSGVO abschliessen). ☐ **Folgende Massnahmen** sollten ergriffen werden, damit die Anforderung erfüllt ist: ☐ Es sollten die Länder, in welchen die Daten gelagert werden, abgeklärt werden. ☐ Es sollten die Länder, von welchen aus auf die Daten zugegriffen werden kann, abgeklärt werden.

Im Detail:

An folgenden Orten können unsere Daten vom Auftragsbearbeiter **gelagert** werden:

☐ Schweiz ☐ EU/EWR ☐ UK ☐ USA ☐ weltweit

Von folgenden Orten aus kann der Auftragsbearbeiter auf unsere Daten **zugreifen**:

☐ Schweiz ☐ EU/EWR ☐ UK ☐ USA ☐ weltweit

Der Auftragsbearbeiter **dokumentiert** dies unter folgendem Link:

☐ Es sollten die Länder zur Lagerung bzw. für den Zugriff wie folgt eingeschränkt werden (z.B. durch Wahl der entsprechenden Service-Option):

☐ Andere:

☐ 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 Auftragsbearbeitung wie folgt einschränken/stoppen:

Q3

Auswahl des Auftragsbearbeiters

Der Auftragsbearbeiter ist sorgfältig ausgewählt. Er bietet Gewähr für die Einhaltung der vertraglichen Vorgaben, einschliesslich der Datensicherheit (dazu Q4). Den datenschutzrechtlichen Risiken ist im Rahmen seiner Auswahl und Beauftragung Rechnung getragen.

Es ist nicht mit einem guten Vertrag getan. Der Verantwortliche muss sich vergewissern, dass der Auftragsbearbeiter in jeder Hinsicht in der Lage ist, den Vertrag auch einzuhalten und den dazu nötigen Willen aufweist. Insbesondere sollte sich der Verantwortliche ein Bild darüber machen, ob seine Daten beim Auftragsbearbeiter dereinst sicher sein werden. Diese "Due Diligence" ist vor der Auslagerung zu betreiben, hängt aber in ihrer Tiefe stark von den mit der Auslagerung verbundenen Risiken ab, und natürlich den Möglichkeiten des Verantwortlichen. Wenn ein KMU seine durchschnittlich heiklen Kundendaten in die Cloud zu einem der grossen, etablierten Anbieter in diesem Bereich auslagert, kann von diesem KMU keine eingehende Überprüfung der IT-Sicherheit erwartet werden. Das KMU wird sich auf den guten Ruf und die Zusicherungen des Anbieters verlassen, und den Umstand, dass auch grosse Unternehmen, die über eigene Sicherheitsexperten verfügen, diesen Anbieter einsetzen. Es ist also auch in diesem Bereich gesunder Menschenverstand verlangt.

Kurz und bündig:

☐ Der Auftragsbearbeiter wurde von uns in einem dokumentierten Prozess unter Berücksichtigung der datenschutzrechtlichen Risiken und entsprechenden Anforderungen ausgewählt. → **hier alles OK**

☐ Der Auftragsbearbeiter zählt zu den anerkannten Standardanbietern für solche Aufgaben. Seine Eignung steht unseres Erachtens ausser Frage. → **hier alles OK**

Im Detail:

☐ Mit der Auftragsbearbeitung sind nach unserer Ansicht **keine besonderen Risiken** verbunden. Wir haben ein Unternehmen gewählt, das uns fähig und willens schien, den Auftrag korrekt auszuführen und sich an den Vertrag zu halten. → **hier alles OK**

☐ Mit der Auftragsbearbeitung sind **gewisse datenschutzrechtliche Risiken** verbunden (Verlust wichtiger Daten, Bearbeitung sensitiver Daten, heikle Bearbeitungsvorgänge, etc.). Wir haben daher:

- ☐ Eine **Risikoanalyse** durchgeführt, unter besonderer Berücksichtigung der Datensicherheit.
- ☐ Uns **vergewissert**, dass der Auftragsbearbeiter finanziell, technisch und personell **in der Lage** ist, unsere Daten datenschutzkonform zu bearbeiten und insbesondere den Vertrag und die Datensicherheit einzuhalten.
- ☐ Die Möglichkeit eines **Wechsels** und **Ausfalls** des Auftragsbearbeiters berücksichtigt.
- ☐ Und sind in allen Punkten zu einem **befriedigenden Ergebnis** gekommen. → **hier alles OK**

☐ Mit der Auftragsbearbeitung sind zwar **gewisse datenschutzrechtliche Risiken** verbunden, aber:

- ☐ Wir **wissen nicht mehr genau**, wie oder warum wir gerade diesen Auftragsbearbeiter gewählt haben:
  - ☐ Wir haben aber **keine Hinweise** oder schlechten Erfahrungen, die uns seine Eignung in Zweifel ziehen lassen. → **hier alles OK**

☐ Die Anforderung ist unseres Erachtens grundsätzlich **erfüllt** und es sind daher **keine Massnahmen nötig.**

☐ **Folgende Massnahmen** sollten ergriffen werden, damit die Anforderung erfüllt ist:

- ☐ Es sollte eine Risikoanalyse durchgeführt werden, um zu beurteilen, ob die Risiken angemessen abgedeckt sind.
- ☐ Der Auftragsbearbeiter sollte auf seine Eignung überprüft werden bzw. die bereits erfolgte Überprüfung sollte vertieft werden.
- ☐ Es sollte sichergestellt werden, dass das Unternehmen bezüglich seiner Datenbearbeitung den Auftragsbearbeiter vernünftig wechseln kann und bei einem Ausfall geschützt ist.
- ☐ Die Auswahl des Anbieters sollte sauber dokumentiert werden.
- ☐ Andere:

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

☐ Situation unklar

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

			☐ Wir haben von fachkundiger Seite die aus unserer Sicht erforderlichen **Empfehlungen** und **Referenzen** für die Beauftragung dieses Unternehmens erhalten. → **hier alles OK** ☐ Wir haben einfach **irgendein Unternehmen** beauftragt. ☐ Unser Auftragsbearbeiter **erfüllt die Anforderungen** an einen Auftragsbearbeiter (unabhängig von der Datensicherheit) in Anbetracht der datenschutzrechtlichen Risiken **nicht (mehr) wirklich:** ☐ 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:
	Q4	**Datensicherheit** Die Einhaltung Datensicherheit ist auch seitens des Auftragsbearbeiters gewährleistet. Die dazu erforderlichen Vorgaben sind festgelegt. *Art. [8] Abs. 2 DSG* Siehe die Bemerkungen zu Q4. In der Praxis liefert die Tatsache, dass ein Anbieter sich nach ISO 27001 hat zertifizieren lassen, meist eine gute Indikation über die Qualität der von ihm betriebenen Datensicherheit, auch wenn die Zertifizierung für sich kein abschliessendes Bild ermöglicht.	*Kurz und bündig:* ☐ Unsere Spezialisten haben die vom Auftragsbearbeiter für unsere Datenbearbeitung vorgesehene Datensicherheit fachmännisch überprüft und erachten sie als in Anbetracht der Risiken als angemessen und dem Stand der Technik entsprechend. → **hier alles OK** ☐ Wir sind zwar keine Spezialisten für Datensicherheit, aber der Auftragsbearbeiter hat diesbezüglich einen guten Ruf, wird von vielen Unternehmen in Anspruch genommen und verfügt über aktuelle Prüftestate nach ISO 27001. → **hier alles OK** ☐ Es handelt sich um ein konzerninternes Outsourcing. Der Auftragsbearbeiter unterliegt vergleichbaren Vorgaben an die Datensicherheit wie wir sie auch haben. → **hier alles OK** ☐ Wir wissen nicht, ob der Auftragsbearbeiter die Datensicherheit gewährleisten kann.	☐ Die Anforderung ist unseres Erachtens grundsätzlich **erfüllt** und es sind daher **keine Massnahmen nötig.** ☐ **Folgende Massnahmen** sollten ergriffen werden, damit die Anforderung erfüllt ist: ☐ Es sollte eine Analyse der Datensicherheitsrisiken durchgeführt werden, damit wir besser verstehen, welche Risiken wie gut abgedeckt sind. ☐ Es sollten die zur Datensicherheit seitens des Auftragsbearbeiters vorgesehenen Massnahmen auf ihre Angemessenheit überprüft werden. ☐ Es sollten Vorgaben zur Datensicherheit definiert und dem Auftragsbearbeiter auferlegt werden. ☐ Es sollten die Massnahmen zur Datensicherheit seitens des Auftragsbearbeiters verstärkt werden, insbesondere um folgende Risiken abzudecken:

Im Detail:

☐ Wir haben uns **Gedanken dazu gemacht**, welchen **Sicherheitsrisiken** unsere Daten und Datenbearbeitung beim Auftragsbearbeiter in Anbetracht ihres Zwecks, ihrer Art und ihres Umfangs ausgesetzt sind. Insbesondere: → 1. **OK**

- ☐ Wir wissen, welche **Art von Personendaten** der Auftragsbearbeiter für uns bearbeitet (Mitarbeiterdaten, Kundendaten, öffentliche Daten, Gesundheitsdaten, Marketingdaten, etc.).
- ☐ Wir wissen, welcher **Vertraulichkeit** die Daten unterliegen (geheim, vertraulich, nur für internen Gebrauch, öffentlich) bzw. haben würden (hätten wir eine Klassifikation).
- ☐ Wir wissen, **wo die Daten gespeichert**, allenfalls auch bearbeitet sein werden (Ortschaft, Art der Standorts wie z.B. privates, dediziertes Hosting in einem RZ, eigene virtuelle Server auf gemeinsamer Infrastruktur mit anderen Kunden, gemeinsame Anwendung).
- ☐ Wir kennen die **Unterauftragnehmer** bzw. haben eine Liste davon.
- ☐ Wir haben uns Gedanken dazu gemacht, wie **wahrscheinlich** es ist und welche **Folgen** es hätte, dass bzw. wenn die vom Auftragsbearbeiter benutzten Systeme dauerhaft nicht mehr verfügbar wären oder unbefugte Dritte (Öffentlichkeit, Konkurrenz) darauf Zugriff erhalten würden. Diese Folgen sind wahrscheinlich:

☐ Unbedeutend	☐ Kunden & Partner	
☐ Gering	☐ Geschäftsbetrieb	
☐ Mittel	☐ Recht und Compliance	
☐ Gross	☐ Finanzwesen	
☐ Existenziell	☐ Ruf	☐ Strategie

☐ Es sollte vorgesehen werden, dass die Datensicherheit des Auftragsbearbeiters überprüft werden kann.

☐ Es sollten die Nachweise der Einhaltung der Datensicherheit des Auftragsbearbeiters überprüft werden.

☐ Andere:

☐ 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.

☐ Bemerkungen:

☐ Die **nötigen Massnahmen** zur Datensicherheit sind im Rahmen der Auftragsbearbeitung:

- ☐ **Von uns vorgegeben** und vom Auftragsbearbeiter so **akzeptiert** und **vertraglich vereinbart**. → 2. **OK**
- ☐ Sind **vom Auftragsbearbeiter** nach seinen Standards **definiert**, die wir für akzeptabel befunden haben. → 2. **OK**
- ☐ Durch unseren **gemeinsamen Konzern** festgelegt; der Auftragsbearbeiter und wir haben dieselben Vorgaben, die uns auch für angemessen erscheinen. → 2. **OK**
- ☐ Sind vom Auftragsbearbeiter nach seinen Standards definiert, aber **wir haben sie nicht überprüft**.
- ☐ Sind **nicht definiert**.

☐ Damit **sichergestellt** ist, dass der Auftragsbearbeiter die Massnahmen zur Datensicherheit auch **tatsächlich einhält**:

- ☐ Haben wir ein **Recht**, dies beim Auftragsbearbeiter zu **überprüfen** und entsprechende Unterlagen einzusehen. → 3. **OK**
- ☐ Lässt der Auftragsbearbeiter dies regelmässig **von dritten Prüfstellen überprüfen**, wobei wir diese Testate einsehen können. → 3. **OK**
- ☐ Haben wir **keine besonderen Vorkehrungen** getroffen. Das erscheint angesichts der geringen Risiken aber auch als nicht nötig. → 3. **OK**
- ☐ Wird seitens des **Konzerns sichergestellt**. → 3. **OK**
- ☐ **Wissen wir nicht** und können wir auch **nicht überprüfen**.

☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

			☐ Wir möchten noch Folgendes vermerken: [ ]	
	Q5	**Keine entgegenstehenden Geheimhaltungspflichten** Es bestehen keine gesetzlichen oder vertraglichen Geheimhaltungspflichten seitens des Unternehmens, welche die Beauftragung eines Dritten mit der Bearbeitung der Daten untersagen. *Art. [8] Abs. 1 Bst. b DSG* In seltenen Fällen kann es vorkommen, dass der Verantwortliche gegenüber den Personen, deren Daten er bearbeitet, eine Geheimhaltungspflicht hat, die ihm die Auslagerung der Datenbearbeitung an einen Provider untersagt. Ob dies der Fall ist, hängt von der Art und Tragweite der Geheimhaltungspflicht ab. Diese ergibt sich u.a. aus der Natur der Geheimhaltungspflicht (Bankgeheimnis, Anwaltsgeheimnis, Arztgeheimnis, Fernmeldegeheimnis, anderes vertragliches Geheimnis, etc.) und dem, was mit den Kunden bzw. Geheimnisherrn vereinbart worden ist. So gilt das Bankgeheimnis als besonders restriktiv, was die grenzüberschreitende Bekanntgabe ohne Bankgeheimnisverzicht des Kunden betrifft: Eine Schweizer Bank darf zum Beispiel ohne Einwilligung seitens des Kunden dessen Daten normalerweise nicht ins Ausland übermitteln. Die Nutzung einer Cloud in der EU würde gegen das Bankgeheimnis verstossen und wäre daher unzulässig. Hingegen lässt das Bankgeheimnis eine Auslagerung an eine Cloud in der Schweiz ohne Weiteres zu, wenn diese über eine hinreichende Datensicherheit verfügt.	*Kurz und bündig:* ☐ Die Daten unterliegen keinen besonderen Geheimhaltungspflichten, die ein Outsourcing der Datenbearbeitung irgendwie verbieten würden (z.B. Personaldaten). → **hier alles OK** ☐ Wir haben zwar Geheimhaltungspflichten, aber Fachspezialisten haben diese Frage schon abgeklärt und die Auftragsbearbeitung für zulässig befunden. → **hier alles OK** ☐ Die Daten unterliegen einem Berufsgeheimnis, haben diese Frage aber nicht geprüft. Die Daten können über die Cloud oder sonst durchaus auch ins Ausland gelangen. *Im Detail:* ☐ Es liegt **einer** der **folgenden Fälle** vor: → **hier alles OK** ☐ **Öffentlich zugängliche Daten**. ☐ Daten des **eigenen Personals**. ☐ Daten der **Besucher unserer Website** oder Benutzer unserer **Apps** und wir haben ihnen nicht versprochen, dass wir die Bearbeitung ihrer Daten nicht auslagern. ☐ Daten von Personen, die **davon ausgehen müssen**, dass wir die Bearbeitung ihrer Daten wie hier auslagern, und unsere Verträge mit ihnen sprechen auch nicht dagegen. ☐ **Weder Kundendaten noch** sonst Daten einer **Person, mit welcher wir einen Vertrag haben**, und es gibt auch keinen Grund, warum die betroffenen Personen darauf vertrauen dürfen, dass wir ihr Daten nicht einem Dritten zur Bearbeitung geben. ☐ Die Daten stehen im Zusammenhang mit **Vertragsbeziehungen**, in denen wir uns **zur Geheimhaltung verpflichtet** haben (wenn nicht: → 1. **OK**):	☐ Die Anforderung ist unseres Erachtens grundsätzlich **erfüllt** und es sind daher **keine Massnahmen nötig.** ☐ **Folgende Massnahmen** sollten ergriffen werden, damit die Anforderung erfüllt ist: ☐ Es sollte die anwendbaren Geheimhaltungsklauseln im Hinblick auf die Auslagerung geprüft werden. ☐ Es sollte von den Vertragsparteien, die die Auslagerung mit ihren Geheimhaltungsklauseln verbieten, eine Zustimmung zur Auftragsbearbeitung eingeholt werden. ☐ Es sollten von den betroffenen Kunden eine Zustimmung zur Auftragsbearbeitung eingeholt werden. ☐ Es sollte mit dem Auftragsbearbeiter eine Geheimhaltungserklärung abgeschlossen werden. ☐ Die Geheimhaltungserklärung des Auftragsbearbeiters sollte in folgenden Punkten verbessert werden: [ ] ☐ Es sollten die folgenden Daten anonymisiert werden. Damit löst sich das Geheimhaltungsproblem: [ ] ☐ Andere: [ ]

Andere Geheimhaltungspflichten sind weniger restriktiv. Die sozialversicherungsrechtliche Schweigepflicht oder das Arzt- und Apothekergeheimnis verbietet die grenzüberschreitende Bekanntgabe nach herrschender Auffassung zum Beispiel nicht. Die Auslagerung sogar ins Ausland kann hier ohne Weiteres erlaubt sein, aber besondere Vorkehrungen wie z.B. die Unterzeichnung einer zusätzlichen Vertraulichkeitserklärung seitens des Auftragsbearbeiters können nötig sein.

Es sollte daher geprüft werden, ob bezüglich der auszulagernden Daten irgendwelche Geheimhaltungspflichten bestehen, die der Auslagerung entgegenstehen könnten.

- ☐ Die Geheimhaltungsklausel **behält Auslagerungen ausdrücklich vor**. → 1. **OK**
- ☐ Die Geheimhaltungsklausel **sagt nichts zur Frage**, ob wir die Daten einem Auftragsbearbeiter geben dürfen, aber es gibt keinen Grund zur Annahme, dass die Parteien die vorliegende Auslagerung damit ausschliessen wollten. → 1. **OK**
- ☐ Die Geheimhaltungsklausel **verbietet die Auslagerung**.

☐ Wir unterstehen mit Bezug auf die Daten einem **Amts- oder Berufsgeheimnis** (wenn nicht: → 2. **OK**), nämlich:

- ☐ **Berufliche Schweigepflicht** gemäss Art. [56] DSG → 2. **OK**
- ☐ **Sozialversicherungsrechtliche Schweigepflicht** gemäss Art. 33 ATSG → 2. **OK**
- ☐ **Arzt- und Apothekergeheimnis** → 2. **OK**
- ☐ **Fernmelde-, Bank-, Börsenhändler-, Anwalts- und Revisionsgeheimnis:**
  - ☐ Die Daten **bleiben in der Schweiz** (kein Zugriff aus dem Ausland). → 2. **OK**
  - ☐ Die Daten **gehen ins Ausland**, aber es liegen Zustimmungserklärungen vor. → 2. **OK**
  - ☐ Die Daten **gehen ins Ausland**, aber es liegt **keine Zustimmung** vor und auch kein anderer Rechtfertigungsgrund.
- ☐ **Amtsgeheimnis:**
  - ☐ Die Daten **bleiben in der Schweiz** (kein Zugriff aus dem Ausland). → 2. **OK**
  - ☐ Die Daten **gehen ins Ausland**, aber es sind nicht Daten, an denen eine ausländische Behörde ein erhöhtes Interesse hat. → 2. **OK**
  - ☐ Die Daten **gehen ins Ausland** und sie sind für die Behörden in jenen Ländern aus **fiskalischen, politischen, nachrichtendienstlichen** oder **anderen Gründen** von Interesse.

☐ 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:

			☐ Andere **gesetzliche Geheimhaltungspflicht**: ☐ Soweit die Daten einem **Amts- oder Berufsgeheimnis** oder **vertraglichen Geheimhaltungspflicht** unterstehen (wenn nicht: → 3. + 4. **OK**): ☐ Haben wir den **Auftragsbearbeiter** zur Geheimhaltung der Daten **verpflichtet**. → 3. **OK** ☐ Haben wir **keine Gründe anzunehmen**, dass der Auftragsbearbeiter die Daten **nicht geheim halten wird**. → 4. **OK** ☐ Wir möchten noch Folgendes vermerken:	
	Q6	**Vertrag (nur DSG)** *Falls auch die DSGVO zu beachten ist, kann gleich mit Q7 weiterverfahren werden. Die dortigen Anforderungen sind strenger als jene nach DSG.*	*Kurz und bündig:* ☐ Die Datenschutzbestimmungen, die für die Auftragsbearbeitung gelten, wurden von Spezialisten überprüft und für nach dem bisherigen DSG oder EU-Datenschutzrecht für rechtskonform befunden. Ferner sieht der Vertrag vor, dass Unterauftragsbearbeiter nur mit unserer Genehmigung beigezogen werden dürfen. → **hier alles OK** ☐ Die vertraglich anwendbaren Datenschutzbestimmungen entsprechen den Vorgaben der DSGVO gemäss Q7. → **hier alles OK** ☐ Die vertraglich anwendbaren Datenschutzbestimmungen entsprechen inhaltlich den Vorgaben der EU-Musterklauseln für Auftragsbearbeiter. → **hier alles OK** ☐ Es gelten die Online-Service-Terms von Microsoft (OST Version September 2017 oder jünger, https://www.microsoft.com/en-us/licensing/product-licensing/products.aspx) und die Datenbearbeitung weist keine besonderen Risikofaktoren auf, die allenfalls zu berücksichtigen wären. → **hier alles OK**	☐ Die Anforderung ist unseres Erachtens grundsätzlich **erfüllt** und es sind daher **keine Massnahmen nötig.** ☐ **Folgende Massnahmen** sollten ergriffen werden, damit die Anforderung erfüllt ist: ☐ Es sollten die Allgemeinen Geschäftsbedingungen des Auftragsbearbeiters (AGB) besorgt und geprüft werden. Sie liegen bis jetzt nicht vor. ☐ Es sollte ein Vertrag mit dem Auftragsbearbeiter abgeschlossen werden bzw. das Vertragsverhältnis sollte dokumentiert werden. ☐ Der Vertrag mit dem Auftragsbearbeiter sollte von einem Spezialisten auf seine Konformität mit dem DSG überprüft werden. ☐ Es sollte ein Vertrag gemäss den Vorgaben der DSGVO abgeschlossen werden.

Es besteht ein Vertrag mit dem Auftragsbearbeiter, der seine Bearbeitung der Daten des Unternehmens regelt und sicherstellt, dass dieser sie nur so bearbeitet, wie das Unternehmen selbst es tun dürfte. Insbesondere enthält er ein Weisungsrecht, untersagt dem Auftragsbearbeiter die Bearbeitung der Daten für eigene Zwecke und erlaubt dem Auftragsbearbeiter die Delegation der Bearbeitung an einen Unterauftragsbearbeiter nur mit Genehmigung des Unternehmens (wobei ein Vetorecht für dieses genügt). Der Vertrag muss auch die Einhaltung der Datensicherheit vorsehen, entsprechende Prüfrechte

und sicherstellen, dass der Export ins Ausland den Anforderungen des DSG genügt und der Verantwortliche seinen Pflichten gegenüber den betroffenen

Personen nachkommen kann. Nach Beendigung der Auftragsbearbeitung sind die Daten dem Unternehmen zurückzugeben.

Art. [8] Abs. 1 Bst. a DSG, Art. [8] Abs. 3 DSG

Die Vorgaben des DSG sind etwas weniger formal und weniger streng als jene unter der DSGVO. Muss ohnehin auch die DSGVO eingehalten werden, so ist daher keine separate Prüfung des Vertrags unter dem DSG notwendig.

☐ Die Datenbearbeitung ist weitgehend risikolos. Der Auftragsbearbeiter ist uns gegenüber vertraglich verpflichtet, die Daten nur für unsere Zwecke und nur nach unseren Instruktionen zu bearbeiten, Unterauftragsbearbeiter nur mit unserer Genehmigung beizuziehen, und eine angemessene Datensicherheit zu gewährleisten. Wir haben ihn so instruiert, dass er mit den Daten nur das tut, was wir auch selbst tun dürften. Die Daten bleiben in Europa. → **hier alles OK**

☐ Wir haben keine besonderen Datenschutzbestimmungen im Vertrag und unser Auftragsbearbeiter unterliegt auch keinen besonderen Berufsgeheimnis- und Standesregeln, wie er mit unseren Daten umzugehen hat.

Im Detail:

☐ Die Zusammenarbeit mit dem Auftragsbearbeiter ist **vertraglich** wie folgt geregelt:

- ☐ In einem **schriftlichen** Vertrag. → 1. **OK**
- ☐ In einem **online** abgeschlossenen Vertrag. → 1. **OK**
- ☐ Sie erfolgt auf Basis einer **Bestellung**, auf welche die allgemeinen Geschäftsbedingungen (**AGB**) des Dienstleisters Anwendung finden. Sie liegen uns vor. → 1. **OK**
- ☐ Sie erfolgt auf Basis einer **mündlichen Absprache**. Aber es finden die allgemeinen Geschäftsbedingungen (**AGB**) des Dienstleisters Anwendung. Sie liegen uns vor. → 1. **OK**
- ☐ Es gibt **keine spezifische vertragliche Regelung**, aber der Datenschutz ist geregelt (z.B. durch eine separate Konzernvereinbarung oder verbindliche Konzernrichtlinie). → 1. **OK**
- ☐ Es gibt **keine Regelung**. Der Provider kann im Grunde tun, was er will.
- ☐ Es ist anders:

☐ Der Vertrag sollte in den folgenden Punkten nachgebessert werden:

☐ Andere:

☐ 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:

			Die Vorgaben unter dem revidierten DSG sind gegenüber den bisherigen Vorgaben für eine Auftragsbearbeitung nur in einem Punkt strenger geworden: Der Einsatz von Subunternehmern bedarf neu der Genehmigung des Kunden, wobei es genügt, ihm ein Vetorecht einzuräumen. Die Kriterien in der mittleren Spalte entsprechend den heute gängigen Anforderungen. Von diesen kann allerdings abgewichen werden, je nachdem wie heikel die Auftragsbearbeitung bzw. die Bearbeitung, um die es geht, ist.	☐ Im Rahmen der zwischen uns und dem Auftragsbearbeiter geltende Regelung ist **sichergestellt**, dass er die mit Bezug auf die ihm übergebenen Daten **alle folgenden Punkte erfüllt**: → 2. **OK** ☐ Er bearbeitet sie **nur für unsere Zwecke**, nicht auch für eigene oder Dritte Zwecke. ☐ Er tut dabei nur das, was die **Leistungsumschreibung** oder wir von ihm verlangen. Wir haben im Rahmen der Leistungsumschreibung ein **Weisungsrecht**. Er kann die Leistungen auch nicht ändern, ohne dass wir nicht mindestens ein Veto-Recht haben. ☐ Er darf **Dritte**, jedenfalls wenn sie Zugang zu unseren Daten erhalten, nur beiziehen, **wenn wir das genehmigt haben** oder wir zumindest darüber in Kenntnis gesetzt werden müssen und ein Veto-Recht haben, und für diese Dritten mindestens gleich strenge Regeln gelten wie für den Auftragsbearbeiter. ☐ Er muss für **angemessene technische und organisatorische Massnahmen zur Datensicherheit** sorgen, diese regelmässig überprüfen und auf dem neusten Stand halten. ☐ **Verletzungen der Datensicherheit** müssen uns **umgehend gemeldet** werden. ☐ Er darf Personendaten nur dann **im Ausland zugänglich machen**, wenn wir ihm das erlaubt haben oder ein angemessener Datenschutz sichergestellt ist (z.B. bei Zugriffen aus Europa oder einem Land mit angemessenem Datenschutz, durch Einsatz der Musterklauseln der Europäischen Kommission oder durch BCR). ☐ Er muss **uns bei der Erfüllung unserer Pflichten** gemäss DSG **unterstützen**, so namentlich bei der Erfüllung der Betroffenenrechte, Datenschutzfolgenabschätzungen, Meldepflichten und Anfragen von Aufsichtsbehörden. ☐ Er muss uns unsere **Daten nach Beendigung des Auftrags grundsätzlich zurückgeben und von seinen Systemen löschen** (ohne eine Kopie zu behalten); darf er das aus gesetzlichen Gründen nicht tun, müssen die Datenschutzbestimmungen weiterhin gelten.	☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

☐ Um **überprüfen** zu können, ob der Auftragsbearbeiter die datenschutzrechtlichen Vorgaben, insbesondere die Datensicherheit, einhält, ist Folgendes vorgesehen:

- ☐ Wir dürfen **vor Ort Prüfungen durchführen** oder durchführen lassen und Einblick in die nötigen Unterlagen des Auftragsbearbeiters nehmen. → 3. **OK**
- ☐ Der Auftragsbearbeiter lässt seine Datensicherheit und ggf. weitere Aspekte von einem **anerkannten Dritten** mindestens jährlich überprüfen, und wir erhalten Einblick in die entsprechenden Testate. → 3. **OK**
- ☐ **Nichts**.
- ☐ Es ist anders:

☐ In unserem Vertrag haben wir zwar nicht alle vorstehenden Anforderungen abgedeckt, aber der Auftragsbearbeiter ist schon kraft **besonderer gesetzlicher Vorgaben** (z.B. Berufsgeheimnis) verpflichtet, diese einzuhalten, so dass wir unseres Erachtens keine besondere Regelung brauchen. → 2. und 3. **OK**

☐ Wir möchten noch Folgendes vermerken:

Q7

Vertrag (nur DSGVO)

Mit dem Auftragsbearbeiter besteht ein schriftlicher Vertrag, welcher die Vorgaben von Art. 28 DSGVO erfüllt. Der Vertrag muss folgende Punkte regeln:

- Vertragsgegenstand: Gegenstand der Auftragsverarbeitung
- Zweckbestimmung: Zwecke der Auftragsverarbeitung
- Festlegung der Daten: Art der personenbezogenen Daten, die verarbeitet werden
- Zeitbestimmung: Dauer der Auftragsverarbeitung
- Betroffene Personen: Kategorien von betroffenen Personen, deren Daten Gegenstand der Auftragsverarbeitung sind
- Weisungsgebundenheit: Der Auftragsverarbeiter darf nur auf dokumentierte Weisung des Verantwortlichen verarbeiten
- Informationspflicht: Der Auftragsverarbeiter muss den Verantwortlichen bei Ausnahmen von der Weisungspflicht aufgrund von Rechtsvorschriften unterrichten (wenn nicht die einschlägige Rechtsvorschrift eine solche Mitteilung verbietet)

Kurz und bündig:

☐ Die Datenschutzbestimmungen, die für die Auftragsbearbeitung gelten, wurden von Spezialisten überprüft und als im Einklang mit Art. 28 DSGVO erachtet. → **hier alles OK**

☐ Es kommt ein Vertrag über die Auftragsdatenverarbeitung gemäss dem Muster einer etablierten EU-Branchenorganisation oder einer EU-Datenschutzbehörde zum Einsatz. → **hier alles OK**

☐ Es gelten die Online-Service-Terms von Microsoft (OST Version September 2017 oder jünger) und die Datenbearbeitung weist keine besonderen Risikofaktoren auf, die allenfalls zu berücksichtigen wären. → **hier alles OK**

☐ Wir haben keine besonderen Datenschutzbestimmungen im Vertrag bzw. wir wissen nicht, ob diese den Anforderungen von Art. 28 DSGVO genügen.

Im Detail:

☐ Die Zusammenarbeit mit dem Auftragsbearbeiter ist vertraglich wie folgt geregelt:

- ☐ In einem **schriftlichen** Vertrag. → 1. **OK**
- ☐ In einem **online** abgeschlossenen Vertrag. → 1. **OK**
- ☐ Sie erfolgt auf Basis einer **Bestellung**, auf welche die allgemeinen Geschäftsbedingungen (**AGB**) des Dienstleisters Anwendung finden. Sie liegen uns vor. → 1. **OK**
- ☐ Sie erfolgt auf Basis einer **mündlichen Absprache**. Aber es finden die allgemeinen Geschäftsbedingungen (**AGB**) des Dienstleisters Anwendung. Sie liegen uns vor. → 1. **OK**
- ☐ Es gibt **keine spezifische vertragliche Regelung**, aber der Datenschutz ist geregelt (z.B. durch eine separate Konzernvereinbarung oder verbindliche Konzernrichtlinie). → 1. **OK**
- ☐ Es gibt **keine Regelung**. Der Provider kann im Grunde tun, was er will.

☐ Die Anforderung ist unseres Erachtens grundsätzlich **erfüllt** und es sind daher **keine Massnahmen nötig.**

☐ **Folgende Massnahmen** sollten ergriffen werden, damit die Anforderung erfüllt ist:

- ☐ Es sollten die Allgemeinen Geschäftsbedingungen des Auftragsbearbeiters (AGB) besorgt und geprüft werden. Sie liegen bis jetzt nicht vor.
- ☐ Es sollte ein Vertrag mit dem Auftragsbearbeiter abgeschlossen werden bzw. das Vertragsverhältnis sollte dokumentiert werden.
- ☐ Der Vertrag mit dem Auftragsbearbeiter sollte von einem Spezialisten auf seine Konformität mit der DSGVO überprüft werden.
- ☐ Der Vertrag entspricht nicht den Vorgaben der DSGVO. Dem Auftragsbearbeiter sollte ein Vertragszusatz gesendet werden, der die nötigen Regelungen enthält.
- ☐ Der Vertrag sollte in den folgenden Punkten nachgebessert werden:

- ☐ Andere:

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

• Vertraulichkeit: Gewährleistung des Auftragsverarbeiters, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen • Datensicherheit: Der Auftragsverarbeiter muss alle nach Art. 32 DSGVO vorgeschriebenen Massnahmen ergreifen • Unterauftragsverarbeiter: Auftragsverarbeiter darf keine weiteren Unterauftragsverarbeiter ohne vorherige gesonderte oder allgemeine Zustimmung des Verantwortlichen einsetzen; bei allgemeiner Zustimmung Informationspflicht des Auftragsverarbeiters über vorgesehene Änderung im Einzelfall und Einspruchsrecht des Verantwortlichen • Unterstützung bei der Einhaltung der DSGVO: Regelungen dazu, wie der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung seiner Pflichten in Bezug auf Betroffenenrechte nach Art. 12 bis Art. 22 DSGVO, der Datensicherheit, der Meldung von Verletzungen der Datensicherheit und Datenschutzfolgenabschätzungen unterstützt	☐ Es ist anders: ☐ Die Vereinbarung mit dem Auftragsbearbeiter **erfüllt <u>alle</u> folgenden Voraussetzungen**: → 2. **OK** ☐ Es geht aus dem Vertrag hervor, **was** genau der Auftragsbearbeiter tun soll und für **wie lange**, um welche Kategorien von Personendaten und betroffenen Person es geht. ☐ Der Vertrag sieht vor, dass die Daten nur auf **dokumentierte Weisung von uns** bearbeitet werden; diese Weisungen sind im Vertrag selbst festgehalten oder werden von uns erteilt. ☐ Der Auftragsbearbeiter darf die Daten nur **mit unserer Einwilligung** oder auf unsere Weisung hin **ausserhalb der EU zugänglich machen**. ☐ Der Auftragsbearbeiter muss uns **informieren**, falls er den **Vertrag** oder unsere Weisungen **nicht einhalten kann**, ausser das Gesetz untersagt dies. ☐ Der Auftragsbearbeiter muss verpflichtet sein, alle seine **Mitarbeiter** vertraglich zur **Geheimhaltung der Daten** zu verpflichten, falls sie dies nicht schon gesetzlich sind. ☐ Der Auftragsbearbeiter muss **angemessene technische und organisatorische Massnahmen** zur Datensicherheit treffen, aufrechterhalten und bei Bedarf verbessern; diese Massnahmen sind zu dokumentieren (z.B. in einem Anhang). ☐ Der Auftragsbearbeiter darf **Dritte**, jedenfalls wenn sie Zugang zu unseren Daten erhalten, nur beiziehen, wenn wir das **genehmigt haben** oder wir zumindest darüber in Kenntnis gesetzt werden müssen und ein Veto-Recht haben, und für diese Dritten mindestens gleich strenge Datenschutzbestimmungen gelten wie für den Auftragsbearbeiter.	☐ 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:

		• Rückgabe oder Löschung: Auftragsverarbeiter muss alle personenbezogenen Daten nach Erbringung der Verarbeitungsleistungen nach Wahl des Verantwortlichen löschen oder zurückgeben, sofern keine Rechtspflichten entgegenstehen • Nachweispflichten: Der Auftragsverarbeiter unterstützt den Verantwortlichen beim Nachweis der Einhaltung der Vorschriften zur Auftragsverarbeitung und stellt dem Verantwortlichen hierfür erforderliche Informationen zur Verfügung • Kontrollen: Der Auftragsverarbeiter ermöglicht und unterstützt Überprüfungen und Inspektionen bezüglich der Einhaltung der Vorgaben der DSGVO oder sonstiger Datenschutzbestimmungen der EU oder ihrer Mitgliedsstaaten • Unterrichtung bei Verstössen: Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder sonstige Datenschutzbestimmungen der EU oder ihrer Mitgliedsstaaten verstösst	☐ Der Auftragsbearbeiter ist verpflichtet, uns bei **der Einhaltung der Betroffenenrechte** wo nötig zu **unterstützen**. ☐ **Verletzungen der Datensicherheit** müssen uns **umgehend gemeldet** werden (spätestens jedoch so, dass wir unsere eigene Meldefrist von 72 h einhalten können). ☐ Der Auftragsbearbeiter ist verpflichtet, uns bei unseren **Datenschutzfolgenabschätzungen**, bei unserer eigenen **Datensicherheit** und bei unseren **Meldepflichten** im Falle von Datensicherheitsverstösse wo nötig zu **unterstützen**. ☐ Der Auftragsbearbeiter muss uns unsere **Daten** nach Beendigung des Auftrags grundsätzlich **zurückgeben und von seinen Systemen löschen** (ohne eine Kopie zu behalten); darf er das aus gesetzlichen Gründen nicht tun, müssen die Datenschutzbestimmungen weiterhin gelten. ☐ Um **überprüfen** zu können, ob der Auftragsbearbeiter die datenschutzrechtlichen Vorgaben, insbesondere die Datensicherheit, einhält, ist Folgendes vorgesehen: ☐ Wir dürfen **vor Ort Prüfungen durchführen** oder durchführen lassen und Einblick in die nötigen Unterlagen des Auftragsbearbeiters nehmen. → 3. **OK** ☐ Der Auftragsbearbeiter lässt seine Datensicherheit und ggf. weitere Aspekte von einem anerkannten **Dritten** mindestens jährlich **überprüfen**, und wir erhalten Einblick in die entsprechenden Testate. → 3. **OK** ☐ **Nichts**. ☐ Es ist anders: ☐ Wir haben die Vereinbarung **daraufhin geprüft**, ob sie auch **folgende Punkte** vorsehen sollte: → 4. **OK** ☐ Der Auftragsbearbeiter muss **uns umgehend sagen**, falls er der Meinung ist, eine **Weisung** von uns würde **EU-Recht verletzen**.	

Art. 28 DSGVO

Art. 28 DSGVO enthält klare Vorgaben, welche Punkte ein Vertrag mit einem Auftragsbearbeiter mindestens abzudecken hat. Der Vertrag hat schriftlich zu erfolgen, was allerdings nur bedeutet, dass er in Textform dokumentiert sein muss, d.h. auch elektronisch erfolgen kann. In der Praxis finden sich sehr ausführliche Verträge, welche die einzelnen Punkte von Art. 28 DSGVO ausdeutschen und mit Details versehen. Die meisten Verträge jedoch übernehmen mehr oder weniger den Wortlaut von Art. 28 DSGVO. Musterverträge gibt es von diversen Organisationen, aber "offizielle" Verträge wie im Falle der Standardklauseln der Europäischen Kommission bei grenzüberschreitenden Datenübermittlungen existieren bis jetzt nicht.

In der Praxis verwenden die meisten IT-Provider ihre eigenen Standardvertragsklauseln, um diesbezüglich über eine möglichst einheitliche Regelung über ihre gesamte Kundenbasis zu haben. Dies ist aus Kundensicht rechtlich nicht zu beanstanden, und in den meisten Fällen die einfachste Lösung. Wesentlich ist, dass die Punkte gemäss Art. 28 DSGVO abgedeckt sind. In vielen Fällen ist der Abschluss eines Vertrages nach DSGVO jedenfalls für Schweizer Unternehmen ohnehin ein reines Entgegenkommen gegenüber den Providern, da die Schweizer Unternehmen in vielen Fällen selbst der DSGVO gar nicht unterstehen, d.h. nur der Auftragsbearbeiter es tut und daher nur er gesetzlich verpflichtet ist, einen solchen Vertrag abzuschliessen. Aus Kundensicht sind solche Verträge jedoch regelmässig ein Vorteil, da die Vorgaben nach Art. 28 DSGVO ihre Rechtspositionen stärken und den Anforderungen des Schweizer Rechts genügen. Mit anderen Worten: Wer als Schweizer Unternehmen in der Rolle des Verantwortlichen einen Vertrag nach Art. 28 DSGVO abschliesst, hat damit auch seine diesbezüglichen Pflichten unter Schweizer Recht in aller Regel erfüllt.

- ☐ Werden wir von einem Dritten ins Recht gefasst, weil der Auftragsbearbeiter die datenschutzrechtlichen Vorgaben nicht einhält, muss er uns **schad- und klaglos halten**.
- ☐ Die **Kostenverteilung** für etwaige datenschutzrechtlich erforderliche Zusatzaktivitäten und Prüfungen ist angemessen geregelt.

☐ Wir möchten noch Folgendes vermerken:

		Aus kommerzieller Sicht ist jedoch darauf zu achten, welche über Art. 28 DSGVO hinausgehenden Bestimmungen der Vertrag mit dem Auftragsbearbeiter enthält. Besonderes Augenmerk ist auf die Regelungen der Kostentragung, der Garantien bzw. Gewährleistungen seitens des Kunden und der Einschränkung der Kundenrechte mit Bezug auf Instruktion und Veto gegen Subunternehmer zu richten. Drei Punkte seien hier besonders erwähnt: • Erstens wird das Instruktionsrecht in vielen Verträgen von Anbietern von standardisierten IT-Services so formuliert, dass der Kunde zwar ein Instruktionsrecht hat, aber gleichzeitig festgeschrieben wird, wie er es ausübt, nämlich indem die vertraglichen Vereinbarungen, die Leistungsumschreibungen und die Art und Weise, wie er die Services konfiguriert, zu den abschliessenden Weisungen erklärt werden (und daher nicht mehr bzw. nur noch im Rahmen der Konfigurationsmöglichkeiten bzw. Services geändert werden können). Diese Vorgehensweise ist unter der DSGVO zulässig. • Zweitens wird der Genehmigungsvorbehalt betr. Subunternehmer so formuliert, dass der Kunde dann, wenn ihm ein Subunternehmer nicht passt, im Grunde nur die Möglichkeit hat, den Service zu kündigen. Auch dies ist unter der DSGVO zulässig. In der Praxis dürften Widersprüche gegen Subunternehmer die absolute Ausnahme sein.		

		• Drittens schränken vor allem Anbieter von IT-Standardleistungen die Audit-Rechte des Kunden insofern ein, als dass sie keine Vor-Ort-Audits zulassen, um stattdessen im Namen aller Kunden von einem Dritten ein jährliches Audit durchführen lassen und diesen Kunden dann den entsprechenden Bericht bzw. Attest zur Verfügung stellen. Auch dies ist unter der DSGVO jedenfalls bei solchen Standarddienstleistungen normalerweise zulässig. Ausnahme sind Outsourcings, bei welchen das Aufsichtsrecht vorschreibt, dass auch die Behörde jederzeit eine Vor-Ort-Kontrolle durchführen können muss, wie dies z.B. in der Schweiz bei Finanzdienstleistern der Fall ist. In diesen Fällen räumen die Provider dieses Recht denn auch in aller Regel ein. Solche Vor-Ort-Kontrollen kommen aber in der Praxis kaum vor. Einige Auftragsbearbeiter werden vom Verantwortlichen schliesslich noch verlangen, dass er ihnen bestätigt, dass sie eine eigene Risikoeinschätzung vorgenommen haben und zum Ergebnis gekommen sind, dass die technischen und organisatorischen Massnahmen des Auftragsbearbeiters zur Datensicherheit angemessen sind. Eine solche Risikoeinschätzung ist in der Tat erforderlich (vgl. Q4), aber sie schriftlich festzuhalten ist nicht vorgeschrieben.		

Q8

Grenzüberschreitende Bekanntgabe

Gelangen im Rahmen der Auftragsbearbeitung Daten ins Ausland, so muss ein angemessener Datenschutz sichergestellt sein. Innerhalb von Europa und sicheren Drittstaaten (→ Glossar) geschieht dies durch die jeweilige lokale Datenschutzgesetzgebung. In den USA geschieht dies bei zertifizierten Unternehmen im Rahmen des "Privacy Shield". Bei allen anderen Unternehmen und in anderen Staaten ist normalerweise der Abschluss eines Datentransfervertrags nach dem Muster der Europäischen Kommission erforderlich.

Art. [13] f. DSG, Art. 44–49 DSGVO

Zu prüfen sind vorliegenden zwei Situationen: Die erste Situation ist der Transfer der Daten vom Verantwortlichen zum Auftragsbearbeiter. Befindet sich der Auftragsbearbeiter in einem unsicheren Drittstaat, sind hier Vorkehrungen zu treffen, wie z.B. der Abschluss der Standardklauseln der Europäischen Kommission.

Die zweite Situation ist der grenzüberschreitende Transfer innerhalb der Organisation des Auftragsbearbeiters, d.h. der Fall, in welchem der in Europa befindliche Provider die für den Kunden bearbeiteten Personendaten an eine Konzerngesellschaft oder sonstigen Subunternehmer in einem anderen Land weitergibt. Je nach Situation sind auch hier entsprechende Vorkehrungen zu treffen, die dann im Vertrag mit dem Verantwortlichen vorgesehen sein müssen.

Kurz und bündig:

- ☐ Der Auftragsbearbeiter ist in Europa und wird die Daten ausschliesslich in Europa bearbeiten bzw. bearbeiten lassen. → **hier alles OK**
- ☐ Der Auftragsbearbeiter ist in Europa und kann die Daten weltweit bearbeiten lassen, aber alle, die von ausserhalb eines sicheren Drittstaats darauf zugreifen, müssen die EU-Musterklauseln abschliessen. → **hier alles OK**
- ☐ Der Auftragsbearbeiter ist zwar nicht in einem sicheren Drittstaat, aber wir haben mit ihm einen Vertrag (auch) auf Basis der EU-Musterklauseln abgeschlossen. → **hier alles OK**
- ☐ Der Auftragsbearbeiter verfügt über eine gültige "Privacy Shield"-Zertifizierung für die hier relevanten Daten und ist vertraglich verpflichtet, sie aufrecht zu erhalten. → **hier alles OK**
- ☐ Es gelten die Online-Service-Terms von Microsoft (OST Version September 2017 oder jünger), einschliesslich den Bestimmungen für die DSGVO, und die Datenbearbeitung weist keine besonderen Risikofaktoren auf, die allenfalls zu berücksichtigen wären. → **hier alles OK**

Im Detail:

- ☐ Der Auftragsbearbeiter befindet sich in **Europa** oder einem **sicheren Drittstaat**. Er ist **verpflichtet**:
  - ☐ Die Daten **ausschliesslich in Europa** oder einem **sicheren Drittstaat** zu **bearbeiten** bzw. bearbeiten zu lassen und darf seinen Mitarbeitern und Subunternehmen im Ausland keinen Zugriff gestatten. → **hier alles OK**
  - ☐ Mit allen **Subunternehmern**, die von ausserhalb Europas oder sicherer Drittstaaten Zugang zu den Daten erhalten, vorgängig einen **Vertrag** auf Basis der EU-Musterklauseln abzuschliessen oder sie verpflichten, von einer EU-Behörde genehmigte "Processor BCR" einzuhalten. → **hier alles OK**
  - ☐ Der **Zugriff** auf unsere Daten aus dem Ausland durch den Auftragsbearbeiter und seine Subunternehmen ist **weder besonders geregelt noch eingeschränkt**.

- ☐ Die Anforderung ist unseres Erachtens grundsätzlich **erfüllt** und es sind daher **keine Massnahmen nötig.**
- ☐ **Folgende Massnahmen** sollten ergriffen werden, damit die Anforderung erfüllt ist:
  - ☐ Im Vertrag mit dem Auftragsbearbeiter ist vorzusehen, dass er unsere Daten nur im Inland bearbeiten darf (kein Export).
  - ☐ Im Vertrag mit dem Auftragsbearbeiter ist vorzusehen, dass er unsere Daten nur in Europa oder einem sicheren Drittstaat bearbeiten darf.
  - ☐ Wir sollten mit dem Auftragsbearbeiter die EU-Musterklauseln für Auftragsbearbeiter abschliessen.
  - ☐ Wir sollten den Auftragsbearbeiter verpflichten, die EU-Musterklauseln für Auftragsbearbeiter mit allen von ihm ausserhalb Europas oder einem sicheren Drittstaat beigezogenen Dritten abzuschliessen.
  - ☐ Wir sollten die mit dem Auftragsbearbeiter getroffene Regelung für die Bekanntgabe unserer Daten ins Ausland auf ihre Konformität mit dem DSG bzw. der DSGVO prüfen lassen.
  - ☐ Der Auftragsbearbeiter sollte mit seiner Datenbearbeitung für uns in das bestehende konzerninterne Datentransferabkommen (IGDTA) eingebunden werden.
  - ☐ Der Vertrag mit dem Auftragsbearbeiter sollte in den folgenden Punkten nachgebessert werden:

  - ☐ Andere:

☐ Der Auftragsbearbeiter befindet sich **weder in Europa noch einem sicheren Drittstaat**.

- ☐ Er befindet sich in den **USA**, hat eine gültige "Privacy Shield"-Zertifizierung und ist vertraglich verpflichtet, sie für die gesamte Vertragsdauer aufrecht zu erhalten. → **hier alles OK**
- ☐ In unserem Vertrag mit ihm schliessen wir, nebst anderem, die **EU-Musterklauseln für Auftragsbearbeiter** ab. → **hier alles OK**
- ☐ Es handelt sich um ein **Konzernunternehmen**, welches in eine konzernweite Regelung für gruppeninterne Datentransfers auf Basis der EU-Musterklauseln oder genehmigter BCR eingebunden ist. Die Regelung erfasst auch vorliegende Datenbearbeitung. → **hier alles OK**
- ☐ Wir haben **keine Regelung** betreffend die grenzüberschreitende Bekanntgabe von Personendaten.

☐ Es ist anders:

☐ 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:

Q9

Interaktion mit dem Auftragsbearbeiter

Es ist sichergestellt, dass dem Auftragsbearbeiter die nötigen Weisungen erteilt worden sind oder werden, damit dieser die Daten des Unternehmens nur so bearbeitet, wie es dies selbst auch tun dürfte. Es sind auch die Verantwortlichkeiten und Schnittstellen für die sonstige, zur Einhaltung des Datenschutzes erforderliche Interaktion definiert (Betroffenenrechte, Unter-Auftragsbearbeiter, Meldung von Verletzungen der Datensicherheit, andere Anforderungen).

Art. [8] Abs. 1 Bst. a DSG, Art. 28 DSGVO, Art. 33 Abs. 2 DSGVO

Es genügt nicht, nur einen Vertrag abzuschliessen, der die Rechte, Pflichten und Verantwortlichkeiten klärt. Er muss auch operativ umgesetzt werden, d.h. das Unternehmen muss sein Weisungsrecht entsprechend ausüben, soweit es das nicht bereits durch die Vorgaben im Vertrag getan hat. Es muss auch definiert werden, wie die beiden Beteiligten miteinander in den verschiedenen Situationen interagieren.

Zu berücksichtigen ist insbesondere, wie mit Anfragen von betroffenen Personen umgegangen wird, welche Angaben die beiden Parteien benötigen, um ihren Inventar-, Dokumentations- und Meldepflichten sowie der Pflicht zur Durchführung einer Datenschutzfolgenabschätzung nachkommen zu können. Besonders wichtig ist eine Klärung schliesslich im Bereich von Verletzungen der Datensicherheit, da ein Auftragsbearbeiter diese dem Verantwortlichen umgehend zu melden hat, damit er die nötigen Schritte unternehmen kann.

Kurz und bündig:

☐ Der Auftragsbearbeiter weiss genau, was er zu tun hat und von wem die Anweisungen kommen. Diese sind datenschutzkonform. Die datenschutzrechtlich erforderlichen Schnittstellen und Verantwortlichkeiten sind definiert. → **hier alles OK**

☐ Wir haben zwar einen Vertrag mit dem Auftragsbearbeiter, der die Anforderungen erfüllt. Die operative Umsetzung muss allerdings noch geklärt werden.

Im Detail:

☐ Wir können unser **Weisungsrecht** auf folgende Weise **umsetzen**:

- ☐ Wir haben eine **Online-Schnittstelle**, über welche wir die Dienstleistung und damit die Bearbeitung unserer Daten konfigurieren und steuern können, soweit sich diese nicht bereits aus dem Vertrag ergibt. → **1. OK**
- ☐ Wir haben entsprechende **Kontaktpersonen** auf Seiten des Auftragsbearbeiters. Diesen können wir unsere Wünsche mitteilen, soweit sich die vorzunehmenden Arbeiten nicht schon aus dem Vertrag ergeben. → **1. OK**
- ☐ Es ergibt sich alles Nötige bereits aus dem **Vertrag** und den ausgetauschten Unterlagen. → **1. OK**
- ☐ Dies **muss noch festgelegt werden**.

☐ Wir achten darauf, dass wir den Auftragsbearbeiter mit unseren Daten **nur Dinge machen lassen**, die nach unserer Ansicht **datenschutzkonform** sind. → **2. OK**

☐ Wir haben mit dem Auftragsbearbeiter **organisiert**, wie er uns **Verletzungen der Datensicherheit** in seinem Bereich **meldet** und es ist sichergestellt, dass wir darauf sofort reagieren können. → 3**. OK**

☐ Wir haben die **Genehmigung** neuer **Unter-Auftragsbearbeiter** organisiert:

- ☐ Er **meldet** uns solche und erbittet unsere **Genehmigung**. → 4**. OK**

☐ Die Anforderung ist unseres Erachtens grundsätzlich **erfüllt** und es sind daher **keine Massnahmen nötig**

☐ **Folgende Massnahmen** sollten ergriffen werden, damit die Anforderung erfüllt ist:

- ☐ Wir sollten klären, wie wir unser Weisungsrecht am besten operativ umsetzen, und dies implementieren.
- ☐ Wir sollten einen Prozess einführen um sicherzustellen, dass unsere Weisungen an den Auftragsbearbeiter datenschutzkonform sind.
- ☐ Wir sollten einen Prozess einführen bzw. die nötigen Verantwortlichkeiten festlegen um sicherzustellen, dass wir Meldungen zur Verletzung der Datensicherheit sofort bearbeiten können, um unseren eigenen Meldepflichten nachkommen zu können.
- ☐ Wir sollten festlegen, wie wir damit umgehen, wenn der Auftragsbearbeiter uns meldet, dass er einen neuen Unter-Auftragsbearbeiter beiziehen will.
- ☐ Wir sollten klären, wer seitens des Auftragsbearbeiters für etwaige datenschutzrechtliche Anliegen zuständig ist.
- ☐ Wir sollten auf unserer Seite eine Stelle festlegen, an welche sich der Auftragsbearbeiter bei datenschutzrechtlichen Anliegen hinwenden kann.
- ☐ Andere:

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

			☐ Er orientiert uns über **geplante** neue Unter-Auftragsbearbeiter und teilt uns mit, wo wir bei Bedarf **opponieren** können. → 4**. OK** ☐ Wir müssen **selbst nachfragen** bzw. auf einer Liste im Internet nachschauen, ob sich da was verändert. ☐ Wir haben mit dem Auftragsbearbeiter **organisiert**, wie wir vorgehen müssen, wenn wir seine **Unterstützung** für andere datenschutzrechtliche Belange benötigen: ☐ Er **stellt uns** für die meisten Belange (insb. Erfüllung von Betroffenenrechte) **online entsprechende Tools bereit**. Für alles andere haben wir eine Anlaufstelle definiert. → 5**. OK** ☐ Wir haben eine **Anlaufstelle** definiert, wo wir uns mit unseren Anliegen hinwenden können. → 5**. OK** ☐ Wir **wissen nicht**, wo wir uns mit unseren Anliegen hinwenden müssen. ☐ 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:
	Q10	**Prüfungen und Inspektionen** Das Unternehmen prüft regelmässig die Einhaltung der vertraglichen Vorgaben zum Datenschutz durch den Auftragsbearbeiter, so insbesondere die Vorgaben zur Datensicherheit. *Art. [8] Abs. 1 Bst. a und Abs. 2 DSG, Art. 28 DSGVO*	*Kurz und bündig:* ☐ Unsere Prüfer haben den Auftrag, auch diesen Auftragsbearbeiter im Rahmen ihrer Audits von Zeit zu Zeit auf die Einhaltung der vertraglichen Vorgaben, mindestens jedoch der Datensicherheit, zu prüfen. → **hier alles OK** ☐ Der Auftragsbearbeiter stellt uns mindestens ein Mal im Jahr einen unabhängigen Prüfbericht bezüglich der Einhaltung der Datensicherheit vor bzw. verfügt über aktuelle Prüftestate nach ISO 27001. → **hier alles OK**	☐ Die Anforderung ist unseres Erachtens grundsätzlich **erfüllt** und es sind daher **keine Massnahmen nötig.** ☐ **Folgende Massnahmen** sollten ergriffen werden, damit die Anforderung erfüllt ist: ☐ Wir sollten uns die Prüftestate des Auftragsbearbeiters mindestens ein Mal im Jahr ansehen und schauen, ob er die Voraussetzungen noch erfüllt. ☐ Wir sollten unsere Prüfer bitten, von Zeit zu Zeit auch diesen Auftragsbearbeiter unter die Lupe zu nehmen. ☐ Wir sollten einen Prüfplan für diesen Auftragsbearbeiter ausarbeiten und implementieren.

Der Verantwortliche muss sich auf die eine oder andere Weise Gewissheit darüber schaffen, dass die vertraglichen Vorgaben eingehalten werden. Klassischerweise geschieht dies durch ein Audit bzw. eine Prüfung vor Ort. Dies ist aber mit viel Aufwand verbunden, und manche Auftragsbearbeiter lassen es nicht zu, weil es den Betrieb stören würde, wenn jeder Kunde sich vor Ort vergewissern möchte, ob alles richtig läuft. Abgesehen davon kann bei einer Vor-Ort-Kontrolle in einem Rechenzentrum ausser den Sicherheitsvorkehrungen nichts geprüft werden. In der Praxis kommen Audits von Auftragsbearbeitern daher kaum vor, auch bei grossen Unternehmen nicht.

Eine verbreitete Alternative zur Prüfung durch den Verantwortlichen ist die Prüfung durch einen spezialisierten Dritten, der zwar im Auftrag des Auftragsbearbeiters tätig wird, aber seine Prüfung unabhängig zu Händen der Kunden durchführt. Häufig sind diese Prüfungen auf die Einhaltung der Vorgaben der Datensicherheit fokussiert, was allerdings in der Praxis auch am wichtigsten ist. Die Kunden eines solchen Providers können dann die entsprechenden Prüfberichte bzw. Testate bei Bedarf einsehen. Aus rechtlicher Sicht wird dies in vielen Fällen genügen.

Ohnehin ist auch hier eine risikobasierte Vorgehensweise angezeigt: Wie weit ein Unternehmen gehen muss, hängt davon ab, wie heikel die Datenbearbeitung ist (aus Sicht der betroffenen Personen) und welchen Ruf der Auftragsbearbeiter hat; gilt er als zuverlässig, setzen ihn andere Unternehmen mit einem datenschutzrechtlich guten Ruf ein, so wird sich ein Unternehmen womöglich zurecht nicht veranlasst sehen, selbst ebenfalls eine Prüfung vorzunehmen.

In der einfachsten Form kann die Aufsichtspflicht damit erfüllt werden, dass der Kunde seinen Provider aufmerksam beobachtet, verfolgt, ob es Hinweise auf ein vertragswidriges Verhalten gibt und bei Bedarf dies weiter nachforscht bzw. interveniert und nötigenfalls kündet.

☐ Wir überprüfen nicht, ob der Auftragsbearbeiter sich an die Vorgaben der Datensicherheit hält. Der Auftragsbearbeiter hat diesbezüglich aber einen guten Ruf, wird von vielen Unternehmen in Anspruch genommen und besonderes sensitiv sind unsere Daten nicht. → **hier alles OK**

☐ Wir überprüfen nicht, ob der Auftragsbearbeiter sich an die Vorgaben der Datensicherheit hält.

Im Detail:

☐ Wir **prüfen nicht**, ob unser Auftragsbearbeiter die **Datensicherheit einhält**:

- ☐ Weil die von ihm bearbeiteten **Daten nicht sensitiv** sind. Es würde nichts oder nicht viel ausmachen, wenn sie in fremde Hände gelangen würden. → **1. OK**
- ☐ Weil der Auftragsbearbeiter einen **guten Ruf** hat, von vielen Unternehmen für diese Leistungen ebenfalls in Anspruch genommen wird und unsere Daten nicht besonders sensitiv sind. → **1. OK**
- ☐ Weil es sich um eine **Konzerngesellschaft** handelt, die bereits vom Konzern auf die Einhaltung der Datensicherheit geprüft wird. Wir haben Einsicht in diese Unterlagen. → **1. OK**
- ☐ Weil wir dafür **kein Fachwissen** haben.
- ☐ Weil wir dafür **keine Ressourcen** haben.
- ☐ Weil wir uns **nicht damit auseinandergesetzt** haben.

☐ Wir **prüfen**, ob unser Auftragsbearbeiter die **Datensicherheit einhält**:

- ☐ Indem wir **von Zeit zu Zeit kontrollieren**, ob er über aktuelle Prüftestate nach ISO 27001 oder andere Unterlagen von unabhängigen Prüfern verfügt, die die Einhaltung der Vorgaben bestätigen. Diese liegen uns jederzeit vor. → **1. OK**
- ☐ Indem wir **von Zeit zu Zeit eigene Kontrollen durchführen** bzw. durchführen lassen, einschliesslich Vor-Ort-Kontrollen, wenn dies als angemessen erscheint. → **1. OK**

- ☐ Wir sollten prüfen, ob eine eingehendere, regelmässige Prüfung der Einhaltung der vertraglichen Vorgaben durch diesen Auftragsbearbeiter angezeigt ist.
- ☐ Wir sollten herausfinden, was dieser Auftragsbearbeiter tut um zu belegen, dass er die Datensicherheit und ggf. weiteren Vorgaben einhält.
- ☐ Wir sollten jemanden definieren, der dafür verantwortlich ist, beim Verdacht auf die Nichteinhaltung der nötigen Datensicherheit durch den Auftragsbearbeiter zu reagieren.
- ☐ Andere:

  [ ]

- ☐ 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.

			☐ Indem wir **jährlich eigene Kontrollen durchführen** bzw. durchführen lassen, einschliesslich Vor-Ort-Kontrollen, wenn dies als angemessen erscheint. → **1. OK** ☐ **Kommt uns zu Ohren**, dass der Auftragsbearbeiter sich möglicherweise nicht an die vertraglichen Vorgaben hält, gehen wir dem entsprechend nach und erwägen, ob unserseits weitere Schritte nötig sind. Das kann bis zur Kündigung der Zusammenarbeit führen. → **2. OK** ☐ Wir möchten noch Folgendes vermerken:	☐ Treffen wir folgende Sofortmassnahmen: ☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:
	Q11	*Falls anwendbar:* **Vorgaben des Rundschreibens 2018|3 "Outsourcing – Banken und Versicherer" der FINMA (FINMA RS Oursourcing)** Das Unternehmen hält mit der Auslagerung die Vorgaben des FINMA RS Outsourcing ein, darunter insbesondere jene in Bezug auf Auswahl, Überwachung und Instruktion des Auftragsbearbeiters, die Sicherheit der Auslagerung, die Fortführung der ausgelagerten Funktion und die Gewährleistung der Aufsicht durch die FINMA. Es besteht ein schriftlicher Vertrag mit dem Auftragsbearbeiter, der alle Vorgaben des FINMA RS Outsourcing erfüllt.	*Kurz und bündig:* ☐ Die Einhaltung der Vorgaben des FINMA RS Outsourcing wurden separat geprüft und dokumentiert, weshalb wir hier nicht darauf eingehen. → **hier alles OK** ☐ Wir haben geprüft, ob wir die Vorgaben des FINMA RS Outsourcing im konkreten Fall einhalten und sind zum Schluss gelangt, dass dies der Fall ist. Die Auslagerung ist unter dem FINMA RS Outsourcing grundsätzlich zulässig bzw. eine allfällige Bewilligung der FINMA liegt vor. Die Auslagerung wurde intern im dafür vorgesehenen Verfahren bewilligt. Wir haben die ausgelagerte Funktion klar definiert und inventarisiert, den Auftragsbearbeiter sorgfältig ausgewählt und überwachen und instruieren ihn entsprechend. Er bietet Gewähr für eine geordnete Rückführung der ausgelagerten Funktion und ist in unser internes Kontrollsystem eingebunden. All das ist dokumentiert. Ebenso liegt ein Sicherheitsdispositiv vor, das die Weiterführung der ausgelagerten Funktion in Notfällen erlaubt. Es besteht ein schriftlicher Vertrag, der alle erforderlichen Punkte abdeckt, insbesondere auch Auskunfts-, Einsichts- und Prüfrechte zugunsten der FINMA und unserer Prüfgesellschaft. → **hier alles OK** ☐ Wir prüfen nicht, ob die Auslagerung die Vorgaben des FINMA RS Outsourcing erfüllt oder wissen, dass es nicht der Fall ist.	☐ Die Anforderung ist unseres Erachtens grundsätzlich **erfüllt** und es sind daher **keine Massnahmen nötig.** ☐ **Folgende Massnahmen** sollten ergriffen werden, damit die Anforderung erfüllt ist: ☐ Wir sollten eine Genehmigung der FINMA einholen. ☐ Wir sollten die folgenden Funktionen von der Auslagerung ausnehmen: ☐ Wir sollten ein Inventar erstellen bzw. das vorhandene Inventar aktualisieren. ☐ Wir sollten sicherstellen, dass die Ziele und Anforderungen an die Leistungserbringung festgelegt und dokumentiert sind. ☐ Der Auftragsbearbeiter sollte auf seine Eignung überprüft werden bzw. die bereits erfolgte Überprüfung sollte vertieft und dokumentiert werden. ☐ Wir sollten eine Risikoanalyse durchführen, um zu prüfen, ob die mit der Auslagerung verbundenen Risiken angemessen abgedeckt sind, und diese Analyse dokumentieren.

			Das Outsourcing-Rundschreiben der FINMA beschreibt, welche Anforderungen die FINMA an ein wesentliches Outsourcing bei den von ihr regulierten Finanzmarktunternehmen stellt. Erfasst sind somit nicht alle Outsourcings, sondern nur solche, die wesentlich sind, was das Rundschreiben wiederum für Banken und Versicherungen unterschiedlich definiert (ursprünglich galt das Outsourcing-Rundschreiben nur für die Banken). Soweit es sich um eine Versicherung handelt, genügt die Einhaltung des Rundschreibens nicht. Erforderlich ist auch die Genehmigung durch die FINMA, soweit die Auslagerung den Geschäftsplan der Versicherung tangiert. Auf diesen Punkt wird hier nicht näher eingegangen; nebst allgemeinen Kriterien ist hier eine individuelle Betrachtung erforderlich und in der Praxis häufig auch eine Abstimmung mit der FINMA selbst. In der mittleren Spalte werden die Anforderungen aus dem Rundschreiben abgefragt, auch wenn sie sich teilweise mit den Punkten, die anderswo in diesem Formular erhoben werden, bereits abgedeckt sind.	*Im Detail:* ☐ Die **Zustimmung der FINMA** zur Auslagerung: ☐ ist **nicht erforderlich**, denn wir sind eine Bank und|oder ein Effektenhändler, aber kein Versicherungsunternehmen. → **1. OK** ☐ ist **erforderlich**, da wir ein Versicherungsunternehmen sind, die Auslagerung geschäftsplanrelevant und deshalb genehmigungspflichtig ist; die Zustimmung ☐ **liegt vor** → **1. OK** ☐ **liegt noch nicht vor**, aber dies **wird geschehen**, bevor der Vertrag umgesetzt wird; der Vertrag enthält einen Vorbehalt → **1. OK** ☐ liegt **nicht** vor und der Vertrag enthält auch keinen Vorbehalt. ☐ Die Auftragsbearbeitung betrifft **keine der gemäss** FINMA RS Outsourcing auslagerbaren Funktionen, **insbesondere geht es nicht um**: → **2. OK** ☐ Oberleitung, Aufsicht und Kontrolle durch das Oberleitungsorgan. ☐ Zentrale Führungsaufgaben der Geschäftsleitung. ☐ Funktionen, die das Fällen strategischer Entscheide umfassen. ☐ Entscheide, über die Aufnahme und den Abbruch von Geschäftsbeziehungen. ☐ bei Unternehmen der Aufsichtskategorie 1 bis 3: Risikomanagement und Compliance-Funktion (davon ausgenommen: operative Aufgaben im Bereich Risikomanagement und Compliance). ☐ Wir verfügen über ein **aktuelles Inventar** der ausgelagerten Funktion, das die ausgelagerte Funktion umschreibt, Auftragsbearbeiter (inkl. ggf. Subunternehmer, die eine wesentliche Funktion erfüllen) und Empfänger sowie die bei uns verantwortliche Stelle nennt. → **3. OK** ☐ Wir haben **vor dem Vertragsabschluss** die Vorgaben des FINMA RS Outsourcing eingehalten, d.h. insbesondere: → **4. OK**	☐ Wir sollten einen Prozess für die interne Bewilligung von Auslagerungen und die Zuständigkeit für Vertragsabschlüsse definieren. ☐ Es sollte sichergestellt werden, dass das Unternehmen bezüglich der ausgelagerten Funktion den Auftragsbearbeiter vernünftig wechseln kann und bei einem Ausfall geschützt ist. ☐ Das Sicherheitsdispositiv sollte überprüft werden. ☐ Wir sollten die folgenden Punkte im Sicherheitsdispositiv ergänzen bzw. anders regeln: ☐ Wir sollten prüfen, ob der Vertrag mit dem Auftragsbearbeiter die Vorgaben des FINMA RS Outsourcing erfüllt. ☐ Wir sollten die folgenden Punkte im Vertrag ergänzen bzw. anders regeln: ☐ Wir sollten prüfen und sicherstellen, dass die Aufsicht durch die FINMA nicht aufgrund der Auslagerung erschwert wird. ☐ Wir sollten die folgenden Massnahmen umsetzen, um die Aufsichtsrechte durch die FINMA zu gewährleisten: ☐ Wir sollten prüfen und sicherstellen, dass die Sanierbarkeit bzw. Abwickelbarkeit und der Zugriff auf die dafür notwendigen Informationen in der Schweiz jederzeit gewährleisten ist.

☐ die **Ziele und Anforderungen** an die Leistungserbringung festgelegt und dokumentiert und eine **Risikoanalyse** durchgeführt. → **4. OK**

☐ den Auftragsbearbeiter **sorgfältig ausgewählt**, unter Berücksichtigung seiner Fähigkeiten und Ressourcen, eines allfälligen Konzentrationsrisikos (bei Auslagerung mehrerer Funktionen an denselben Auftragsbearbeiter) sowie der Möglichkeiten und Folgen eines Wechsels des Anbieters. → **4. OK**

☐ Es geht um eine **konzern- bzw. gruppeninterne** Auslagerung. Wir kennen den Auftragsbearbeiter und wissen bereits, dass dieser in der Lage ist, die ausgelagerte Funktion qualitativ gut und ohne relevante Zusatzrisiken zu erbringen. → **4. OK**

☐ Wir verfügen über ein **internes Bewilligungsverfahren** für Outsourcing-Projekte und haben die Zuständigkeiten für Vertragsabschlüsse festgelegt.

☐ Das Verfahren **wurde erfolgreich** durchlaufen. → **5. OK**

☐ Das Verfahren **muss erfolgreich** durchlaufen werden, bevor der Vertrag unterzeichnet bzw. umgesetzt wird. → **5. OK**

☐ Wir durchlaufen dieses Verfahren **nicht.**.

☐ Der Auftragsbearbeiter bietet **Gewähr für eine geordnete Rückführung** der ausgelagerten Funktion. Das ist sichergestellt durch: → **6. OK**

☐ entsprechenden Vertragspflichten.

☐ folgende praktischen Vorkehrungen:

☐ Wir sollten durch folgende Massnahmen sicherstellen, um die Sanierbarkeit bzw. Abwickelbarkeit und den Zugriff auf die dafür notwendigen Informationen in der Schweiz jederzeit zu gewährleisten:

☐ Speicherung der dafür nötigen Daten in der Schweiz.

☐ Andere:

☐ 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:

				☐ Die ausgelagerte Funktion ist in das **interne Kontrollsystem** integriert und die mit der Auslagerung verbundenen **Risiken** werden systematisch **identifiziert, überwacht, quantifiziert und gesteuert**. Wir haben eine **verantwortliche Stelle definiert**, die für die Überwachung und Kontrolle des Auftragsbearbeiters zuständig ist und wir überwachen und beurteilen die Leistungen des Auftragsbearbeiters fortlaufend. → **7. OK** ☐ Wir haben mit dem Auftragsbearbeiter ein **Sicherheitsdispositiv** erarbeitet, das die Weiterführung der ausgelagerten Funktion in Notfällen erlaubt. → **8. OK** ☐ Mit dem Auftragsbearbeiter besteht ein **schriftlicher Vertrag**, der **alle** der folgenden Punkte regelt: → **9. OK** ☐ Bezeichnung der Parteien; ☐ Beschreibung der ausgelagerten Funktion; ☐ Festlegung und Abgrenzung der Zuständigkeiten; ☐ Weisungs- und Kontrollrechte; ☐ Sicherheitsanforderungen; ☐ Verpflichtung, die für die Führung des Inventars notwendigen Informationen zu liefern; ☐ Genehmigungspflicht für Subunternehmer, die wesentliche Funktionen erbringen, und Überbindung der Pflichten und Zusicherungen des Auftragsbearbeiters, soweit diese zur Erfüllung des FINMA RS Outsourcing erforderlich sind; ☐ Jederzeitiges, vollumfängliches und ungehindertes Einsichts- und Prüfrecht in Bezug auf die ausgelagerte Funktion zu Gunsten von uns, unserer Prüfgesellschaft und der FINMA; ☐ Verpflichtung des Auftragsbearbeiters gegenüber der FINMA, der FINMA sämtliche Auskünfte und Unterlagen bezogen auf die ausgelagerte Funktion zur Verfügung zu stellen, die die FINMA für die Aufsichtstätigkeit benötigt;	☐ Sollten wir die Datenbearbeitung wie folgt einschränken/stoppen:

				☐ Sofern Prüftätigkeiten an die Revisionsstelle des Auftragsbearbeiters delegiert werden: Verpflichtung, den Bericht der Revisionsstelle des Auftragsbearbeiters unserer internen Revision, unserer Prüfstelle und der FINMA auf Anfrage zur Verfügung zu stellen. ☐ Wir sind zur Auffassung gelangt, dass die Auslagerung der Funktion die **Aufsicht durch die FINMA nicht erschwert**. → **10. OK** ☐ Bei einer Auslagerung ins **Ausland** (wenn nicht: → **11. + 12. OK**): ☐ Wir können ausdrücklich zusichern, dass wir, unsere Prüfgesellschaft und die FINMA die **Einsichts- und Prüfrechte** wahrnehmen und durchsetzen können; → **11. OK** ☐ Die **Sanierbarkeit bzw. Abwickelbarkeit** in der Schweiz bleibt jederzeit gewährleistet und der **Zugriff auf die dafür notwendigen Informationen** ist in der Schweiz jederzeit möglich. → **12. OK** ☐ Wir möchten noch Folgendes vermerken:	