Kompetenzzentrum
Sicheres Österreich

Datenschutz-Reifegrad

Schema 2024

Versionskontrolle

Version	Datum	Freigabe
0.1	12. Feber 2024	Datenschutz Advisory Board
1.0	13. März 2024	Datenschutz Advisory Board

Inhaltsverzeichnis

1 Einführung

Organisationen, die personenbezogene Daten nach DSGVO verarbeiten, sind rechtlich verpflichtet, hinsichtlich des Umgangs mit Lieferanten (Dritten) entsprechende Datenschutzvorkehrungen zu treffen. Für jede Organisation, die die Vertrauenswürdigkeit ihrer Lieferanten (Dritten) hinsichtlich des Datenschutzes prüfen will, stellt das Datenschutz-Rating eine effiziente und effektive Methode zur Ergänzung der Auswahlsorgfalt dar.

Der Datenschutz-Reifegrad wird im Datenschutz-Rating abgebildet und ist ein Schema zur Einschätzung des ersten Risikos (Reifegradbestimmung), ob Organisationen (Unternehmen, Vereine, etc.) aus datenschutzrechtlicher Sicht zum Zeitpunkt der Validierung aufgrund ihrer Selbstdeklaration grundsätzlich als „vertrauensvoll“ oder „nicht vertrauensvoll“ betrachtet werden können. Das vorliegende Dokument beschreibt die relevanten Aspekte der Reifegradbestimmung.

Das Datenschutz-Rating wird auf Grundlage der Validierung erstellt. Es gibt zunächst Auskunft, ob die Selbstdeklaration der Organisation die Mindestanforderungen für das Datenschutz-Rating erfüllt. Wenn die Validierung im Hinblick auf die Mindestanforderungen positiv ausfällt, gibt das Datenschutz-Rating darüber hinaus Auskunft, in welchem Reifegrad die Anforderungen für das Datenschutz-Rating nach der Selbstdeklaration der Organisation umgesetzt sind. Dies drückt sich in einer ersten Risikoeinschätzung aus, ob eine Organisation aufgrund der getätigten Antworten in der Selbstdeklaration zum Zeitpunkt der Validierung grundsätzlich als „vertrauensvoll“ oder „nicht vertrauensvoll“ betrachtet werden kann. Die Kennzahl des Datenschutz-Ratings kann einen Wert zwischen 100 und 700+ annehmen.

Das Dokument basiert auf den Vorschriften der Datenschutzgrundverordnung (DSGVO) (siehe Anhang C: Begriffsbestimmungen).

Zielsetzung von Reifegradbestimmungen ist die Bildung von Vertrauen in die bewerteten Organisationen. Eine Reifegradbestimmung zielt darauf ab, die Erfüllung definierter Anforderungen zum Bewertungsobjekt (einer Organisation) darzulegen. Der Wert einer solchen Beurteilung wird bestimmt vom Vertrauen, das in die zugehörige Reifegradbestimmung gesetzt wird. Dieses umfasst unter anderem die **Anforderungen** selbst, die **Überprüfungsmethoden (Validierung)** sowie die **Steuerungsmechanismen** zur Prüfung und Weiterentwicklung der Reifegradbestimmung.

Das Datenschutz-Rating kann eine konkrete datenschutzrechtliche Prüfung für den Einzelfall sowie ggf. Audits nicht ersetzen und stellt keine Zertifizierung dar. Dem Datenschutz-Rating kann insbesondere kein Aussagegehalt darüber entnommen werden, ob Datenverarbeitungen, die von einer Organisation vorgenommen werden, rechtmäßig im Sinne der DSGVO erfolgen. Auch bei Organisationen, die zum Zeitpunkt der Validierung über einen hohen Reifegrad und somit über ein „geringes“ Risiko verfügen, können insbesondere „Data Breaches“ oder ähnliche Datenschutzverletzungen auftreten.

2 Grundlegende Prinzipien und Ziele

Die grundlegenden Werte des Datenschutz-Reifegrads sind Sicherheit und Vertrauen, ebenso wie Offenheit, Transparenz und Nachvollziehbarkeit. Der Datenschutz-Reifegrad soll Vertrauen in die bewertete Organisation erzeugen, dass diese das Thema Datenschutz ernst nimmt und in angemessener Weise behandelt. Durch Offenlegung des Datenschutz-Reifegrads und der damit zusammenhängenden Kriterien und Bewertungsmethoden (Validierung) soll sichergestellt werden, dass dies in einer offenen, transparenten und nachvollziehbaren Art und Weise geschieht.

Speziell die Anforderungen für das Datenschutz-Rating (siehe Anhang A: Anforderungen) stellen Basisanforderungen an den Datenschutz dar, die jede Organisation bei der Verarbeitung personenbezogener Daten erfüllen muss. Zielsetzung ist es auch, durch die Einführung und Verbreitung des Datenschutz-Ratings in den internationalen Lieferketten eine Verbesserung des Datenschutzes zu erreichen.

Eine starke Verbreitung von Organisationen mit einem guten Datenschutz-Reifegrad ist somit eine positive Aussage über die Einhaltung der Datenschutzvorschriften nach der DSGVO.

3 Umfang

Das Datenschutz-Rating bzw. der Datenschutz-Reifegrad beziehen sich immer auf eine konkrete Organisation, definiert durch eine Firmenbuchnummer (oder äquivalentes). Die Beantwortung der Fragen bzw. Anforderungen für das Datenschutz-Rating beziehen sich auf den Wirkungskreis der eigenen Organisation, das heißt die Systeme, Prozesse und Mitarbeiter, die unter der eigenen Kontrolle der Organisation stehen.

4 Datenschutz-Reifegrad Schema

Das vorliegende Datenschutz-Reifegrad Schema beschreibt die Anforderungen für das Datenschutz-Rating, deren Erfüllung im Rahmen der Validierung zu bestätigen ist, sowie die Prüfmethoden und erforderlichen schriftlich zu formulierenden Nachweise, die zur objektiven Bewertung der Erfüllung bzw. Nichterfüllung herangezogen werden.

Der Datenschutz-Reifegrad unterscheidet in der Bewertung (Validierung) zwischen MUSS-Anforderungen (Anforderungen, die gemäß DSGVO unbedingt eingehalten werden müssen; „Mindestanforderungen“) und sogenannten KANN-Anforderungen, die eine Steigerung der Qualität des Reifegrades zum Ausdruck bringen.

4.1 Reifegrad

Der Reifegrad bewertet den Anspruch eines **Basisdatenschutzniveaus** einer Organisation. Die definierten datenschutzrechtlichen Anforderungen beziehen sich auf ein grundlegendes Schutzniveau, das von jeder Organisation (auch von kleinen) eingehalten werden muss. Die gestellten datenschutzrechtlichen Anforderungen und die verlangten Nachweise in

schriftlicher Form sind dementsprechend allgemein gehalten, erfordern aber dennoch eine definierte Mindestqualität.

4.2 Verifiziertes Assessment

Die Bewertungsmethode (Validierung) ist eine **Selbstdeklaration** der Organisation. Es handelt sich demnach um eine erste Konformitätsprüfung. Die Organisationen bewerten hierbei selbst, inwiefern sie die vom Datenschutz-Reifegrad Schema definierten datenschutzrechtlichen Anforderungen (siehe Anhang A: Anforderungen) erfüllen und dies anhand der definierten Nachweise (Evidenzen in schriftlicher Form) im Bedarfsfall auch nachweisen können. Um die Nachvollziehbarkeit und Plausibilisierung der Selbstbewertung zu gewährleisten, müssen die Organisationen zu jeder Frage eine Beschreibung abgeben, wie jede Anforderung in der Organisation konkret erfüllt ist und welche Evidenzen dazu im Bedarfsfall vorgelegt werden können.
Im Rahmen der Validierung der vorgelegten Selbstdeklarationen wird von einem qualifizierten Validierer (für die Mindestanforderungen an Validierer siehe

Anhang B: Qualifikationen) eine Bewertung der Beschreibungen vorgenommen, inwiefern diese die gestellten Anforderungen erfüllen. Sollte eine Beschreibung unvollständig oder unklar sein oder Fragen bezüglich der Erfüllung offenlassen, so erfolgt eine Rückmeldung des Validierers an die Organisation zur Klärung.

Diese Rückmeldung ist innerhalb von zwei Wochen seitens der Organisation zu beantworten. Sollte die geforderte Beantwortung unterbleiben oder die Klarstellung nicht in der erforderlichen Qualität erfolgen, so wird die gegenständliche Frage (bzw. Anforderung) als nicht erfüllt bewertet. Spätere Klarstellungen können nur im Rahmen einer gänzlich neuen Validierung vorgenommen werden. Auf Basis der final validierten Selbstdeklaration wird der Datenschutz-Reifegrad berechnet und gemeinsam mit den zugrundliegenden Detailinformationen dem Auftraggeber mitgeteilt. Das Rating wird weiters in der Rating-Datenbank von KSV1870 Nimbusec GmbH gespeichert.

Sollte sich herausstellen, dass im Rahmen der Selbstdeklaration vorsätzlich oder grob fahrlässig Falschangaben gemacht wurden, treten die im Kapitel 4.5 beschriebenen Maßnahmen in Kraft.

4.3 Gültigkeitsdauer

Das Datenschutz-Rating hat eine Gültigkeitsdauer von **einem Jahr** ab Abschluss der Validierung.

4.4 Erneuerungsprozess

Inhaber des Datenschutz-Ratings werden 1 Monat vor Ablauf der Gültigkeit daran erinnert, den verifizierten Assessment-Prozess erneut zu durchlaufen. Für eine durchgängige Gültigkeit des Datenschutz-Ratings mit demselben Stichtag ist ein Abschluss des erneuten Datenschutz-Ratings in einer Periode bis zu 4 Wochen *vor* und 8 Wochen *nach* dem

Gültigkeitsstichtag zulässig. Wenn das Rating 8 Wochen nach dem Gültigkeitsstichtag noch nicht erneuert ist, wird es in der Datenbank auf *inaktiv* (grau) gesetzt; wenn es 6 Monate nach dem Gültigkeitsstichtag noch nicht erneuert ist, wird es aus der Datenbank gelöscht.

Bei einer Erneuerung des Datenschutz-Ratings kann dieses als *Delta-Betrachtung* durchgeführt werden. Die validierte Organisation kann sich – aufbauend auf den im Vorjahr gemachten Angaben – darauf beschränken, allfällige Änderungen gegenüber den im Vorjahr gemachten Angaben bekannt zu geben. Bei Veränderungen des vorliegenden Datenschutz-Reifegrad bzw. Anpassungen der Anforderungen für das Datenschutz-Rating oder der Definitionen der Anforderungskriterien muss jedenfalls auf die neuen / geänderten Anforderungen in der Beantwortung eingegangen werden. Wenn sich weder in der Organisation noch bei dem Datenschutz-Reifegrad etwas verändert hat, kann die Beantwortung des Vorjahres fortgeschrieben werden, muss jedoch erneut bestätigt und validiert werden.

4.5 Überprüfungs-Audits und Zurückziehung von Ratings

Der Wert einer Reifegradbestimmung bemisst sich an dem Vertrauen, das in diese gesetzt wird. Dafür werden die oben beschriebenen Prüfmechanismen nach bestem Wissen und Gewissen eingesetzt. Kein Bewertungsschema (Reifegrad) kann jedoch eine hundertprozentige Aussage zum tatsächlichen Status Quo in einer Organisation treffen. Im Zuge der Validierung wird kein Audit vorgenommen, um die Angaben der Organisationen in der Selbstdeklaration auf ihre tatsächliche Richtigkeit zu kontrollieren. Die Validierung ist daher auf die wahrheitsgemäßen Angaben der Organisationen angewiesen.

Wenngleich bei der Validierung keine Audits vorgenommen werden, verpflichtet sich grundsätzlich jede Organisation, die sich einem Datenschutz-Rating unterzieht, bereits vorab, einem allfälligen Überprüfungs-Audit zuzustimmen. Überprüfungs-Audits können notwendig werden, wenn es einen schwerwiegenden Datenschutzvorfall bei einer validierten Organisation gegeben hat oder wenn es Verdachtsmomente zu Missbrauch oder Falschinformationen gibt. Weiters können Überprüfungs-Audits stichprobenartig ohne Angabe von Gründen durchgeführt werden. Die Entscheidung über die Durchführung und die Beauftragung eines Überprüfungs-Audits liegt bei KSV1870 Nimbusec GmbH.

Sollte die Abweichung im Datenschutz-Rating zwischen Selbstdeklaration und Überwachungs-Audit signifikant sein, dann wird das Datenschutz-Rating *entzogen* und ein neues Ratingverfahren kann frühestens nach einer Cool-Off-Periode von 6 Monaten – auf Kosten der Organisation – erneut durchgeführt werden. In der Zwischenzeit wird in der Rating-Datenbank das Rating der Organisation als „Zurückgezogen“ gekennzeichnet. Weiters werden alle Organisationen, die in den letzten 12 Monaten das Datenschutz-Rating der betroffenen Organisation angefordert hatten, über den Status „Zurückgezogen“ des zugehörigen Ratings informiert. Wenn das Datenschutz-Rating zurückgezogen wird, muss dieses insbesondere innerhalb von Monatsfrist von allen Webseiten und Unterlagen der Organisation entfernt werden.

5 Steuerung des Datenschutz-Reifegrad Schemas

Der Urheber des Datenschutz-Reifegrad Schemas ist das **Datenschutz Advisory Board** und stellt das Schema dem **Kompetenzzentrum Sicheres Österreich** (KSÖ) als neutralem und überparteilichem Verein, der der Erhöhung des Datenschutzes in Österreich verpflichtet ist, zur Verfügung. Das **Datenschutz Advisory Board** setzt sich aus ausgewählten Personen verschiedener Organisationen unterschiedlicher Branchen zusammen. Diese sind fachlich qualifiziert und nehmen in ihrem jeweiligen Organisationen eine verantwortliche Rolle zum Thema Datenschutz ein (beispielsweise in der Rolle des Datenschutz-beauftragten). Sie bringen ihre Erfahrung und ihr Know-How zur Gestaltung und Weiterentwicklung des Datenschutz-Reifegrad Schemas ein, um dieses bestmöglich an die datenschutzrechtlichen Vorschriften auszurichten. Der Beschluss über die Annahme des Datenschutz-Reifegrad Schemas erfolgt durch das **Datenschutz Advisory Board**.

6 Durchführung des Datenschutz-Ratings

Grundsätzlich kann sich jede Organisation einem Datenschutz-Rating unterziehen. Die Organisation kann dies selbst beauftragen oder es kann von einer anderen Organisation angefordert werden (zum Beispiel im Rahmen einer Lieferantenüberprüfung).

6.1 Ablauf der Anforderung eines Datenschutz-Ratings

Wenn eine Organisation das Datenschutz-Rating einer anderen Organisation anfordert (zum Beispiel im Rahmen seines Lieferantenrisikomanagements), so erhält die betroffene Organisation in der Regel eine E-Mail mit der Bitte, an dem verifizierten Assessment zur Erstellung des Datenschutz-Ratings mitzuwirken. Der Name der anfordernden Organisation kann dabei offengelegt werden. KSV1870 Nimbusec GmbH bemüht sich nach besten Möglichkeiten, den geeigneten Ansprechpartner zu identifizieren und diesem den Zweck und die Notwendigkeit sowie den Ablauf zu erklären:

- Wenn die Organisation mit der Mitwirkung an dem verifizierten Assessment einverstanden ist, erhält sie einen Link zur Plattform von KSV1870 Nimbusec GmbH und der weitere Ablauf erfolgt, wie im Kapitel 4 beschrieben. Die Organisation beantwortet alle Anforderungen für das Datenschutz-Rating nach bestem Wissen und Gewissen und beschreibt zu jeder beantworteten Frage kurz, aber präzise und wahrheitsgemäß die Art der Umsetzung.
- Sofern auch nach dreimaligen telefonischen und elektronischen Kontaktversuchen keine oder eine abschlägige Antwort durch das Unternehmen erfolgt, sendet KSV1870 Nimbusec GmbH als letzte Maßnahme einen eingeschriebenen Brief an die Organisation mit Darlegung der Sachlage und Bitte, der Aufforderung nachzukommen. Erfolgt auch auf dieses Schreiben innerhalb von zwei Wochen keine positive Reaktion, dann erhält die Organisation ein „Null-Rating“.

Der Rating Owner (Eigentümer) des Datenschutz-Ratings ist KSV1870 Nimbusec GmbH.

6.2 Voraussetzungen für ein Datenschutz-Rating

Folgende Informationen müssen von einer Organisation, die sich einem Datenschutz-Rating unterzieht, verpflichtend angegeben werden:

- Eindeutige Identifikation der bewerteten Organisation (Name, Sitz der Organisation, Firmenbuchnummer bzw. Vereinsnummer o.ä.)
- Ansprechpartner in der Organisation (Name, Funktion, Telefon, E-Mail)

7 Sicherheit der verarbeiteten Daten

Sicherheits- und Risikobewertungen von Organisationen stellen schützenswerte Daten dar. Dementsprechend werden zum Schutz dieser Daten von allen Beteiligten des Datenschutz-Ratings entsprechend hohe Sicherheitsmaßnahmen eingehalten.

Die gesamte Kommunikation mit der bewerteten Organisation erfolgt verschlüsselt (sofern die Organisation dies unterstützt):

- über TLS verschlüsselte Webseiten bzw.
- über S/MIME verschlüsselte E-Mails.

8 Anhang A: Anforderungen

8.1 Anforderungen für das Datenschutz-Rating

Anforderung	Anforderungskriterien
Haben Sie einen Ansprechpartner für Datenschutzangelegenheiten?	**Geben Sie an, ob es in Ihrem Unternehmen eine oder mehrere Personen gibt, die konkret als Ansprechpartner für Datenschutzangelegenheiten fungieren.**
Ist Ihr Ansprechpartner für Datenschutzangelegenheiten bei einer europäischen Datenschutzbehörde gemeldet?	**Haben Sie einen freiwilligen oder verpflichtenden Datenschutzbeauftragten, der bei einer europäischen Datenschutzbehörde offiziell gemeldet wurde? Sofern Sie ein Unternehmen mit Sitz außerhalb der EU/EWR sind, geben Sie bekannt, ob Sie einen Vertreter iSd Art. 27 DSGVO bekannt gegeben haben?**
Haben Sie ein Verarbeitungsverzeichnis, das regelmäßig überprüft wird?	**Gibt es eine Übersicht über alle Verarbeitungstätigkeiten mit personenbezogenen Daten (Daten, die einer natürlichen Person zuordenbar sind; iSd Art. 4 DSGVO). Mit „Verarbeitungstätigkeit“ in diesem Zusammenhang werden jegliche Maßnahmen gemeint, die mit diesen personenbezogenen Daten durchgeführt werden. Hierbei kann es sich um eine Liste von Verarbeitungstätigkeiten handeln, zu deren Erfüllung die Verarbeitung von personenbezogenen Daten erforderlich ist. In dieser Liste sind z.B. der Zweck der Verarbeitung, die Daten/Datenkategorien, Empfänger/Empfängerkategorien, Angaben zu Löschfristen (soweit möglich) und Datensicherheitsmaßnahmen anzuführen?**
Haben Sie einen im Unternehmen festgelegten Aktualisierungs- und Reviewprozess für Ihr Verarbeitungsverzeichnis?	**Beschreiben Sie, wie das Verarbeitungsverzeichnis aktuell gehalten wird. Weiters bitten wir um Angabe, wer Bearbeitungen vornehmen darf und wie sichergestellt ist, dass Änderungsbedarf den zuständigen Personen mitgeteilt wird. Gibt es eine regelmäßige bzw. periodische Überprüfung?**
Haben Sie technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten implementiert?	**Es bedarf technischer und organisatorischer Maßnahmen (sogenannte TOM) um sicherzustellen, dass der Schutz personenbezogener Daten gewährleistet ist. Technische Maßnahmen können beispielsweise sein: Technische Zugangs- und Zugriffskonzepte, Pseudonymisierung, Verschlüsselung, automatisierte Löschroutinen, etc. Organisatorische Maßnahmen können beispielsweise sein: Passwort-Policy, Schulungen, Weisungen, Verträge, Verschwiegenheitsverpflichtungen etc.**
Können Sie uns Beispiele für Maßnahmen nennen, wie Sie die Integrität von personenbezogenen Daten sicherstellen?	**Integrität bedeutet den Schutz vor unautorisierten Änderungen von Informationen (Schutz vor ungewollter Veränderung), sowie die Verlässlichkeit (Schutz der Korrektheit) und Vollständigkeit (Schutz vor Verlust) von Informationen.**
Können Sie uns Beispiele für Maßnahmen nennen, wie Sie die Vertraulichkeit von personenbezogenen Daten sicherstellen?	**Vertraulichkeit bedeutet, dass personenbezogene Daten nur dem Personenkreis zugänglich gemacht werden dürfen, die befugt sind darauf zuzugreifen. Die Befugnis ergibt sich aus der Erforderlichkeit zur Aufgabenerfüllung einer jeweiligen Funktion („need-to-know-Prinzip“).**
Können Sie uns Beispiele für Maßnahmen nennen, wie Sie die Verfügbarkeit von personenbezogenen Daten sicherstellen?	**Verfügbarkeit bedeutet, dass personenbezogene Daten vereinbarungsgemäß zur Verfügung stehen müssen. Dies unabhängig davon, ob es zu technischen Einschränkungen (Datensicherheitsvorfällen, Angriffe auf das technische System etc.) kommt oder zuständige Personen greifbar sind (Urlaube, Krankenstände, Vertretungsregelungen etc.).**

Können Sie uns Beispiele für Maßnahmen nennen, wie Sie die Belastbarkeit Ihrer Datenverarbeitungssysteme sicherstellen?	**Belastbarkeit von Systemen bedeutet, dass diese gegen Cyber-Angriffe geschützt sein müssen (inkl. Ausfallsicherheit). Ziel ist es in solchen Fällen weiterhin eine rechtskonforme Verarbeitung von personenbezogenen Daten zu gewährleisten.**
Sind Sie bereit eine Auftragsverarbeitervereinbarung abzuschließen, deren Inhalte über die gesetzlichen Mindestanforderungen hinausgehen?	**Art. 28 DSGVO sieht als Mindestinhalt vor: Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen, Pflichten und Rechte des Verantwortlichen. Mögliche Erweiterungen wären beispielsweise Vertragsstrafen bei grob fahrlässigen oder vorsätzlichen Verstößen gegen die DSGVO.**
Lassen Sie Datenschutzaudits zu?	**Erklären Sie in welchem Umfang, welchen zeitlichen Abständen und mit welcher Vorlaufzeit Sie Ihrem Vertragspartner ein Einsichtsrecht gewähren.**
Verfügt Ihr Unternehmen über ein Löschkonzept?	**Daten dürfen nur so lange gespeichert werden, wie es dem Verarbeitungszweck entspricht und/oder andere gesetzliche Vorgaben bestehen, die eine Speicherung vorsehen.**
Können Sie Kundendaten nach Vorgabe innerhalb der laufenden Vertragsbeziehung löschen?	**Auf einen Löschauftrag muss flexibel reagiert werden können. D.h. es muss die Möglichkeit bestehen, dass Daten spezifisch herausgefiltert und unwiederbringlich gelöscht werden. Eine Anonymisierung kann – je nach vertraglicher Vereinbarung – an dieser Stelle nicht ausreichen. Differenzieren Sie daher in Ihrer Antwort.**
Können Sie Kundendaten nach Beendigung des Vertragsverhältnisses nach Wahl löschen und/oder in einem gängigen maschinenlesbaren Format zurückgeben?	**Können Sie nach dem Ende der Vertragsbeziehung – je nach Wahl des Vertragspartners – die Daten unwiederbringlich löschen und/oder in einem gängigen maschinenlesbaren Verfahren (z.B. CSV-Datei oder XML-Format) zur Verfügung stellen?**
Existieren Regelungen zur datenschutzkonformen Vernichtung von Datenträgern bzw. Dokumenten?	**Es ist erforderlich, dass in Ihrem Unternehmen eine Vorgehensweise angewandt wird, die sicherstellt, dass Datenträger bzw. Dokumente endgültig vernichtet werden (z.B. Schredder, Datentonnen).**
Können Sie sicherstellen, dass im Fall des Einsatzes eines (Sub-) Auftragsverarbeiters die Anforderungen der DSGVO eingehalten werden?	**Geben Sie Daten, die Sie vom Auftraggeber erhalten, an Subauftragnehmer weiter? Es muss in diesem Fall zwischen Ihnen und dem Subauftragsverarbeiter eine Auftragsverarbeitervereinbarung geben, die die gleichen Anforderungen erfüllt wie Ihre Auftragsverarbeitervereinbarung mit Ihrem Auftragsgeber.**
Können Sie sicherstellen, dass im Fall eines Transfers personenbezogener Daten in ein Land außerhalb der EU/EWR die datenschutzrechtlichen Anforderungen eingehalten werden?	**Ein Transfer personenbezogener Daten in ein sogenanntes Drittland liegt beispielsweise vorbei:** • **Unternehmenssitz außerhalb der EU/EWR (sofern kein Angemessenheitsbeschluss iSd Art. 45 DSGVO vorhanden ist)Serverstandort außerhalb der EU/EWR (sofern kein Angemessenheitsbeschluss iSd Art. 45 DSGVO vorhanden ist)** • **Übermittlung an „Dritte“, z.B. Subauftragsverarbeiter, gemeinsam Verantwortlicher etc. außerhalb der EU/EWR (sofern kein Angemessenheitsbeschluss iSd Art. 45 DSGVO vorhanden ist)**

	• **Konzernmutter außerhalb der EU/EWR (sofern kein Angemessenheitsbeschluss iSd Art. 45 DSGVO vorhanden ist)** **Oft liegt Drittstaatenbezug beispielsweise beim Einsatz von Cloud-Lösungen oder eines Call-Centers im Ausland vor.**
Sind alle Datentransfers in die USA über Standard Contractual Clauses und ergänzende Maßnahmen und/oder Zertifizierung nach dem EU-U.S. Data Privacy Framework abgedeckt?	**In dieser Frage sollen Datentransfers in die USA zusätzlich speziell evaluiert werden. Wenn kein Datentransfer in die USA vorliegt, klicken Sie „Ja“ an und erläutern Sie dies unten im Erklärungstext.**
Wird regelmäßig überprüft, dass diese datenschutzrechtlichen Anforderungen im Zusammenhang mit Drittstaatentransfers eingehalten werden?	**Erläutern Sie, wie die Einhaltung dieser Anforderungen überprüft wird. Die Überprüfung der Anforderungen muss nachweislich belegt werden können, beispielsweise durch Spot-Checks, Audit-Kataloge, Lieferanten-Audits, ein im Vertrag ausverhandeltes Einsichtsrecht etc.**
Werden alle Beschäftigten (inkl. Freelancer, Praktikanten etc.) hinsichtlich des Datenschutzes über ihre Pflichten und Verantwortung sensibilisiert und geschult?	**Es ist erforderlich, dass alle Personen im Unternehmen regelmäßig über ihre Pflichten und Verantwortungen sensibilisiert und geschult werden (z.B. Basisschulung, Neuigkeiten, Änderungen).**
Stellen Sie die Verschwiegenheit der Beschäftigten (inkl. Freelancer, Praktikanten etc.) über das Ausscheiden hinaus sicher?	**Es ist iSd § 6 DSG erforderlich, dass Verschwiegenheitsverpflichtungen von Personen, die mit personenbezogenen Daten arbeiten – auch über das (Arbeits-) Vertragsverhältnis hinaus – sichergestellt werden.**
Existiert ein Prozess zur Meldung von Datenschutzverletzungen?	**Eine Datenschutzverletzung nach Art. 33 DSGVO liegt z.B. vor: bei unberechtigtem Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, versehentlicher Verlust oder Veröffentlichung, Veränderung oder Zerstörung von personenbezogenen Daten.**
Gibt es zusätzliche externe Nachweise, die die Qualität des Datenschutzes darlegen?	**Wenn ja, legen Sie diese dar z.B:** • **Zertifikat einer akkreditierten Stelle** • **ISO 27701, ISO 27001** • **Code of Conduct** • **Vergleichbare anerkannte Standards**
Gibt es einen Prozess, der sicherstellt, dass für alle Verarbeitungstätigkeiten, für die die Notwendigkeit einer Datenschutz-Folgenabschätzung (DSFA) besteht, eine solche auch durchgeführt wird?	**Die DSFA zeigt auf, ob weitere Maßnahmen (zum Schutz von personenbezogenen Daten) umzusetzen sind. Als Ergebnis können abgeleitet werden: technische, organisatorische und/oder rechtliche Maßnahmen.**
Existiert ein Prozess, wie Betroffenenrechte umgesetzt werden?	**Im Sinne des Art. 12ff DSGVO muss es definierte Prozess zur Wahrung von Betroffenenrechten und zur Beantwortung von Anfragen durch Betroffene (Löschung, Auskunft, Berichtigung etc.) geben.**

9 Anhang B: Qualifikationen

9.1 Mindestanforderung an Validierer

Die Validierung der Selbstdeklarationen erfolgt durch die EPU Mag. Manfred Spanner, MSc. & die RA-Kanzlei Raabe-Stuppnig.

Mit der Validierung befasste Personen müssen mindestens ein Studium der Rechtswissenschaft oder vergleichbares wie „Wirtschaftsrecht“ an der WU-Wien (weitere Alternativen natürlich willkommen) vorlegen. Darüber hinaus müssen diese über mindestens 3 Jahre nachweisliche Erfahrung im Datenschutz verfügen.

10 Anhang C: Begriffsbestimmungen

DSGVO
Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

Schema-Owner
Schema-Owner (Eigentümer) des Datenschutz-Reifegrad Schemas ist das Datenschutz Advisory Board. Dieses ist für die Entwicklung und Instandhaltung des Datenschutz-Reifegrad Schemas verantwortlich.

Anforderungen für das Datenschutz-Rating
Eine Anforderung ist ein Erfordernis oder eine Erwartung, das oder die niedergelegt ist. Die Anforderungen für das Datenschutz-Rating bestehen aus 25 Fragen zur Umsetzung datenschutzrechtlicher Anforderungen (siehe Anhang A: Anforderungen).

Selbstdeklaration
Die Organisation bewertet selbst, ob und gegebenenfalls, inwiefern diese die Anforderungen für das Datenschutz-Rating erfüllt. Sie verfasst die Antworten auf die Anforderungen für das Datenschutz-Rating.

Validierung
Die Validierung erfolgt anhand bestimmter Anforderungskriterien (siehe Anhang A: Anforderungen in der Spalte „Anforderungskriterien“). Im Rahmen der Validierung prüft der Validierer, ob die Selbstdeklaration der Organisation den Anforderungskriterien für das Datenschutz-Rating entspricht.

Zurückziehung
Entziehung des Datenschutz-Ratings. Zu einer Entziehung kommt es insbesondere, wenn begründete Zweifel an der Stichhaltigkeit der Validierung nicht ausgeräumt werden können.