Compliance Check IV – Datenschutz-Folgenabschätzung (für Verantwortliche) Formular G.1

Unternehmenseinheit: _____ Ausgefüllt von: _____ Stand vom: _____

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

Beilagen: _____

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

Dieses Formular wird durchgeführt:

☐ Zum ersten Mal (d.h. vorgängig)

☐ Als Wiederholung, weil:

- ☐ Seit dem letzten Mal drei oder mehr Jahre vergangen sind (Datum der letzten Datenschutz-Folgenabschätzung: _____)
- ☐ Weil sich die Datenbearbeitung oder die Verhältnisse wesentlich verändert haben: _____
- ☐ Weil es verlangt oder sonst erforderlich wurde: _____

☐ Lediglich zur Dokumentation, dass keine Datenschutz-Folgenabschätzung erforderlich ist (→ Abschnitt A).

Weiterführende Angaben zur Durchführung dieser Datenschutz-Folgenabschätzung 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 dieser Datenschutz-Folgenabschätzung tragen:

☐ Ich/wir

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

Arbeitsanweisung:

- Dieses Formular dient dazu zu beurteilen, ob eine Datenschutz-Folgenabschätzung (**DSFA**) (→ Glossar) nach revidiertem DSG und DSG-VO erforderlich ist, und diese, falls nötig, durchzuführen. Die grundsätzlichen Bemerkungen von Formular E.1 zur Methodik gelten auch hier.

- Im ersten Teil des Formulars (Abschnitt A) wird geprüft, ob eine DSFA erforderlich ist. Hierzu müssen Fragen beantwortet werden, anhand welcher ermittelt wird, ob **wahrscheinlich ein "hohes" Risiko** für die betroffenen Personen vorliegt. Ist dies der Fall, verlangt das Gesetz grundsätzlich eine DSFA, es sei denn, eine der Ausnahmen greift. Ebenso ist eine DSFA für bestimmte Fälle standardmässig durchzuführen, wenn eine DSGVO-Aufsichtsbehörde dies verlangt. Ist keine DSFA erforderlich, dient das Formular zur Dokumentation, warum keine nötig ist. In diesem Fall ist das betreffende Feld auf Seite 1 anzukreuzen und das Formular aufzubewahren. Eine DSFA sollte grundsätzlich **alle drei Jahre wiederholt** werden, oder wenn es zu **wesentlichen Änderungen** an der Datenbearbeitung kommt.

- Im zweiten Teil des Formulars (Abschnitt B) findet die DSFA statt. Im ersten Punkt (Q5) wird eine **Beschreibung der Datenbearbeitung** verlangt. Hierbei kann teilweise auf Formular B.2 zurückgegriffen werden, aber die dortigen Angaben genügen nicht. Insbesondere muss näher beschrieben werden, wie die Bearbeitung funktioniert. Es kann dabei auch auf Beilagen verwiesen werden.

- Als nächster Schritt muss geprüft werden, ob die **datenschutzrechtlichen Anforderungen** erfüllt sind. Hierzu gibt es zwei Optionen: **Option 1** (Q6) setzt im Wesentlichen auf eine separate Prüfung (z.B. mit dem Formular E.1) und separate Dokumentation der Massnahmen (z.B. in einem Datenschutzkonzept). Für einfachere Fälle erlaubt **Option 2** (Q7) eine Prüfung der Konformität direkt in diesem Formular, auch wenn zum Schluss ebenfalls auf Formular E.1 verwiesen wird. Anders als die Compliance-Prüfung in Formular E.1 ist es für eine DSFA wichtig, dass sie auch die zur Sicherstellung des Datenschutzes und Schutz der betroffenen Personen getroffenen Massnahmen umschreibt. Mit Option 2 geschieht dies in rudimentärer Weise direkt in Q7; sie ist für einfachere Vorhaben geeignet.

- In der Folge müssen in Q8 die **Restrisiken für die betroffenen Personen** beurteilt werden, d.h. es muss ermittelt werden, in welchen Fällen die Datenbearbeitung für die betroffenen Personen noch Nachteile mit sich bringen kann, obwohl Massnahmen zum Datenschutz (wie in Q6 und Q7 dokumentiert) getroffen wurden. Sind solche Fälle definiert, muss beurteilt werden, ob in einem dieser Fälle die Nachteile für die betroffenen Personen so gewichtig und so wahrscheinlich sind, dass sie als "hohes Risiko" gelten.

- Liegt ungeachtet aller Massnahmen noch immer ein hohes Risiko vor, so muss die **Datenschutzbehörde konsultiert** werden, damit diese ggf. einschreiten kann. Die DSGVO schreibt noch **weitere Konsultationspflichten** vor (beim Datenschutzbeauftragten und bei den betroffenen Personen), die ebenfalls über das Formular dokumentiert werden können. Es kann darin auch dokumentiert werden, wenn das Unternehmen sich entscheidet, Empfehlungen nicht umzusetzen. Eine DSFA wird immer **vom Unternehmen selbst** in eigener Verantwortung gemacht; der Datenschutzbeauftragte berät bloss. Am Ende des Formulars kann das Unternehmen bzw. der Prozessowner seine **Gesamtbeurteilung** und weiteren Schritte festhalten, die Datenschutzstelle ebenso ihre Stellungnahme dazu.

A. Prüfung der Erforderlichkeit einer DSFA

	Anforderung	Anforderung erfüllt?	Was zu tun ist
Q1	**Erforderlichkeit einer DSFA I** Eine DSFA ist erforderlich, wenn eine Datenbearbeitung ein voraussichtlich ein hohes Risiko mit sich bringt für eine der Personen, über die Personendaten bearbeitet werden. Ein hohes Risiko kann sich aus Art, Umfang, Umständen und Zweck der Bearbeitung ergeben. *Art. [20] Abs. 1 DSG, Art. 35 Abs. 1, 3, und 5 DSGVO* Der Gesetzgeber hat drei Fälle definiert, in denen auf jeden Fall von einem hohen Risiko auszugehen ist. Diese drei Fälle sind aber nicht abschliessend. Es ist daher zu prüfen, ob die Datenbearbeitung für die betroffene Person ein hohes Risiko darstellt, auch wenn keiner der drei Fälle vorliegt. Mit einem Risiko ist die Wahrscheinlichkeit von negativen Folgen aufgrund der Bearbeitung der Daten der betroffenen Person gemeint, sei es in Form von gewollten Folgen (z.B. eines Entscheids aufgrund der Bearbeitung der Daten), oder ungewollten Folgen (z.B. wegen eines Missbrauchs der Daten). Wie hoch ein Risiko ist, wird allgemein anhand der Wahrscheinlichkeit und der Höhe eines Schadens bzw. negativer Folgen wie folgt beurteilt:	*Kurz und bündig:* ☐ Die Datenbearbeitung ist irgendwie heikel. → **voraussichtlich hohes Risiko** ☐ Die Datenbearbeitung ist in keiner Hinsicht heikel, völlig alltäglich und es ist nicht ersichtlich, dass sie negative Folgen für die betroffenen Personen haben könnte. Es findet keinerlei Profilbildung oder sonstige Beurteilung der Personen statt und die Bearbeitung der Daten ist letztlich sehr beschränkt. *Im Detail:* ☐ Es liegt **einer der Fälle** vor, in welchem der **Gesetzgeber** von einem voraussichtlich hohen Risiko ausgeht (*Kriterien gemäss Gesetz*): → **voraussichtlich hohes Risiko** ☐ Es erfolgt eine **umfangreiche Bearbeitung** von: ☐ **Besonders schützenswerten Personendaten** nach DSG (→ Glossar). ☐ **Besonderen Kategorien von Personendaten** nach DSGVO (→ Glossar). ☐ Daten über **strafrechtliche Verurteilungen** und Straftaten oder damit zusammenhängende Sicherungsmassregeln nach DSGVO (→ Glossar). ☐ **Öffentliche Bereiche** werden **systematisch** und **umfangreich überwacht** (z.B. durch Videokameras, die nicht nur einen Eingang oder Aufzug filmen; auch private, aber öffentlich zugängliche Räume wie z.B. in Kaufhäusern, Restaurants oder Tiefgaragen sind erfasst; erfasst ist auch, wenn aufgezeichnet wird, wer einen öffentlichen Bereich benutzt). ☐ Es findet ein **automatisierter Einzelfallentscheid** im Sinne der DSGVO oder des DSG statt (→ Q25 [DSG] und Q26 [DSGVO] in Formular E.1), dem eine **systematische und umfassende Bewertung** persönlicher Aspekte durch einen Computer zugrunde liegt.	☐ Es gibt unseres Erachtens mindestens einen Grund, von einem **voraussichtlich hohen Risiko** für die betroffenen Personen auszugehen. Eine **DSFA** ist daher **erforderlich**. → Q3 bzw. Q4 (Prüfung der Ausnahmen) ☐ Ob tatsächlich ein voraussichtlich hohes Risiko für die betroffenen Personen vorliegt, ist unseres Erachtens zwar **nicht klar**. Wir erachten eine **DSFA** aber dennoch für **angezeigt**. ☐ Unsere internen Regelungen schreiben eine solche für den vorliegenden Fall vor. → Q3 bzw. Q4 (Prüfung der Ausnahmen) ☐ Die Datenbearbeitung birgt unseres Erachtens voraussichtlich **kein hohes Risiko** für die betroffenen Personen. Es ist daher **keine DSFA** erforderlich oder angezeigt. → Q2 (Prüfung der Erforderlichkeit II; nur DSGVO) ☐ Andere Einschätzung: ☐ **Situation unklar** Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren

Wahrscheinlich	Mittleres Risiko	Hohes Risiko	Hohes Risiko
Möglicherweise	Tiefes Risiko	Mittleres Risiko	Hohes Risiko
Unwahrscheinlich	Tiefes Risiko	Tiefes Risiko	Mittleres Risiko
	Spürbare Nachteile	Gewichtige Nachteile	Bedrohliche Nachteile

Die EU-Datenschutzbehören (WP29) haben zur Beurteilung der Frage, ob ein hohes Risiko vorliegt, in ihrer Empfehlung WP248 einen Katalog von Risikofaktoren ausgearbeitet. Als Faustregel gilt, dass wenn zwei oder mehr der Risikofaktoren vorliegen, eine DSFA durchgeführt werden sollte. Auf diesen Katalog wird hier ebenfalls abgestellt, auch für die Zwecke des DSG, da die Kriterien unter dem DSG vergleichbar sind.

Zu beachten ist, dass zwischen einem voraussichtlich hohen Risiko und einem tatsächlich hohen Risiko zu unterscheiden ist. Die Eingangsfrage ist lediglich, ob mit einer gewissen Wahrscheinlichkeit ein hohes Risiko eines Nachteils für eine betroffene Person besteht. Ob es wirklich besteht, und zwar unter Berücksichtigung aller Massnahmen, um die Gefahren für die betroffenen Personen einzudämmen, ist eine andere, in der DSFA selbst zu prüfende Frage.

Nur falls DSG anwendbar:

☐ Es findet ein **Profiling** nach DSG (→ Glossar) statt, auch ohne, dass es einem Entscheid dient, der rechtliche Folgen oder sonstige Nachteile für die betroffene Person haben kann.

☐ Es liegen **mindestens <u>zwei</u> der folgenden Risikofaktoren vor**, die auf ein voraussichtlich hohes Risiko für die betroffene Person hinweisen (*Kriterien gemäss WP29*): **→ voraussichtlich hohes Risiko**

☐ Betroffene Personen werden im Rahmen der Datenbearbeitung **bezüglich persönlicher Aspekte irgendwie bewertet**, eingestuft oder einem Scoring, einer Prognose oder einem Profiling im Sinne der DSGVO (→ Glossar) unterzogen (z.B. mit Bonitätscodes, als Betrugsverdachtsfälle, zwecks Beurteilung des Risikos der Geldwäsche oder Terrorfinanzierung, zur Einschätzung von Gesundheitsrisiken, in Form von Verhaltens- und Marketingprofilen von Website-Nutzern).

☐ Es finden **automatisierte Einzelfallentscheide** im Sine der DSGVO oder des DSG statt (→ Q25 [DSG] und Q26 [DSG-VO] in Formular E.1).

☐ Betroffene Personen werden **systematisch** und **umfangreich überwacht**, nachverfolgt oder ihr Verhalten wird sonst in einem bestimmten Bereich aufgezeichnet oder ausgewertet (z.B. mittels Kameras, Zugangskontrollen, Bewegungsdaten, permanenten Cookies auf Websites, Überwachung am Arbeitsplatz, laufende oder fallbezogene Auswertung von E-Mails, Überwachung des Netzwerksverkehrs zu Sicherheitszwecken)

☐ Es werden **vertrauliche** oder **höchst persönliche Daten** bearbeitet, einschliesslich (aber nicht nur) besondere Kategorien von Personendaten nach DSGVO (→ Glossar), besonders schützenswerte Personendaten nach DSG (→ Glossar) und Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmassregeln nach DSGVO (→ Glossar). Als vertraulich bzw. höchstpersönlich gelten alle Daten, bei denen angenommen werden muss, dass die betroffenen Personen sie nicht allgemein zugänglich machen möchten (z.B. persönliche Dokumente, E-Mails, private Fotos, Lifelogging-Anwendungen, finanzielle Angaben).

☐ Es findet eine **Datenbearbeitung in grossem Umfang** statt unter Berücksichtigung der Anzahl betroffener Personen, des Volumens betroffener Datensätze sowie der Dauer und der

		geografischen Ausdehnung der Datenbearbeitung. ☐ Es werden Datensätze **abgeglichen oder zusammengeführt**, insbesondere aus verschiedenen Datenbearbeitungen und -quellen (z.B. die Ergänzung oder Aktualisierung von bestehenden Kundendaten durch Daten aus Drittquellen, die Verknüpfung von Einträgen einer Person in einer Datenbank mit ihren Einträgen in einer anderen Datenbank). ☐ Es sind Daten **schutzbedürftiger Personen** betroffen, d.h. zwischen dem Unternehmen und den betroffenen Personen gibt es ein grösseres Machtungleichgewicht zugunsten des Unternehmens (z.B. bei Daten über Kinder, Arbeitnehmer, psychisch Kranke, Asylbewerber, Senioren, Patienten). ☐ Es erfolgt eine **innovative Nutzung oder Anwendung neuer Techniken**, d.h. neue Anwendungen, die hinsichtlich ihrer möglichen negativen Folgen für die betroffenen Personen oder auch das Unternehmen noch nicht vollumfänglich eingeschätzt werden können (z.B. gewisse Anwendungen des Internets der Dinge, Gesichtserkennungssysteme, Handy-Tracking, intelligente E-Mail-Analysen zur Erkennung von Datendiebstahl; der Einsatz von *Cookies* an sich ist noch keine innovative Nutzung). ☐ Die Datenbearbeitung kann dazu führen, dass eine betroffene Person daran **gehindert** oder es ihr erschwert wird, **eine Dienstleistung in Anspruch zu nehmen**, einen Vertrag abzuschliessen oder sonst ein Recht auszuüben oder zu erhalten (z.B. die Prüfung der Kreditvergabe durch eine Bank, der Betrieb einer Plattform für Wohnungs- oder Stellenbewerber, die Führung einer "schwarzen Liste", ein System zur Betrugsbekämpfung). ☐ Es gibt **andere Gründe**, die nach unserer Einschätzung für ein voraussichtlich hohes Risiko sprechen: → **voraussichtlich hohes Risiko** ☐ Die Datenbearbeitung und ggf. damit verbundene weitere Datenbearbeitungen weisen eine hohe Komplexität auf und sind daher in ihren Auswirkungen schwer abschätzbar. ☐ Die Intensität der Datenbearbeitung ist besonders gross. ☐ Die Datenbearbeitung könnte für die betroffenen Personen in irgendeiner Weise unangenehme Folgen haben oder sonst als unangenehm empfunden werden. ☐ Die bearbeiteten Daten bergen ein besonderes Missbrauchs-	

			potenzial, falls sie in die falschen Hände gelangen. ☐ Die Datenbearbeitung würde auf öffentliche Kritik stossen, wenn sie bekannt würde. ☐ Andere Gründe: ☐ Wir möchten noch Folgendes vermerken:	
	Q2	*Nur, falls Q1 keine DSFA erfordert:* **Erforderlichkeit einer DSFA II (nur DSGVO)** Eine DSFA ist immer dann erforderlich, wenn die für das Unternehmen zuständige Aufsichtsbehörde eine solche verlangt. *Art. 35 Abs. 4 DSGVO* Die DSGVO räumt den Datenschutzbehörden die Möglichkeit ein, für bestimmte Fälle standardmässig eine DSFA zu verlangen. Hierzu können sie Listen veröffentlichen (sog. *Schwarze Listen*). Die Websites der Datenschutzbehörden geben darüber in aller Regel Auskunft. Einige Fälle sind bereits bekannt und in der mittleren Spalte vereinfacht und beispielhaft aufgelistet. Eine abschliessende Aufzählung ist hier jedoch weder möglich noch sinnvoll, da jede Aufsichtsbehörde ihre eigene Liste veröffentlichen kann, die jeweils nur für deren Zuständigkeitsbereich gilt. Die in der mittleren Spalte publizierten Angaben basieren auf den Ende Mai 2018 publizierten *Schwarzen Listen* der Aufsichtsbehörden für die	*Kurz und bündig:* ☐ Wir werden eine DSFA durchführen. Es spielt für uns also keine Rolle, ob unsere Aufsichtsbehörde eine solche ohnehin vorschreibt. Wir haben das daher nicht weiter geprüft. *Im Detail:* ☐ Wir haben die **Website der für uns zuständigen Aufsichtsbehörde** im EWR **geprüft** bzw. angefragt, ob sie für bestimmte Datenbearbeitungen DSFAs vorschreibt. ☐ Wir sind ein Unternehmen **mit Sitz ausserhalb der EU** bzw. des EWR und haben uns daher an der Datenschutzbehörde am Ort unseres Vertreters nach Art. 27 DSGVO orientiert. → **1. OK** ☐ Wir sind ein Unternehmen **mit Sitz in der EU** bzw. im EWR und haben uns daher an der Datenschutzbehörde an unserem Sitz bzw. Hauptsitz orientiert. → **1. OK** ☐ Wir haben **keinen Vertreter** nach Art. 27 DSGVO, weil wir das nicht brauchen, und haben uns daher im Sinne eines risikobasierten Entscheids nirgends orientiert. Wir richten uns nach den Vorgaben von Q1. → **hier alles OK**	☐ Es ist eine **DSFA durchzuführen**, da unsere Aufsichtsbehörde eine solche verlangt, auch wenn sonst die Kriterien nicht erfüllt wären. → Abschnitt B (Q5 ff.) ☐ Ob für die Datenbearbeitung von unserer Aufsichtsbehörde tatsächlich eine DSFA verlangt wird, ist unseres Erachtens zwar **nicht klar**. Wir erachten eine **DSFA** aber dennoch für **angezeigt**. → Abschnitt B (Q5 ff.) ☐ Es ist auch gemäss der Vorgaben unserer Aufsichtsbehörde **keine DSFA** erforderlich oder angezeigt. ☐ Andere Einschätzung: ☐ **Situation unklar** Grund:

		deutschen Bundesländer Baden-Württemberg, Saarland, Schleswig-Holstein und Rheinland-Pfalz; bis auf die Beispiele "umfassende Profile" und "Leistungsfähigkeit", die bei der *Schwarzen Liste* von Rheinland-Pfalz nicht enthalten sind, führen die genannten Aufsichtsbehörden in ihren *Schwarzen Listen* neben weiteren Fällen sämtliche in der mittleren Spalte erwähnten Beispiele auf. Quelle: datenrecht.ch (https://goo.gl/ybkdkJ). Wir vertreten hier die Haltung, dass für Unternehmen, die vom One-Stop-Mechanismus nicht profitieren können, vorliegend nur die Aufsichtsbehörde am Sitz des Vertreters massgebend ist. Diese Position ist in der DSGVO nicht zwingend angelegt und verlangt daher einen Risikoentscheid des Verantwortlichen.	☐ Wir haben uns bei folgenden bzw. folgender Datenschutzbehörde(n) orientiert: → **1. OK** ☐ Unsere Aufsichtsbehörde hat soweit wir das sehen **keine Schwarze Liste publiziert**. Wir richten uns somit weiterhin nach den Vorgaben von Q1. → **2. OK** ☐ Wir sind bei der **Konsultation der Schwarzen Liste** unserer Aufsichtsbehörde zum Schluss gekommen: ☐ Die Schwarze Liste schreibt für die vorliegende Datenbearbeitung **keine DSFA** vor. → **2. OK** ☐ Die Schwarze Liste **schreibt** für die vorliegende Datenbearbeitung **eine DSFA vor**: → **2. OK** ☐ Weil die Datenbearbeitung umfangreich ist und Daten umfasst: ☐ Die einer **gesetzlichen Geheimhaltungspflicht** unterstehen (z.B. Sozial-, Berufs- oder Amtsgeheimnis). ☐ Über den **Aufenthaltsort** von Personen (z.B. Fahrzeugdatenverarbeitung, Verkehrsstromanalyse anhand von Standortdaten des öffentlichen Mobilfunknetzes). ☐ Weil bei der Datenbearbeitung **umfassende Profile** über die Interessen, das persönliche Beziehungsnetz oder die Persönlichkeit von betroffenen Personen erstellt werden (z.B. Betrieb von Dating- und Kontaktportalen oder grossen sozialen Netzwerken). ☐ Weil die Datenbearbeitung umfangreiche Angaben über das **Verhalten von Angestellten** beinhaltet, mit denen ihre Arbeitstätigkeit derart bewertet werden kann, dass sich Rechtsfolgen oder sonst erhebliche Nachteile für die betroffenen Personen ergeben können (z.B. Geolokalisierung von Angestellten). ☐ Weil bei der Datenbearbeitung zur Bewertung der Persönlichkeit von betroffenen Personen **Video- oder Audio-Aufnahmen** automatisiert ausgewertet werden	☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren

			(z.B. Telefongespräch-Auswertung mittels Algorithmen). ☐ Weil ein **öffentlicher Bereich** mobil und mittels elektronischer Hilfsmittel optisch erfasst wird, ohne dass dies für die betroffenen Personen transparent ist (z.B. Daten von Fahrzeug-Umgebungssensoren). ☐ Weil bei der Datenbearbeitung **künstliche Intelligenz** zum Einsatz kommt, um die Interaktion mit betroffenen Personen zu steuern oder ihre persönlichen Aspekte zu bewerten (z.B. Telefongespräch-Auswertung mittels Algorithmen). ☐ Weil die Daten mittels Sensoren erhoben, an einer zentralen Stelle bearbeitet und dazu verwendet werden, die **Leistungsfähigkeit** von betroffenen Personen zu bestimmen (z.B. Speicherung von Sensor-Messdaten von Smartphones oder Fitnessarmbändern). ☐ Aus **anderen Gründen**: ☐ Wir sind zu folgendem Ergebnis gekommen: ☐ Wir möchten noch Folgendes vermerken:	
	Q3	*Nur, falls Q1 eine DSFA erfordert:* **Ausnahmen (nur DSG)** Das DSG definiert eine Reihe von Fällen, in welchen keine DSFA erforderlich ist, so insbesondere, wenn die Datenbearbei-	☐ Es wurde bereits eine **DSFA für eine andere Datenbearbeitung** durchgeführt, deren Art, Umfang, Umstände und Zwecke sich von der vorliegenden Datenbearbeitung **nur in geringem Mass unterscheiden**, nämlich:	☐ Die Ausnahmen sind nicht relevant, da gemäss Q1 keine DSFA erforderlich ist. ☐ Es ist eine **DSFA durchzuführen**, da keine der Ausnahmen gegeben ist → Abschnitt B (Q5 ff.) ☐ Es ist unseres Erachtens **keine DSFA durchzuführen**, da

		tung der Erfüllung einer gesetzlichen Pflicht dient, anderswie bereits auf ihre Risiken beurteilt wurde oder nicht mehr relevant ist. *Art. [20] Abs. 4 und Abs. 5, Art. [63] Abs. 2 und Art. [64] Abs. 3 DSG* Die Ausnahmen ergeben sich direkt aus dem Gesetz, einschliesslich der Übergangsbestimmungen. Noch ungewiss ist, ob die Ausnahme auch dann gilt, wenn die Datenbearbeitung nicht nur, aber auch zur Erfüllung einer gesetzlichen Pflicht dient. Das Gesetz spricht zwar davon, dass eine DSFA "vorgängig", d.h. vor der Aufnahme der Datenbearbeitung erstellt werden muss. Dies bedeutet jedoch nicht, dass dies ein einmaliger Vorgang ist. Eine DSFA wird im Laufe der Zeit wiederholt werden müssen. Das ist zum Einen der Fall, wenn sich die Datenbearbeitung in ihren datenschutzrechtlich wesentlichen Aspekten verändert oder die Verhältnisse, in welchen sie zur Anwendung gelangen (z.B. die Umstände der betroffenen Personen, die Bedeutung der Datenbearbeitung), sich wesentlich verändert haben. Zum Anderen wird eine DSFA nach einer gewissen Zeit auch ohne solche Anpassungen erneuert werden müssen. Als Faustregel gilt, dass eine DSFA alle drei Jahre erneuert werden muss.	☐ Wir sind ein privates Unternehmen und die Datenbearbeitung, um die es geht, nehmen wir vor, weil das **Schweizer Recht uns dazu verpflichtet**, d.h. konkret: ☐ Um die uns auferlegten Pflichten zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung zu erfüllen. ☐ Um die uns auferlegten Pflichten zur Leistung der Sozialabgaben zu erfüllen. ☐ Um unseren aufsichtsrechtlichen Dokumentationspflichten nachzukommen. ☐ Um unseren aufsichtsrechtlichen Meldepflichten nachzukommen. ☐ Um unseren arbeitsrechtlichen Pflichten nachzukommen, einschliesslich der Sicherstellung der Gleichberechtigung, Arbeitssicherheit und -gesundheit und sonstigen Pflichten als Arbeitgeber (dies erfasst z.B. die Führung des Personal–dossiers). ☐ Um unserer Pflicht zur Führung unserer Geschäftsbücher und Abrechnung unserer Steuerpflichten nachzukommen (dies erfasst z.B. das Rechnungswesen). ☐ Weil wir im Rahmen der Datenbearbeitung als Bundesorgan im Sinne des DSG gelten und diese sich ausschliesslich im Rahmen unserer gesetzlichen Grundlage bewegt (z.B. Art. 84 und 84a KVG). ☐ Andere gesetzliche Pflicht: ☐ Wir sind ein privates Unternehmen, das mit Bezug auf die Datenbearbeitung einen **Verhaltenskodex** im Sinne von Art. [10] DSG einhält, der alle der folgenden Voraussetzungen erfüllt: ☐ Er beruht auf einer DSFA, mit welcher die Art der Datenbearbeitung, um die es geht, bereits generisch geprüft wurde. ☐ Er sieht Massnahmen zum Schutz der Persönlichkeit oder der Grundrechte der betroffenen Personen vor. ☐ Er wurde dem EDÖB vorgelegt.	mindestens einer der Ausnahmegründe erfüllt ist ☐ Andere Einschätzung: ☐ **Situation unklar** Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren

				☐ Wir sind ein privates Unternehmen und haben die Datenbearbeitung, um die es geht, bereits im Rahmen von Art. [12] Abs. 1 DSG hinsichtlich der Datenschutzkonformität bewerten und erfolgreich zertifizieren lassen (**Datenschutz-Qualitätszeichen**). Verändert sich die Datenbearbeitung, wird eine neue Bewertung erforderlich. ☐ Die **Datenbearbeitung** ist zum Zeitpunkt des Inkrafttretens des revidierten DSG ([Datum]) bereits **abgeschlossen** (d.h. nach dem gewöhnlichen Gang der Dinge ist sie auf eine Aufbewahrung bzw. Speicherung der Daten beschränkt; Ausnahmen wie z.B. Auskunftsersuchen, Rückgriffe aufgrund von Datenverlusten oder Rechtsstreitigkeiten bleiben vorbehalten). ☐ Die **Datenbearbeitung** hat vor dem Inkrafttreten des DSG ([Datum]) **begonnen** (d.h. es finden erste Vorkehrung zur Bearbeitung von Personendaten statt, wie z.B. das Programmieren eines Online-Fragebogens, der Entwurf einer Einwilligungserklärung, die Instruktion des Personals oder das Aufsetzen der betreffenden Systeme) und es sind folgende zwei Voraussetzungen kumulativ erfüllt: ☐ Es hat sich ihr Zweck nicht verändert (verändert hat sich der Zweck nur dann, wenn er nicht schon vor Inkrafttreten mindestens teilweise verfolgt wurde oder hätte gestützt auf Art. 4 Abs. 3 altes DSG hätte verfolgt werden dürfen). ☐ Es wurden keine neuen Daten beschafft. ☐ Das revidierte DSG ([Datum]) ist seit **weniger als zwei Jahren in Kraft** (ansonsten muss die DSFA nachgeholt werden, falls keine der anderen Ausnahmen greift). ☐ Es liegt einer der Fälle vor, für welchen unsere **Aufsichtsbehörde** erklärt hat, dass keine DSFA nötig ist (*Weisse Liste*): ☐ Wir möchten noch Folgendes vermerken:	

Q4

Nur, falls Q1 oder Q2 eine DSFA erfordert:

Ausnahmen (nur DSGVO)

Die DSGVO definiert einige wenige Fälle, in welchen keine DSFA erforderlich ist, so insbesondere, wenn für eine ähnliche Datenbearbeitung bereits eine solche durchgeführt worden oder die Behörden die Risiken für die betroffenen Behörden bereits geprüft und für akzeptabel befunden haben.

Art. 35 Abs. 1, 4 und 10 DSGVO

Die DSGVO räumt den Datenschutzbehörden die Möglichkeit ein, für bestimmte Fälle zu erklären, dass keine DSFA erforderlich ist. Hierzu können sie Listen veröffentlichen (sog. *Weisse Listen*). Die Websites der Datenschutzbehörden geben darüber in aller Regel Auskunft. Allerdings sind diese mit Vorsicht zu geniessen; darauf stützen können sich Unternehmen nur dann, wenn sie in den örtlichen Zuständigkeitsbereich dieser Behörden fallen. Bei Unternehmen ausserhalb der EU bzw. des EWR wird es nur selten eine einzige zuständige Behörde geben, auch wenn ein Unternehmen sich aus Gründen der Praktikabilität auf jene Behörde ausrichten kann, in deren Zuständigkeitsbereich sie ihren Vertreter nach Art. 27 DSGVO bestellt hat. Publiziert hat bisher (Ende Mai) erst eine Behörde eine weisse Liste (Belgien). Einige der darin enthaltenen Fälle sind vereinfacht in der mittleren Spalte aufgeführt. Quelle: datenrecht.ch (https://goo.gl/ybkdkJ).

☐ Es wurde **bereits eine DSFA durchgeführt**:

- ☐ Für eine **andere Datenbearbeitung**, deren Art, Umfang, Umstände und Zwecke sich von der vorliegenden Datenbearbeitung nur **in geringem Mass unterscheiden**.
- ☐ **Im Rahmen der Schaffung einer gesetzlichen Bestimmung** des Rechts der EU oder eines Mitglieds der EU (bzw. des EWR), auf welche sich die Datenbearbeitung als **Rechtsgrundlage** i.S. von Art. 6 Abs. 1 Bst. c oder e DSGVO stützt (d.h. Erfüllung einer rechtlichen Verpflichtung oder Wahrnehmung einer Aufgabe, die im öffentlichen Interesse ist oder in Ausübung öffentlicher Gewalt).

☐ Die Datenbearbeitung wurde bereits vor dem Inkrafttreten der DSGVO (25. Mai 2018) **von einer Aufsichtsbehörde überprüft** und sie wird noch immer auf dieselbe Art durchgeführt (Umfang, Zweck, erfasste Personendaten, Identität des Verantwortlichen oder Empfängers, Datenspeicherfrist, technische und organisatorische Massnahmen etc.).

☐ Es liegt einer der folgenden Fälle vor, für welche die für uns zuständige **Aufsichtsbehörde** (vgl. Q2) erklärt hat, dass keine DSFA nötig ist (*Weisse Liste*):

- ☐ Die Datenbearbeitung ist erforderlich zur **Erfüllung einer rechtlichen Verpflichtung**, die von uns verlangt, den Missbrauch sowie den unbefugten Zugriff oder die unbefugte Weitergabe der Daten zu verhindern.
- ☐ Die Datenbearbeitung ist erforderlich zur:
  - ☐ **Verwaltung** von:
    - ☐ **Personal** oder dessen **Gehälter**;
    - ☐ **Aktionären** oder anderen Mitgliedern;
    - ☐ **Kunden** oder **Lieferanten**;
    - ☐ **Schülern** oder **Studenten** durch eine Bildungseinrichtung im Rahmen der Lehrtätigkeit;
  - ☐ **Registrierung von Besuchern** im Rahmen einer Zu-

☐ Die Ausnahmen sind nicht relevant, da gemäss Q1 keine DSFA erforderlich ist.

☐ Es ist eine **DSFA durchzuführen**, da keine der Ausnahmen gegeben ist

→ Abschnitt B (Q5 ff.)

☐ Es ist unseres Erachtens **keine DSFA durchzuführen**, da mindestens einer der Ausnahmegründe erfüllt ist

☐ Andere Einschätzung:

☐ **Situation unklar**

Grund:

- ☐ Weitere Abklärungen sind nötig
- ☐ Experte konsultieren

gangskontrolle;

- ☐ **Buchführung**;

und dient nur diesem Zweck. Die entsprechenden Daten werden anderen Personen nur soweit rechtlich zulässig mitgeteilt und nicht länger als nötig aufbewahrt.

☐ Unsere Aufsichtsbehörde ist (vgl. Q2):

- ☐ Jene an unserem Sitz.
- ☐ Jene am Sitz unseres Vertreters nach Art. 27 DSGVO.

☐ Wir möchten noch Folgendes vermerken:

Weitere Bemerkungen:

B. Datenschutz-Folgenabschätzung (DSFA)

Q5

Beschreibung der Datenbearbeitung

Es ist die Datenbearbeitung bezüglich ihrer Art, Umstände und Zwecke und verfolgten Interessen sowie ihres Umfangs zu beschreiben. Es ist auch zu beschreiben, welche Mittel zum Einsatz kommen, wie die Bearbeitung in groben Zügen funktioniert und wer Daten erhält.

Art. [20] Abs. 3 DSG und Art. 35 Abs. 7 Bst. a und Abs. 8 DSGVO

Die Angaben sollten etwas ausführlicher als im Inventar gemäss Art. 30 DSGVO bzw. Art. [11] DSG erfolgen. Es kann aber bei Bedarf darauf verwiesen werden. Es müssen nur jene Aspekte und Details angeführt werden, die für ein generelles Verständnis der Datenbearbeitung und die Beurteilung der damit für die betroffenen Personen verbundenen Risiken von Relevanz sein können.

Mit genehmigten Verhaltensregeln sind Verhaltensregeln gemäss Art. [10] DSG bzw. Art. 40 DSGVO gemeint.

Worum es bei der Bearbeitung geht:

☐ Videoüberwachung ☐ Zugangskontrollsystem

☐ Tracking und Profilierung der Benutzer der Website

☐ Forensische Auswertung von E-Mails und Dokumenten

☐ Vgl. Beilage

Welchen Zwecken die Bearbeitung dient:

☐ Wahrung der Sicherheit, Ahndung von Sicherheitsverstössen

☐ Untersuchung möglicher Missbräuche

☐ Individuelles Direktmarketing (z.B. persönliche Werbung)

☐ Zugangskontrolle

☐ → Formular B.2 (liegt bei bzw. ist abrufbar: _____)

☐ Vgl. Beilage

Welches Interesse wir an der Bearbeitung haben:

☐ Wir sind der Meinung, dass die Beschreibung in den hier relevanten Punkten **vollständig** und **aktuell** ist.

☐ Es sind Änderungen in der Datenbearbeitung geplant, die aber noch nicht reflektiert sind:

☐ Die Beschreibung ist noch **nicht vollständig** oder noch **nicht aktuell**. Dies muss noch nachgeholt werden.

☐ Die Beschreibung muss noch **geprüft** werden:

☐ Andere Einschätzung:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

		☐ Schutz von Kunden, Mitarbeitern und anderen Personen und Schutz der Daten, Geheimnisse und Vermögenswerte des Unternehmens und solche, die diesem anvertraut worden sind, Sicherheit der Systeme und Gebäude des Unternehmens ☐ Einhaltung der rechtlichen und regulatorischen Anforderungen und internen Regeln ☐ Kundenbetreuung, Kontaktpflege und sonstige Kommunikation mit Kunden auch ausserhalb der Vertragsabwicklung ☐ Aufrechterhaltung und Organisation des Geschäftsbetriebs, einschliesslich des Betriebs und einer erfolgreichen Weiterentwicklung der Website und anderer IT-Systeme ☐ Verkauf und Lieferung von Produkten und Dienstleistungen, auch mit Bezug auf Personen, die nicht direkt Vertragspartner sind (wie z.B. begünstigte Personen) ☐ Sinnvolle Unternehmensführung und -entwicklung ☐ Nachvollzug von Kundenverhalten, -aktivitäten, -vorliegen und -bedürfnissen, Marktstudien ☐ Verbesserung der bestehenden Produkte und Dienstleistungen und Entwicklung neuer Produkte und Dienstleistungen ☐ Durchführung von Werbung und Marketing ☐ Erfolgreicher Verkauf oder Kauf von Geschäftsbereichen, Gesellschaften oder Teilen von Gesellschaften und andere gesellschaftsrechtliche Transaktionen ☐ Interesse an der Verhinderung von Betrug, Vergehen und Verbrechen sowie an Untersuchungen im Zusammenhang mit solchen Delikten und sonstigem unangebrachten Verhalten, Behandlung von rechtlichen Klagen und Vorgehen gegenüber dem Unternehmen, Mitwirkung an Rechtsverfahren und Kooperation mit Behörden, und sonst die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. **Welche Personendaten erhoben und sonst bearbeitet werden:**	

☐ Videoaufzeichnungen ☐ Nutzung der Website und Apps

☐ E-Mails und Dokumente von Mitarbeitern bzw. aus dem Betrieb

☐ → Formular B.2 (liegt bei bzw. ist abrufbar: _____)

☐ Vgl. Beilage

Wieviele Personen und Personendaten betroffen sind:

☐ Vgl. Beilage

Wie und wo die Bearbeitung erfolgt:

☐ Nur Live-Bilder im Sicherheitszentrum

☐ Aufzeichnung von Videobildern, Aufbewahrung 24-48h

☐ Vgl. Beilage

Welche Dritte Zugang zu Personendaten erhalten:

☐ Auftragsbearbeiter, andere Dienstleister für unsere Zwecke

☐ Auf Datenanalysen spezialisierte Firma

☐ Konzerngesellschaften

☐ Beteiligte an einem zivilrechtlichen Gerichtsverfahren (Inland)

☐ Beteiligte an einem zivilrechtlichen Gerichtsverfahren (Ausland)

☐ Strafbehörden (Inland) ☐ Aufsichtsbehörden (Inland)

☐ Strafbehörden (Ausland) ☐ Aufsichtsbehörden (Ausland)

☐ → Formular B.2 (liegt bei bzw. ist abrufbar: _____)

☐ Vgl. Beilage

Welche Hardware, Software, Netzwerke, Personen und Übermittlungswege zum Einsatz kommen:

☐ Videokameras ☐ E-Mail-Analysesoftware

☐ Netzwerksicherheitssysteme

☐ Dokumenten-Review-Systeme

☐ Vgl. Beilage

☐ Weitere Angaben finden sich in:

☐ Liegt bei

☐ Die Bearbeitung folgt genehmigten Verhaltensregeln:

		☐ Wir möchten noch Folgendes vermerken: [ ]	
Q6	*Option 1:* **Prüfung der Einhaltung des Datenschutzrechts und Dokumentation der Massnahmen** Es ist zu ermitteln, ob die Datenbearbeitung die Vorgaben des anwendbaren Datenschutzrechts einhält und welche weiteren Massnahmen ggf. erforderlich sind. Die getroffenen Massnahmen sind in einem Datenschutzkonzept festzuhalten. *Art. [20] Abs. 3 DSG, Art. 35 Abs. 7 Bst. b und d DSGVO* Wenn im Rahmen einer DSFA die Risiken einer Datenbearbeitung für die Persönlichkeit der betroffenen Personen abzuschätzen ist, ist immer auch zu prüfen, ob jene allgemeinen Vorgaben des anwendbaren Datenschutzrechts eingehalten werden, die zum Schutz der Persönlichkeit aufgestellt sind. Dies entspricht auch den Empfehlungen der EU-Datenschutzbehörden (WP29) in WP248. Hierbei ist nicht nur zu prüfen, ob die Vorgaben eingehalten werden, sondern die Massnahmen, mit denen dies sichergestellt wird, sind rudimentär zu dokumentieren (wie dies im Formular E.1 nicht geschieht). Dieses Formular für eine DSFA sieht zwei Optionen vor, wie dieses Erfordernis erfüllt werden kann. Es kann eine Prüfung gestützt auf das Formular E.1 erfolgen, mit einer separaten Dokumentation der Massnahmen im Sinne eines Datenschutzkonzepts (Option 1), oder die Dokumentation kann in diesem Formular erfolgen (Option 2). Beide Varianten sind möglich, wobei Option 2 für kleinere, weniger komplexe Vorhaben gedacht ist.	☐ Wir haben die Datenbearbeitung auf die **Einhaltung der Vorgaben des anwendbaren Datenschutzrechts**, einschliesslich der Einhaltung der Betroffenenrechte geprüft: → **1. OK** ☐ Mit → **Formular E.1.** ☐ Das vollständig ausgefüllte Formular E.1 liegt bei bzw. ist abrufbar: _____ ☐ **Interne Beurteilung** durch Fachspezialist ☐ Rechtsdienst ☐ Fachstelle Datenschutz ☐ Datenschutzbeauftragten i.S.v. Art. 37 DSGVO ☐ Liegt bei bzw. ist abrufbar: _____ ☐ **Externe Beurteilung** durch Fachspezialist ☐ Liegt bei bzw. ist abrufbar: _____ ☐ Folgendes getan, um herauszufinden, dass die Datenbearbeitung notwendig und verhältnismässig ist: [ ] ☐ Wir sind gestützt darauf zur Ansicht gelangt, dass die Datenbearbeitung: ☐ Die Anforderungen **grundsätzlich erfüllt**. → **2. OK**	☐ Wir wählen nicht Option 1. *Weiter zu → Q7 (Option 2)* ☐ Wir sind der Meinung, dass die Datenbearbeitung die **Vorgaben des anwendbaren Datenschutzrechts** so weit wie für uns möglich **erfüllt**. ☐ Die Massnahmen sind bereits dokumentiert. ☐ Die Massnahmen sollten noch dokumentiert werden. *Weiter zu → Q8 (Restrisiken)* ☐ Wir sind der Meinung, dass die Datenbearbeitung nicht die **Vorgaben** des anwendbaren Datenschutzrechts erfüllt. ☐ Folgende Massnahmen sollten noch getroffen werden: [ ] ☐ Gem. Beilage ☐ Auch die Dokumentation der Massnahmen sollte noch nachgeholt werden *Weiter zu → Q8 (Restrisiken)* ☐ Andere Einschätzung: [ ]

		Wird eine Vorgabe des anwendbaren Datenschutzrechts nicht eingehalten, besteht ein Defizit und damit ein Risiko, das in Q7 beurteilt werden muss.	☐ Die Anforderungen grundsätzlich erfüllt, aber mit folgenden **Ausnahmen**. Soweit hier Massnahmen nach unserer Meinung möglich sind, haben wir sie vorgesehen. → **2. OK** ☐ Die Anforderungen in zu vielen Punkten **nicht erfüllt**, als dass sie hier aufgeführt werden können. ☐ Wir haben die zum Datenschutz (insbesondere zum Schutz der betroffenen Personen) getroffenen Massnahmen: ☐ In einem Datenschutzkonzept **dokumentiert**. → **3. OK** ☐ Liegt bei bzw. ist abrufbar: _____ ☐ **Nicht dokumentiert**. ☐ Wir möchten noch Folgendes vermerken:	☐ **Situation unklar** Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren
	Q7	*Option 2:* **Prüfung der Einhaltung des Datenschutzrechts und Dokumentation der Massnahmen** Es ist zu ermitteln, ob die Datenbearbeitung die Vorgaben des anwendbaren Datenschutzrechts einhält und welche weiteren Massnahmen ggf. erforderlich sind. Die getroffenen Massnahmen sind festzuhalten. *Art. [20] Abs. 3 DSG, Art. 35 Abs. 7 Bst. b und d DSGVO* Wenn im Rahmen einer DSFA die Risiken einer Datenbearbeitung für die Persönlichkeit der betroffenen Personen abzuschätzen sind, ist immer	☐ Wir haben in der Ausgestaltung der Datenbearbeitung folgende **Massnahmen zur Sicherstellung des Datenschutzes** umgesetzt bzw. vorgesehen: → **1. OK** ☐ Den betroffenen Personen ist **klar**, dass und **wie wir ihre Personendaten erheben** und bearbeiten, insbesondere für welche Zwecke wir dies tun: ☐ Hinweis ☐ Datenschutzerklärung (direkt oder per Link) ☐ Andere Massnahme(n): ☐ Erfüllen wir nicht bzw. Massnahme fehlt ☐ Die Daten werden von uns **nicht für andere Zwecke** bear-	☐ Wir wählen nicht Option 2. *Zurück zu → Q6 (Option 1)* ☐ Wir haben in einem ersten Schritt alle **Massnahmen dokumentiert**, welche wir zur Sicherstellung des Datenschutzes umgesetzt bzw. vorgesehen haben. Zu einem **späteren Zeitpunkt** sollte noch eine vollständige Prüfung mit → Formular E.1 stattfinden. *Weiter zu → Q8 (Restrisiken)* ☐ Wir sind der Meinung, dass die Datenbearbeitung die **Vorgaben des anwendbaren Datenschutzrechts** so weit wie für uns möglich **erfüllt**. ☐ Die Massnahmen sind bereits dokumentiert. ☐ Die Massnahmen sollten noch dokumentiert werden. *Weiter zu → Q8 (Restrisiken)* ☐ Wir sind der Meinung, dass die Datenbearbeitung die

auch zu prüfen, ob jene allgemeinen Vorgaben des anwendbaren Datenschutzrechts eingehalten werden, die zum Schutz der Persönlichkeit aufgestellt sind. Dies entspricht auch den Empfehlungen der EU-Datenschutzbehörden (WP29) in WP248. Hierbei ist nicht nur zu prüfen, ob die Vorgaben eingehalten werden, sondern die Massnahmen, mit denen dies sichergestellt wird, sind rudimentär zu dokumentieren (wie dies im Formular E.1 nicht geschieht).

Dieses Formular für eine DSFA sieht zwei Optionen vor, wie dieses Erfordernis erfüllt werden kann. Es kann eine Prüfung gestützt auf das Formular E.1 erfolgen, mit einer separaten Dokumentation der Massnahmen im Sinne eines Datenschutzkonzepts (Option 1), oder die Dokumentation kann in diesem Formular erfolgen (Option 2). Beide Varianten sind möglich, wobei Option 2 für kleinere, weniger komplexe Vorhaben gedacht ist.

Bei Option 2 ist jeweils bei der betreffenden Anforderung anzugeben, wie sie erfüllt wird, falls überhaupt. Ist dies nicht der Fall, besteht ein Defizit und damit ein Risiko, das in Q7 beurteilt werden muss.

beitet, als jene, für die sie erhoben wurden:

☐ Weisung ☐ Eingeschränkter Zugriff

☐ Andere Massnahme(n):

☐ Erfüllen wir nicht bzw. Massnahme fehlt

☐ Unsere Zwecke sind **legitim** und – soweit vom Gesetz verlangt – besteht eine **Rechtsgrundlage**, die uns erlaubt, sie zu verfolgen:

☐ Interne Abklärung ☐ Externe Abklärung

☐ Andere Massnahme(n):

☐ Erfüllen wir nicht bzw. Massnahme fehlt

☐ Wird erheben nur Daten, die für unsere Zwecke **geeignet und erforderlich** sind sowie in einem **vernünftigen Verhältnis** zu den Zwecken stehen:

☐ Weisung ☐ Keine Freitext-Felder

☐ Systeme sind entsprechend programmiert

☐ Überwachungssysteme sind so eingestellt, dass sie nur das erfassen, um das es wirklich geht

☐ Andere Massnahme(n):

☐ Erfüllen wir nicht bzw. Massnahme fehlt

☐ Die Daten sind nur den Personen und **nur solange zugänglich** sind, wie für die Zwecke nötig (*"need-to-know"*):

☐ Weisung ☐ Eingeschränkter Zugriff

Vorgaben des anwendbaren Datenschutzrechts nicht erfüllt bzw. dass gewisse Massnahmen fehlen.

☐ Folgende Massnahmen sollten noch getroffen werden:

☐ Gem. Beilage

Weiter zu → Q8 *(Restrisiken)*

☐ Andere Einschätzung:

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

		☐ Wir anonymisieren die Daten raschmöglichst ☐ Wir pseudonymisieren die Daten raschmöglichst ☐ Andere Massnahme(n): ☐ Erfüllen wir nicht bzw. Massnahme fehlt ☐ Die **Datenbearbeitung** ist auch sonst **auf das einzuschränken**, was wirklich **erforderlich** ist: ☐ Weitere Einschränkungen sind nicht möglich, ohne den Sinn und Zweck der Bearbeitung in Frage zu stellen. ☐ Weitere Einschränkungen sind möglich: ☐ Erfüllen wir nicht bzw. Massnahme fehlt ☐ Die Daten sind soweit für die Zwecke nötig **richtig und vollständig**: ☐ Weisung ☐ Plausibilitätschecks ☐ Betroffene Personen können sie selbst verwalten ☐ Andere Massnahme(n): ☐ Erfüllen wir nicht bzw. Massnahme fehlt ☐ Die Daten werden **gelöscht** (oder anonymisiert), sobald sie für die Zwecke **nicht mehr gebraucht werden**. ☐ Weisung ☐ Manuelle Löschung ☐ Systeme sind entsprechend programmiert	

☐ Daten werden nicht gelöscht, aber sicherheitsverwahrt

☐ Wir pseudonymisieren die Daten raschmöglichst

☐ Andere Massnahme(n):

☐ Erfüllen wir nicht bzw. Massnahme fehlt

☐ Wir gewährleisten die **Rechte der betroffenen Personen**:

☐ **Informationsrecht** (→ Formular E.1, Q24), d.h. den betroffenen Personen werden alle Pflichtangaben gem. Gesetz gemacht

☐ Datenschutzerklärung

☐ Andere Massnahme(n):

☐ Erfüllen wir nicht bzw. Massnahme fehlt

☐ **Auskunftsrecht** (→ Formular E.1, Q23)

☐ Verantwortlichkeit festgelegt

☐ Weisung ☐ Prozess definiert

☐ Systeme sind entsprechend programmiert

☐ Betroffene Personen können Daten selbst abrufen

☐ Andere Massnahme(n):

☐ Erfüllen wir nicht bzw. Massnahme fehlt

☐ **Berichtigungsrecht** (→ Formular E.1, Q15)

☐ Verantwortlichkeit festgelegt

☐ Weisung ☐ Prozess definiert

☐ Systeme sind entsprechend programmiert

☐ Betroffene Personen können Daten selbst ändern

☐ Andere Massnahme(n):

☐ Erfüllen wir nicht bzw. Massnahme fehlt

☐ **Lösch- und Sperrbegehren** (→ Formular E.1, Q21)

☐ Verantwortlichkeit festgelegt

☐ Weisung ☐ Prozess definiert

☐ Systeme sind entsprechend programmiert

☐ Betroffene Personen können Daten selbst löschen bzw. die Verwendung ihrer Daten sperren (inkl. Austragung aus Direkt-Marketing-Listen)

☐ Andere Massnahme(n):

☐ Erfüllen wir nicht bzw. Massnahme fehlt

☐ Die Regeln zur **Auftragsbearbeitung** sind eingehalten (→ Formular F.1):

☐ Vertrag mit Auftragsbearbeiter

☐ Auftragsbearbeiter hat Sicherheitsvorgaben

☐ Auftragsbearbeiter hat Instruktionen

☐ Andere Massnahme(n):

☐ Erfüllen wir nicht bzw. Massnahme fehlt

☐ Die Regeln zur **Bekanntgabe von Daten ins Ausland** sind eingehalten (→ Formular E.1, Q16), soweit sie zur Anwendung kommen:

- ☐ Keine Bekanntgabe in unsichere Drittstaaten
- ☐ Vertrag mit Empfänger in unsicherem Drittstaat
- ☐ Privacy Shield ☐ Vertragsabwicklung
- ☐ Andere Massnahme(n):

☐ Erfüllen wir nicht bzw. Massnahme fehlt

☐ Die **Vertraulichkeit, Integrität und Verfügbarkeit der Daten** ist sichergestellt (Datensicherheit):

- ☐ Persönliche Logins ☐ Rollenbasierter Zugang
- ☐ Audit Trails, Logs ☐ Anti-Malware-Software
- ☐ Weisungen ☐ Abgeschlossene Räume
- ☐ Ausbildung ☐ Kontrollen
- ☐ Firewalls, VPN ☐ 2-Faktor-Authentifikation
- ☐ Data-at-rest ist verschlüsselt
- ☐ Data-in-transit ist verschlüsselt
- ☐ Pseudonymisierung ☐ Anonymisierung
- ☐ Backups ☐ Disaster Recovery Konzept
- ☐ Massnahmen-System zertifiziert nach ISO 27001
- ☐ Andere Massnahme(n):

		☐ Erfüllen wir nicht bzw. Massnahme fehlt ☐ Wir haben die **Datenbearbeitung** mit dem → **Formular E.1 geprüft**: ☐ Es sind nach unserer Meinung **keine weiteren relevanten Massnahmen** erforderlich: → **2. OK** ☐ Es sind **folgende weitere relevanten Massnahmen** erforderlich (die wir umsetzen werden): → **2. OK** ☐ Es sind weitere relevante Massnahmen erforderlich, aber wir können diese **nicht bzw. nicht alle umsetzen**. ☐ Das vollständig ausgefüllte Formular E.1 liegt bei bzw. ist abrufbar: _____ ☐ Wir haben eine im Wesentlichen gleich **gelagerte Datenbearbeitung** bereits auf die Erfüllung der Vorgaben des anwendbaren Datenschutzrechts geprüft. Demnach sind keine weiteren Massnahmen erforderlich, als jene, die oben angegeben sind. → **2. OK** ☐ Gem. Beilage (bzw. hier abrufbar: _____) ☐ Wir möchten noch Folgendes vermerken:	
Q8	**Risiken für betroffene Personen** Es ist zu ermitteln, welche Risiken die Datenbearbeitung für die betroffenen Personen ungeachtet der vorgesehenen Massnahmen mit sich bringen, und es ist zu beurteilen, ob diese Risiken hoch sind. *Art. 35 Abs. 7 Bst. b DSGVO*	☐ Die Datenbearbeitung kann sich in folgenden Fällen **naturgemäss negativ** auf die betroffenen Personen **auswirken** *(weitere Risiken werden weiter unten geprüft)*: ☐ Verweigerung des gewünschten Vertrags bzw. der gewünschten Vertragskonditionen ☐ Verweigerung einer Leistung an die betroffene Person ☐ Kündigung eines Vertrags	☐ Die Restrisiken der Datenbearbeitung sind in Anerkennung der umgesetzten oder vorgesehenen Massnahmen gemäss Q6 bzw. Q7 sowie Q8 nicht bzw. nicht mehr hoch. *Weiter zu → Q9 bzw. Q10 (Konsultationen)* ☐ Die **Restrisiken** der Datenbearbeitung sind in Anerkennung der umgesetzten oder vorgesehenen Massnahmen gemäss Q6 bzw. Q7 sowie Q8 **nach wie vor hoch**. ☐ Die Datenbearbeitung ist in Anbetracht dessen einzu-

Zunächst ist eine Klärung der Begrifflichkeiten nötig, da sie häufig durcheinander gebracht werden. Im vorliegenden Fall sollen betroffene Personen durch die Datenbearbeitung nicht (zu Unrecht) Nachteile erleiden müssen:

- Verschiedenste Umstände können solche Nachteile (*Harms*) verursachen, so z.B. Missbräuche durch interne und externe Stellen, Ausfälle von Systemen, Fehlfunktionen, Verwechslungen oder Ungeauigkeiten. Es sind dies Bedrohungen bzw. Gefahren (*Threats*).
- *Threats* können sich dort verwirklichen (d.h. zu den Nachteilen für die betroffenen Personen führen, den *Harms*), wo die Datenbearbeitung ungeachtet aller Massnahmen noch Schutzlücken oder -schwächen aufweist, z.B. weil Verwechslungen nicht erkannt werden, Ausfälle nicht überbrückt oder unbefugte interne oder externe Zugriffe nicht verhindert werden können (*Vulnerabilities*, Verwundbarkeiten).
- Der Begriff des Risikos (*Risk*) greift dies auf und sagt aus, wie wahrscheinlich welcher Schaden in Anbetracht der bestehen Bedrohungen und Verwundbarkeiten ist. Ob ein tiefes, mittleres oder hohes Risiko vorliegt, kann wie folgt beurteilt werden, wobei auch andere Skalen möglich und gebräuchlich sind:

Wahrscheinlich	Mittleres Risiko	Hohes Risiko	Hohes Risiko
Möglicherweise	Tiefes Risiko	Mittleres Risiko	Hohes Risiko
Unwahrscheinlich	Tiefes Risiko	Tiefes Risiko	Mittleres Risiko
	Spürbare Nachteile	Gewichtige Nachteile	Bedrohliche Nachteile

Für die Zwecke einer DSFA ist entscheidend, ob ungeachtet aller getroffenen Absicherungen und weiteren Massnahmen die Datenbearbeitung noch so "verwundbar" ist, dass angesichts der generell und im konkreten Fall bestehenden Bedrohungen

- ☐ Vertragsstrafen
- ☐ Verweigerung einer Leistung an die betroffene Person
- ☐ Strafanzeige bzw. Anzeige bei der Aufsichtsbehörde
- ☐ Geltendmachung von Rechtsansprüchen gegen die Person
- ☐ *Naming and Shaming*
- ☐ Aussperrung einer Person
- ☐ Weitere negative Folgen materieller oder immaterieller Natur:

☐ Um zu verhindern, dass eine betroffene Person diese Nachteile *zu Unrecht* erleidet, haben wir **folgende Massnahmen** getroffen:

- ☐ Vollkontrolle durch einen Menschen
- ☐ Vier-Augen-Prinzip
- ☐ Stichprobenkontrolle durch einen Menschen
- ☐ Betroffene Person kann sich beschweren
- ☐ Einprogrammierte Plausibilisierungen
- ☐ Konkrete (auf die Bearbeitung zugeschnittene) Anweisung mit einem Kontrollmechanismus
- ☐ Weitere Massnahmen:

schränken:

☐ Es sind weitere mögliche Massnahmen zur Eindämmung der Risiken zu prüfen.

Weiter zu → Q9 bzw. Q10 (Konsultationen)

☐ Andere Einschätzung:

☐ **Situation unklar**

Grund:

- ☐ Weitere Abklärungen sind nötig
- ☐ Experte konsultieren

	ein hohes Risiko gemäss obiger Matrix besteht. In der mittleren Spalte wird ein etwaiges "hohes" Restrisiko einerseits für zwei Konstellationen geprüft: Erstens geht es um negative Folgen für eine betroffene Person, die eine Datenbearbeitung gewollt haben soll (z.B. Verweigerung eines Vertragsschlusses), die aber den Falschen treffen. Zweitens sollen alle anderen Restrisiken "abgefragt" werden, so insbesondere Datensicherheitsrisiken. In dieser zweiten Runde können auch die Restrisiken beurteilt werden, die aufgrund der Nichteinhaltung der Vorgaben des anwendbaren Datenschutzrechts entstehen (d.h. gemäss Q6 bzw. Q7). Dazu werden jeweils die Bedrohungen identifiziert, etwaige Gegenmassnahmen aufgeführt, die nicht schon oben (in Q6 bzw. Q7) aufgeführt sind und dann hinsichtlich der Wahrscheinlichkeit und Schwere ihrer Folgen für die betroffene Person beurteilt (Risikoanalyse gem. Matrix). Verzeichnet wird schliesslich, ob die verbliebenen Restrisiken "hoch" sind oder nicht. Das ist der im Rahmen einer DSFA entscheidende Punkt.	☐ Sind in einem separaten Papier dokumentiert. ☐ Liegt bei bzw. ist abrufbar: _____ ☐ Das **Restrisiko**, dass eine Person aufgrund der Datenbearbeitung trotz etwaiger Massnahmen *zu Unrecht* diese Nachteile erleidet, ist nach unserer Meinung: ☐ Hoch, und zwar in folgenden Fällen: ☐ In allen Fällen nicht bzw. nicht mehr hoch. → **1. OK** ☐ Die Datenbearbeitung ist aufgrund unserer Beurteilung **gegen folgende Bedrohungen** ungeachtet der von uns umgesetzten bzw. vorgesehenen Massnahmen (vgl. Q6 bzw. Q7) **nicht vollständig geschützt ("Verwundbarkeit")**: ☐ Die **Vertraulichkeit** der Daten wird beeinträchtigt (z.B. weil sich unbefugte Personen Zugang verschaffen könnten, oder versehentlich oder vorsätzlich Daten unbefugten Personen offenbart werden, weil Mails falsch versendet, Personen nicht richtig authentifiziert werden, unverschlüsselte Datenträger verloren gehen): ☐ Die **Integrität** der Daten wird beeinträchtigt (z.B. wenn sich unbefugte Personen Zugang verschaffen können, Daten falsch erfasst werden, Malware oder fehlerhafte Software die	

Daten manipuliert oder keine Qualitätskontrolle in der Datenbeschaffung stattfindet, Daten falsch verknüpft oder nicht hinreichend abgeglichen werden):

☐ Die **Verfügbarkeit** der Daten wird beeinträchtigt (z.B. wenn Systeme ausfallen oder nicht mehr richtig funktionieren und so der Datenzugriff gestört ist, Aufzeichnungen fehlerhaft erfolgt sind, ein Denial-of-Service-Angriff den Zugang zu den Systemen blockiert, Datenträger verloren gehen, Referenzcodes zur Identifizierung der richtigen Datensätze fehlen, Zugangscodes verloren gegangen sind, Mitarbeiter mit dem erforderlichen Know-how für den Datenzugriff nicht verfügbar sind):

☐ Die Daten werden **zweckentfremdet** oder sonst **missbräuchlich genutzt** im Unternehmen (z.B. wenn die Daten länger als nötig aufbewahrt, mehr Personen als nötig Zugang haben oder die Zweckbindung nicht sichergestellt wird):

☐ Die Nutzung der Daten kann sich **gegen die betroffene Person** auswirken (z.B. wenn die Daten sensibel oder kommerziell besonders interessant sind):

☐ Die betroffenen Personen fühlen sich **in ihrer Privatsphäre verletzt** (z.B. weil sie merken oder das Gefühl entstehen kann, dass die Datenbearbeitung nicht wirklich transparent ist):

☐ Die betroffenen Personen haben das Gefühl, dass sie **keine Kontrolle** mehr über ihre Daten haben (z.B. weil die Datenbearbeitung nicht mehr transparent ist oder ihre Rechte als betroffene Personen nicht respektiert werden):

☐ Die Datenbearbeitung betrifft eine **Person**, **die sie gar nicht erfassen sollte** (z.B. weil es zu einer Verwechslung kommt oder die Daten zu breit erfasst werden, d.h. es zu einem "Mitfang" von weiteren Personen kommt):

☐ Die Datenbearbeitung ist nicht oder nicht umfassend **dokumentiert und dokumentierbar**:

☐ **Weitere Bedrohungen**, gegen welche die Datenbearbeitung nicht ausreichend geschützt ist und deren Verwirklichung Nachteile für die betroffenen Personen haben können:

			☐ Um zu verhindern, dass eine betroffene Person aufgrund dieser Bedrohungen Nachteile erleidet, sehen wir zusätzlich zu den Massnahmen gemäss Q6 und Q7 noch **folgende Massnahmen** vor: ☐ Sind in einem separaten Papier dokumentiert. ☐ Liegt bei bzw. ist abrufbar: _____ ☐ Das **Restrisiko**, dass eine Person aufgrund der Datenbearbeitung trotz etwaiger Massnahmen aufgrund dieser Bedrohungen Nachteile erleidet, ist nach unserer Meinung: ☐ Hoch, und zwar in folgenden Fällen: ☐ In allen Fällen nicht bzw. nicht mehr hoch. → **2. OK** ☐ Wir möchten noch Folgendes vermerken:	
	Q9	**Konsultation (nur DSG)** Ergibt sich aus einer DSFA, dass die Datenbearbeitung trotz der umgesetzten oder vorgesehenen Massnahmen ein hohes Risiko für die betroffenen Personen	☐ Da die Datenbearbeitung nach unserer Meinung **kein hohes Risiko** zur Folge hat, ist keine Konsultation erforderlich. → **hier alles OK** ☐ Die Datenbearbeitung hat gemäss unserer Meinung ein **hohes Risiko** zur Folge, deshalb ist eine **Konsultation** erforderlich:	☐ In der Konsultation wurden **keine weiteren Massnahmen** empfohlen und vom EDÖB keine **Auflagen gemacht**. ☐ Es wurden **Massnahmen** empfohlen:

zur Folge hat, so muss vorgängig der Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (**EDÖB**) oder ein etwaiger eigener Datenschutzberater im Sinne vom Art. [9] DSG konsultiert werden.

Art. [21] DSG

Die Pflicht zur Konsultation soll sicherstellen, dass der EDÖB bei besonders heiklen Projekten prüfen kann, ob die erforderlichen Massnahmen wirklich identifiziert worden sind bzw. die nötigen Massnahmen tatsächlich umgesetzt werden. In der Praxis dürften Fälle, in denen es zu einer Konsultation des EDÖB kommt, sehr selten sein.

Die meisten Unternehmen werden versuchen, kein "hohes Risiko" ausweisen zu müssen, und falls doch, auf den "Datenschutzberater" ausweichen, da dieser vertraulich und rascher reagieren kann und das Unternehmen besser kennt. Die Voraussetzungen an den "Datenschutzberater" sind nicht besonders hoch.

Liegen Empfehlungen für Anpassungen der Datenbearbeitung vor, so muss das Unternehmen diesen nicht Folge leisten. Will es davon abweichen, sollte es dies jedoch begründen.

☐ Wir verfügen über einen **Datenschutzberater im Sinne von Art. [9] DSG** und haben daher ihn um seine Stellungnahme zur DSFA und der Datenbearbeitung gebeten.

☐ Seine Stellungnahme lautet zusammengefasst: → **hier alles OK**

☐ Keine Einwände.

☐ Liegt bei bzw. ist abrufbar: _____

☐ Wir haben den **EDÖB** um seine Stellungnahme zur DSFA und der Datenbearbeitung gebeten:

☐ Seine Stellungnahme lautet zusammengefasst: → **hier alles OK**

☐ Keine Einwände.

☐ Liegt bei bzw. ist abrufbar: _____

☐ Wir möchten noch Folgendes vermerken:

☐ Diese Massnahmen sollten umgesetzt werden:

☐ Diese Massnahmen sollten nicht umgesetzt werden:

Aus folgendem Grund nicht:

☐ Es wurden vom EDÖB **Auflagen gemacht**:

☐ Diese Auflagen sollten umgesetzt werden:

☐ In diesen Punkten sollten die Auflagen nicht akzeptiert und folgende weiteren Schritte unternommen werden:

					☐ Es ist eine grundsätzliche **Neubeurteilung** der Datenbearbeitung erforderlich. ☐ **Situation unklar** Grund: ☐ Weitere Abklärungen sind nötig ☐ Experte konsultieren
		Q10	**Konsultationen (nur DSGVO)** Bei der Durchführung einer DSFA ist einerseits der Rat des Datenschutzbeauftragten im Sinne von Art. 37 DSGVO einzuholen (falls es einen gibt) und andererseits, wo angezeigt, die Ansicht der betroffenen Personen oder ihrer Vertretung einzuholen. Ergibt sich aus einer DSFA, dass die Datenbearbeitung trotz der umgesetzten oder vorgesehenen Massnahmen ein hohes Risiko für die betroffenen Personen zur Folge hat, so muss vorgängig auch die zuständige Datenschutzbehörde konsultiert werden. *Art. 35 Abs. 2 und Abs. 9 DSGVO, Art. 36 DSGVO* Die Konsultationspflichten im Rahmen der DSGVO gehen wesentlich weiter als unter dem DSG. Zwar sieht auch die DSGVO vor, dass die Datenschutzbehörde zu konsultieren ist, wenn das hohe Risiko einer Datenbearbeitung sich durch Massnahmen nicht weiter reduzieren lässt; hier stimmt die DSGVO mit dem Schweizer Recht überein. Die DSGVO verlangt allerdings auch zwingend die Begrüssung des Datenschutzbeauftragten im Sinne von Art. 37 DSGVO, sowie – wo angezeigt – der	☐ Das Unternehmen hat einen **Datenschutzbeauftragten** im Sinne von Art. 37 DSGVO bestellt. Es hat ihn daher um seinen Rat mit Bezug auf die Datenbearbeitung gebeten bzw. tut dies. ☐ Seine Stellungnahme lautet zusammengefasst: → **1. OK** ☐ Keine Einwände. ☐ Liegt bei bzw. ist abrufbar: _____ ☐ Das Unternehmen hat **keinen Datenschutzbeauftragten** im Sinne von Art. 37 DSGVO bestellt. → **1. OK** ☐ Das Unternehmen hat die **Ansicht der betroffenen Personen** oder ihrer Vertretung zur Datenbearbeitung einzuholen, ausser, es sprechen Gründe dagegen.	☐ In der Konsultation wurden **keine weiteren Massnahmen** empfohlen und von der Datenschutzbehörde keine **Auflagen gemacht**. ☐ Es wurden **Massnahmen** empfohlen: ☐ Diese Massnahmen sollten umgesetzt werden: ☐ Diese Massnahmen sollten nicht umgesetzt werden: Aus folgendem Grund nicht:

betroffenen Personen oder ihrer Vertreter. Auf die Praxis umgemünzt bedeutet dies, dass das Unternehmen sich zwar entscheiden kann, die betroffenen Personen nicht anzuhören, wird dann aber die Gründe dafür dokumentieren müssen.

Dasselbe gilt auch in der rechten Spalte: Soll einer Empfehlung nicht Folge geleistet werden, muss dokumentiert werden, warum dem so ist.

Zu beachten ist, dass eine DSFA nicht vom Datenschutzbeauftragten im Sinne von Art. 37 DSGVO durchgeführt wird. Er berät das Unternehmen lediglich. Die Verantwortung liegt bei letzterem.

☐ Folgende Personen wurden wie folgt befragt (inkl. Angaben, wie diese ermittelt wurden, wo dies nicht offenkundig ist):

☐ Ihre Stellungnahme lautet zusammengefasst: → **2. OK**

☐ Keine Einwände.

☐ Liegt bei bzw. ist abrufbar: _____

☐ Das Unternehmen **verzichtet** auf das Einholen der Ansichten der betroffenen Personen, und zwar deshalb: → **2. OK**

☐ Vertraulichkeit des Vorhabens ist nicht gewährleistet.

☐ Das Vorhaben muss zu kurzfristig realisiert werden.

☐ Sinnvolle Befragung nicht möglich oder mit einem unverhältnismässigen Aufwand verbunden.

☐ Keine einigermassen einheitliche Position zu erwarten.

☐ Der Inhalt der Stellungnahme der betroffenen Personen ist absehbar.

☐ Anderer Grund:

☐ Es wurden von einer Datenschutzbehörde **Auflagen gemacht**:

☐ Diese Auflagen sollten umgesetzt werden:

☐ In diesen Punkten sollten die Auflagen nicht akzeptiert und folgende weiteren Schritte unternommen werden:

☐ Es ist eine grundsätzliche **Neubeurteilung** der Datenbearbeitung erforderlich.

☐ **Situation unklar**

Grund:

☐ Weitere Abklärungen sind nötig

☐ Experte konsultieren

☐ Die Datenbearbeitung hat gemäss vorliegender Analyse ein **hohes Risiko** für die betroffenen Personen zur Folge, weshalb das Unternehmen die zuständige(n) Datenschutzbehörde(n) konsultiert bzw. konsultiert hat:

- ☐ Folgende Behörde(n) wurde(n) konsultiert (und Angabe, warum diese Behörde(n), wo dies nicht offenkundig ist):

- ☐ Seine (bzw. ihre) Stellungnahme(n) lautet zusammengefasst: → **3. OK**

  - ☐ Keine Einwände.
  - ☐ Liegt bei bzw. ist abrufbar: _____

☐ Wir möchten noch Folgendes vermerken:

Weitere Bemerkungen:

Risikobeurteilung

Prozessowner: _____

Prozessowner	Datenschutzstelle
Wir sind der Ansicht, dass die in der DSFA identifizierten Restrisiken der oben beurteilen Datenbearbeitung für die betroffenen Personen in Anbetracht des Interesses an der Datenbearbeitung gerechtfertigt sind ☐ Ja ☐ Nein Die Datenbearbeitung sollte: ☐ nicht umgesetzt, sondern neu überdacht werden ☐ umgesetzt werden ☐ umgesetzt werden, aber mit folgenden Anpassungen: ☐ Die Datenbearbeitung sollte ins Risikoinventar aufgenommen werden	Wir erachten die oben durchgeführte DSFA als vertretbar ☐ Ja ☐ Nein Wir teilen die Ansicht des Prozessowners, wie weiter verfahren werden sollte ☐ Ja ☐ Nein Begründung: Wir schlagen folgende Massnahmen vor: ☐ Die Datenbearbeitung wird ins Risikoinventar aufgenommen

Stellungnahme des Prozessowners zur Beurteilung der Datenschutzstelle:

Die damit verbundenen Risiken (soweit vorhanden) werden von ihm akzeptiert: ☐ Ja ☐ Nein Datum, Name: _____