VEREINBARUNG ÜBER DIE DATENVERARBEITUNG FÜR SAP CLOUD SERVICES

(VERTRAG ÜBER DIE VERARBEITUNG VON PERSONENBEZOGENEN DATEN FÜR SAP CLOUD SERVICES)

1. HINTERGRUND

1.1 Zweck und Anwendung. Dieses Dokument ("DPA") wird in die Vereinbarung einbezogen und ist Teil eines schriftlichen (auch in elektronischer Form geschlossenen) Vertrags zwischen SAP und dem Kunden. Dieses DPA gilt für Personenbezogene Daten, die von SAP und ihren Unterauftragsverarbeitern im Zusammenhang mit der Erbringung des Cloud Services verarbeitet werden. Dieses DPA gilt nicht für von SAP zur Verfügung gestellte Nicht-Produktionsumgebungen des Cloud Service, und der Auftraggeber wird keine Personenbezogenen Daten in solchen Umgebungen speichern.

1.2 Struktur. Die Anhänge 1 und 2 sind Bestandteil dieses DPA. Sie legen den vereinbarten Gegenstand, die Art und den Zweck der Verarbeitung, die Art der Personenbezogenen Daten, die Kategorien der Betroffenen Personen und die anzuwendenden technischen und organisatorischen Maßnahmen fest.

1.3 GDPR / DSGVO. SAP und der Auftraggeber sind sich darüber einig, dass es in der Verantwortung jeder Partei liegt, die Anforderungen zu überprüfen und zu übernehmen, die durch die Datenschutz Grundverordnung 2016/679 ("DSGVO") an die Verantwortlichen und Auftragsverarbeiter gestellt werden, insbesondere in Bezug auf die Artikel 28 und 32 bis 36 der DSGVO, wenn und soweit sie auf die Personenbezogenen Daten des Auftraggebers/der Verantwortlichen anwendbar sind, die im Rahmen der Leistungserbringung verarbeitet werden. Zur Veranschaulichung sind in Anhang 3 die relevanten DSGVO-Anforderungen und die entsprechenden Abschnitte in diesem DPA aufgeführt.

1.4 Governance. SAP wird als Auftragsverarbeiter tätig und der Auftraggeber, und die Rechtspersonen, denen er die Nutzung des Cloud Service gestattet, handeln als Verantwortliche im Rahmen des DPA. Der Auftraggeber ist Einziger Kontaktpunkt und allein verantwortlich für die Einholung aller relevanten Genehmigungen, Zustimmungen und Einwilligungen für die Verarbeitung Personenbezogener Daten gemäß diesem DPA, sowie, soweit erforderlich, der Zustimmung der Verantwortlichen zum Einsatz von SAP als Auftragsverarbeiter. Soweit vom Auftraggeber Genehmigungen, Zustimmungen, Weisungen oder Einwilligungen erteilt werden, werden diese nicht nur im Namen des Auftraggebers, sondern auch im Namen anderer Verantwortlicher, die den Cloud-Service nutzen, erteilt. Wenn SAP den Auftraggeber informiert oder ihm Meldungen übermittelt, gelten diese Informationen oder Meldungen als von denjenigen Verantwortlichen erhalten, denen der Auftraggeber die Nutzung des Cloud-Service gestattet hat. Es liegt in der Verantwortung des Auftraggebers, diese Informationen und Meldungen an die entsprechenden Verantwortlichen weiterzuleiten.

2. SICHERHEIT DER VERARBEITUNG

2.1 Angemessene Technische und Organisatorische Maßnahmen. SAP hat die in Anhang 2 aufgeführten technischen und organisatorischen Maßnahmen umgesetzt und wird diese anwenden. Der Auftraggeber hat diese Maßnahmen geprüft und erklärt sich damit einverstanden, dass hinsichtlich des vom Auftraggeber in der Order Form vereinbarten Cloud-Services die Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, des Kontextes und der Zwecke der Verarbeitung Personenbezogener Daten angemessen sind.

2.2 Änderungen. SAP wendet die in Anhang 2 beschriebenen technischen und organisatorischen Maßnahmen auf alle SAP-Kunden gleichermaßen an, die im selben Rechenzentrum gehostet werden und den gleichen Cloud-Service erhalten. SAP kann die in Anhang 2 aufgeführten Maßnahmen jederzeit ohne Vorankündigung ändern, solange sie ein vergleichbares oder besseres

Sicherheitsniveau aufrechterhält. Einzelne Maßnahmen können durch neue Maßnahmen ersetzt werden, die dem gleichen Zweck dienen, ohne das Sicherheitslevel zum Schutz Personenbezogener Daten zu beeinträchtigen.

3. SAP PFLICHTEN

3.1 Weisungen des Auftraggebers. SAP wird Personenbezogene Daten nur in Übereinstimmung mit den dokumentierten Weisungen des Auftraggebers verarbeiten. Die Vereinbarung (einschließlich dieses DPA) stellt eine solche dokumentierte Erst-Weisung dar, und jede Nutzung des Cloud-Service stellt dann eine weitere Weisung dar. SAP unternimmt alle zumutbaren Anstrengungen, um allen anderen Weisungen des Auftraggebers zu folgen, soweit sie nach Datenschutzrecht erforderlich, technisch durchführbar und ohne Änderungen am Cloud-Service möglich sind. Sollte eine der vorgenannten Ausnahmen zu treffen oder SAP anderweitig einer Weisung nicht nachkommen können oder der Meinung sein, dass eine Weisung gegen das Datenschutzrecht verstößt, wird SAP den Auftraggeber unverzüglich benachrichtigen (E-Mail erlaubt).

3.2 Verarbeitung auf Basis rechtlicher Erfordernisse. SAP kann auch Personenbezogene Daten verarbeiten, sofern dies nach geltendem Recht erforderlich ist. In einem solchen Fall wird SAP den Auftraggeber vor der Verarbeitung über diese rechtliche Anforderungen informieren, es sei denn, das betreffende Recht verbietet solche Informationen wegen eines wichtigen öffentlichen Interesses.

3.3 Befugte Personen. Zur Verarbeitung Personenbezogener Daten gewähren SAP und seine Unterauftragsverarbeiter nur befugten Personen Zugang, die sich zur Vertraulichkeit verpflichtet haben. SAP und seine Unterauftragsverarbeiter werden die Personen, die Zugang zu Personenbezogenen Daten haben, regelmäßig in Bezug auf die anwendbaren Datensicherheits- und Datenschutzmaßnahmen schulen.

3.4 Kooperation. Auf Wunsch des Auftraggebers wird SAP angemessen mit dem Auftraggeber und den Verantwortlichen zusammenarbeiten, um Anfragen von Betroffenen Personen oder Aufsichtsbehörden bezüglich der Verarbeitung Personenbezogener Daten durch SAP oder einer Verletzung Personenbezogener Daten zu bearbeiten. SAP wird den Auftraggeber so bald wie zumutbar möglich über jede Anfrage informieren, die SAP von einer Betroffenen Person im Zusammenhang mit der Verarbeitung Personenbezogener Daten erhalten hat, ohne selbst auf diese Anfrage ohne weitere Weisungen des Auftraggebers zu antworten. SAP stellt Funktionen zur Verfügung, die die Fähigkeit des Auftraggebers unterstützen, Personenbezogene Daten aus dem Cloud-Service zu berichtigen oder zu löschen oder die Verarbeitung gemäß dem Datenschutzgesetz einzuschränken. Wenn eine solche Funktionalität nicht zur Verfügung gestellt wird, wird SAP gemäß den Weisungen des Auftraggebers und dem Datenschutzrecht Personenbezogene Daten berichtigen oder löschen oder deren Verarbeitung einschränken.

3.5 Meldung von Verletzungen des Schutzes Personenbezogener Daten.
SAP wird dem Auftraggeber eine Verletzung des Schutzes Personenbezogener Daten unverzüglich nach Kenntniserlangung melden und ihm angemessene und SAP vorliegende Informationen zur Verfügung stellen, um ihn bei der Erfüllung seiner Verpflichtungen zur Meldung einer Verletzung des Schutzes Personenbezogener Daten gemäß den Anforderungen des Datenschutzrechts zu unterstützen. SAP kann diese Informationen in Abschnitten zur Verfügung stellen, je nachdem, zu welchem Zeitpunkt sie verfügbar werden. Eine solche Meldung ist kein Eingeständnis des Verschuldens oder der Haftung von SAP oder dahingehend auszulegen.

3.6 Datenschutz-Folgenabschätzung. Wenn der Auftraggeber (oder seine für die Verarbeitung Verantwortlichen) gemäß Datenschutzrecht verpflichtet sind, eine Datenschutz-Folgenabschätzung oder eine vorherige Konsultation mit einer Aufsichtsbehörde durchzuführen, stellt SAP auf Wunsch des Auftraggebers diejenigen Dokumente zur Verfügung, die für den Cloud-Service allgemein verfügbar sind (z.B. dieses DPA, die Vereinbarung, Auditberichte oder

Zertifizierungen). Jede zusätzliche Unterstützung wird zwischen den Vertragsparteien einvernehmlich vereinbart.

4. DATEN-EXPORT UND LÖSCHUNG

4.1 Export und Entnahme durch den Auftraggeber. Während der Laufzeit und gemäß den Regelungen der Vereinbarung kann der Auftraggeber jederzeit auf seine Personenbezogenen Daten zugreifen. Der Auftraggeber kann seine Personenbezogenen Daten entnehmen und in einem Standardformat exportieren. Abruf und Export können technischen Beschränkungen und Voraussetzungen unterliegen. In diesem Fall werden sich SAP und Auftraggeber auf eine angemessene Methode zur Ermöglichung des Zugriffs des Auftraggebers auf die Personenbezogenen Daten verständigen.

4.2 Löschung. Vor Vertragsende kann der Auftraggeber die jeweils verfügbaren Self-Service-Export-Tools von SAP verwenden, um einen abschließenden Export der Personenbezogenen Daten aus dem Cloud Service durchzuführen (was einer Rückgabe der Personenbezogenen Daten entspricht). Der Auftraggeber erteilt SAP hiermit die Weisung, nach Vertragsende die auf den zum Hosting des Cloud Service eingesetzten Servern verbliebenen Personenbezogenen Daten innerhalb einer angemessenen Zeit gemäß dem Datenschutzrecht zu löschen (spätestens innerhalb von 6 Monaten), es sei denn, deren Aufbewahrung ist nach anwendbarem Recht erforderlich.

5. ZERTIFIZIERUNGEN UND AUDITS

5.1 Auftraggeberaudit. Der Auftraggeber oder ein von ihm beauftragter unabhängiger externer und für SAP zumutbarer Prüfer (unter Ausschluss von Prüfern, die entweder Wettbewerber der SAP sind, oder nicht angemessen qualifiziert oder unabhängig sind) können die Kontrollumgebung und die Sicherheitspraktiken von SAP im Hinblick auf die von SAP verarbeiteten Personenbezogenen Daten prüfen, wenn:

- **(a)** SAP keinen ausreichenden Nachweis über die Einhaltung der technischen und organisatorischen Maßnahmen, die die Produktivsysteme des Cloud Service schützen, erbracht hat. Dieser Nachweis kann durch (i) eine Zertifizierung über die Einhaltung von ISO 27001 oder anderer Standards (Umfang gemäß der Regelung im Zertifikat) oder (ii) einen gültigen Bericht nach ISAE 3402 und/oder ISAE 3000 oder einen anderen SOC1-3 Auditbericht erfolgen. Auf Anforderung des Auftraggebers sind die Auditberichte oder ISO-Zertifizierungen über den externen Auditor oder SAP verfügbar
- **(b)** Eine Verletzung des Schutzes Personenbezogener Daten vorliegt;
- **(c)** eine Prüfung offiziell durch eine Aufsichtsbehörde des Auftraggebers; oder
- **(d)** der Auftraggeber gemäß zwingendem Datenschutzrecht über ein direktes Auditrecht verfügt, und der Auftraggeber nur einmal binnen eines 12-Monatszeitraums auditiert, es sei den zwingendes Datenschutzrecht verlangt häufigere Audits.

5.2 Audits anderer Verantwortlicher. Jeder andere Verantwortliche darf die Kontrollumgebung und die Sicherheitspraktiken von SAP, die für die von SAP verarbeiteten Personenbezogenen Daten relevant sind, nur dann gemäß Abschnitt 5.1 überprüfen, wenn einer der in Abschnitt 5.1 genannten Fälle auf den anderen Verantwortlichen zutrifft. Eine solche Prüfung muss durch den Auftraggeber gemäß Abschnitt 5.1 durchgeführt werden, es sei denn, die Prüfung muss von dem anderen Verantwortlichen selbst nach dem Datenschutzrecht durchgeführt werden. Wenn mehrere Verantwortliche, deren Personenbezogene Daten von SAP auf der Grundlage der Vereinbarung verarbeitet werden, ein Audit erfordern, wird der Auftraggeber alle angemessenen Mittel einsetzen, um die Audits zu kombinieren und Mehrfach-Audits zu vermeiden.

5.3 Umfang des Audits. Der Auftraggeber ist verpflichtet, Audits mindestens sechzig Tage im Voraus anzukündigen, es sei denn, dass zwingendes Datenschutzrecht oder eine zuständige Datenschutzbehörde eine kürzere Frist vorschreiben. Häufigkeit und Umfang der Audits sind zwischen den Parteien vernünftig und nach Treu und Glauben einvernehmlich zu vereinbaren.

Auftraggeberaudits sind auf maximal drei Werktage beschränkt. Über solche Einschränkungen hinaus werden die Parteien aktuelle Zertifizierungen oder andere Auditberichte verwenden, um wiederholte Audits zu vermeiden oder zu minimieren. Der Auftraggeber hat SAP die Ergebnisse eines jeden Audits zur Verfügung zu stellen.

5.4 Auditkosten. Der Auftraggeber trägt die Kosten von Audits, es sei denn, ein solches Audit deckt einen wesentlichen Verstoß von SAP gegen dieses DPA auf, in diesem Fall trägt SAP die eigenen Kosten des Audits. Falls sich aus einem Audit ergibt, dass SAP ihren Verpflichtungen aus diesem DPA nicht nachgekommen ist, heilt SAP diesen Verstoß umgehend auf eigene Kosten.

6. UNTERAUFTRAGSVERARBEITER

6.1 Zulässiger Einsatz. SAP erhält hiermit eine vorherige allgemeine schriftliche Genehmigung, die Verarbeitung von Personenbezogenen Daten unter den nachfolgenden Voraussetzungen auf Unterauftragsverarbeiter zu übertragen:

(a) SAP oder SAP SE im Namen der SAP beauftragt Unterauftragsverarbeiter im Rahmen schriftlicher Verträge (einschließlich elektronischer Form), die mit den Bestimmungen dieses DPA in Bezug auf die Verarbeitung Personenbezogener Daten durch den Unterauftragnehmer übereinstimmen. SAP haftet für etwaige Verstöße durch den Unterauftragsverarbeiter gemäß den Bestimmungen dieser Vereinbarung;

(b) SAP wird die Sicherheits-, Datenschutz- und Vertraulichkeitspraktiken eines Unterauftragsverarbeiters vor dessen Auswahl bewerten, um festzustellen, dass er in der Lage ist, das in diesem DPA geforderte Schutzniveau für Personenbezogene Daten zu bieten; und

(c) Die bei Vertragsschluss gültige Liste der Unterauftragsverarbeiter der SAP wird von SAP veröffentlicht oder dem Auftraggeber auf Anfrage zur Verfügung gestellt, einschließlich des Namens, der Anschrift und der Rolle jedes Unterauftragsverarbeiters, den SAP zur Erbringung des Cloud Services einsetzt.

6.2 Neue Unterauftragsverarbeiter. Der Einsatz von Unterauftragsverarbeitern erfolgt nach Ermessen der SAP unter der Voraussetzung, dass folgende Regelungen eingehalten werden:

(a) SAP informiert den Auftraggeber im Voraus (per Email oder durch ein Posting auf dem Supportportal, das über den SAP Support bereit gestellt wird) über jegliche geplante Hinzufügungen oder Ersetzungen innerhalb der Liste der Unterauftragsverarbeiter, einsclhießlich des Namens, der Anschrift und der Rolle des neuen Unterauftragsverarbeiters; und

(b) Der Auftraggeber kann solchen Änderungen gemäß Abschnitt 6.3 widersprechen.

6.3 Widerspruch gegen neue Unterauftragsverarbeiter.

(a) Sofern der Auftraggeber gemäß Datenschutzrecht einen berechtigten Grund hat, der Verarbeitung Personenbezogener Daten durch die neuen Unterauftragsverarbeiter zu widersprechen, kann er die Vereinbarung (beschränkt auf den Cloud-Service, für den der neue Unterauftragsverarbeiter eingesetzt werden soll) durch schriftliche Erklärung gegenüber SAP mit Wirkung zu einem vom Auftraggeber festgelegten Zeitpunkt kündigen, spätestens jedoch zum Ablauf von dreißig Tagen nach dem Datum der Mitteilung von SAP an den Auftraggeber über den neuen Unterauftragsverarbeiter. Kündigt der Auftraggeber nicht innerhalb dieser Frist von dreißig Tagen, so gilt der neue Unterauftragsverarbeiter als durch den Auftraggeber genehmigt.

(b) Innerhalb der Dreißig-Tagesperiode ab dem Datum der Mitteilung von SAP an den Auftraggeber, in der der Auftraggeber über den neuen Unterauftragsverarbeiter informiert wird, kann der Auftraggeber verlangen, dass die Parteien in gutem Glauben zusammenkommen und eine Lösung des Widerspruchs besprechen. Diese Besprechungen verlängern die Kündigungsfrist nicht und berühren nicht das Recht von SAP, den/die neuen Unterauftragsverarbeiter nach Ablauf der Frist von dreißig Tagen in Dienst nehmen zu dürfen.

(c) Jede Kündigung nach diesem Abschnitt 6.3 wird von beiden Parteien als unverschuldet betrachtet und unterliegt den Bestimmungen der Vereinbarung.

6.4 Notfallaustausch. SAP kann einen Unterauftragsverarbeiter ohne vorherige Mitteilung austauschen, wenn sich der Grund für den Austausch der zumutbaren Kontrolle von SAP entzieht und der umgehende Austausch aus Sicherheits- oder anderen dringenden Gründen erforderlich ist. In diesem Fall informiert SAP den Auftraggeber über den neuen Unterauftragsverarbeiter unverzüglich nach seiner Ernennung. Abschnitt 6.3 gilt entsprechend.

7. INTERNATIONALE VERARBEITUNG

7.1 Regeln für Internationale Verarbeitung. SAP ist berechtigt, die Verarbeitung von Personenbezogene Daten unter Einbeziehung von Unterauftragsverarbeitern im Sinne dieses DPA außerhalb des Landes, in dem sich der Auftraggeber befindet unter Einhaltung des Datenschutzrechts durchzuführen.

7.2 Standardvertragsklauseln (Standarddatenschutzklauseln). Sofern (i) Personenbezogene Daten eines EWR- oder schweizerischen Verantwortlichen in einem Land ausserhalb des EWR, der Schweiz bzw. außerhalb eines Landes, einer Organisation oder eines Gebiets erfolgt, das von der Europäischen Union als sicheres Land mit einem angemessenen Datenschutzniveau gemäss Art. 45 GDPR anerkannt ist, verarbeitet werden, oder (ii) Personenbezogene Daten eines anderen Verantwortlichen international verarbeitet werden und eine solche internationale Verarbeitung ein angemessenes Mittel nach dem anwendbaren Recht des Verantwortlichen erfordert, und das angemessene Mittel durch den Abschluss von Standardvertragsklauseln erfüllt werden kann, gilt:

(a) SAP und der Auftraggeber vereinbaren die Geltung der Standardvertragsklauseln;

(b) Der Auftraggeber vereinbart die Standardvertragsklauseln mit jedem relevanten Unterauftragsverarbeiter wie folgt: (i) Der Auftraggeber tritt als unabhängiger Inhaber von Rechten und Pflichten den Standardvertragsklauseln bei, die zwischen SAP oder SAP SE und dem Unterauftragsverarbeiter vereinbart wurden („Beitrittsmodell") oder (ii) der Unterauftragsverarbeiter (vertreten durch SAP) vereinbart die Standardvertragsklauseln mit dem Auftraggeber ("Vollmachtsmodell"). Das Vollmachtsmodell gilt, wenn und soweit SAP ausdrücklich über die Liste der Unterauftragsverarbeiter gemäß Abschnitt 6.1(c) oder über eine Mitteilung an den Auftraggeber erklärt hat, dass dieses Modell für einen Unterauftragsverarbeiter verfügbar ist; und/oder

(c) Andere Verantwortliche, denen der Auftraggeber die Nutzung des Cloud Service gemäß der Vereinbarung gestattet, können ebenfalls die Standardvertragsklauseln mit SAP und/oder den relevanten Unterauftragsverarbeitern in gleicher Weise wie der Auftraggeber gemäß den obigen Abschnitten 7.2 (a) und (b) vereinbaren. In diesen Fällen vereinbart der Auftraggeber die Standardvertragsklauseln im Namen der anderen Verantwortlichen.

7.3 Bezug zwischen Standardvertragsklauseln und Vereinbarung. Keine der Bestimmungen in der Vereinbarung darf bei widersprüchlichen Regelungen dahingehend ausgelegt werden, dass sie Vorrang vor einer Bestimmung der Standardvertragsklauseln hat. Zur Klarstellung: Wo dieses DPA Regelungen für Audit und Unterauftragsverarbeiter in den Abschnitten 5 und 6 näher beschreibt, gelten diese Regelungen auch in Bezug auf die Standardvertragsklauseln.

7.4 Für die Standardvertragsklauseln geltendes Recht. Die Standardvertragsklauseln unterliegen dem Recht des Landes, in dem der Verantwortliche seinen Sitz hat.

8. DOKUMENTATION; VERARBEITUNGSVERZEICHNIS

Jede Partei ist für die Einhaltung ihrer Dokumentationspflichten verantwortlich, insbesondere für die Führung von Verarbeitungsverzeichnissen, soweit dies nach dem Datenschutzrecht erforderlich ist. Jede Partei unterstützt die andere Partei in angemessener Weise bei der Erfüllung von deren Dokumentationspflichten, einschließlich der Bereitstellung der Informationen, die die andere Partei von ihr benötigt, in einer von der anderen Partei in angemessener Weise angeforderten Form (z. B. durch

die Verwendung eines elektronischen Systems), damit die andere Partei den Verpflichtungen im Zusammenhang mit der Führung von Verarbeitungsverzeichnissen nachkommen kann.

9. EU ACCESS (EU ZUGRIFF)

9.1 **Optionaler Service.** EU Access ist ein optionaler Service, der von SAP angeboten werden kann. SAP wird den Cloud Service, für den EU Access verfügbar ist, ausschließlich für die Produktivinstanzen gemäß den Regelungen dieses Abschnitts 9 erbringen. Soweit EU Access nicht in der Order Form explizit angegeben und vereinbart ist, ist dieser Abschnitt 9 nicht anwendbar.

9.2 **EU Access.** SAP wird ausschließlich europäische Unterauftragsverarbeiter für Supportleistungen einsetzen, die den Zugriff auf Personenbezogene Daten im Cloud-Service erfordern, und SAP wird keine Personenbezogenen Daten außerhalb des EWR oder der Schweiz exportieren, es sei denn, der Auftraggeber hat ausdrücklich fallweise schriftlich zugestimmt (E-Mail erlaubt), oder einer der in Abschnitt 9.4 genannten Fälle liegt vor.

9.3 **Standort von Rechenzentren.** Zum Wirksamkeitsdatum der Vereinbarung befinden sich die Rechenzentren, auf deren Servern die Personenbezogenen Daten im vereinbarten Cloud Service gehostet werden, innerhalb des EWR oder der Schweiz. SAP darf die Auftraggeber-Instanz ohne die vorherige schriftliche Zustimmung des Auftraggebers (E-Mail ist zulässig) nicht in ein außerhalb der EWR oder der Schweiz befindliches Rechenzentrum auslagern. Sollte SAP die Migration der Auftraggeber-Instanz in ein Rechenzentrum innerhalb des EWR oder in die Schweiz planen, setzt SAP den Auftraggeber spätestens dreißig (30) Tage vor der geplanten Migration schriftlich (E-Mail ist zulässig) davon in Kenntnis

9.4 **Ausschlüsse.** Die folgenden Personenbezogenen Daten unterliegen nicht den Abschnitten 9.2 und 9.3:

- **(a)** Kontaktangaben des Absenders einer Supportmeldung;
- **(b)** Jegliche anderen vom Auftraggeber beim Aufgeben einer Supportmeldung übermittelten Personenbezogenen Daten. Der Auftraggeber hat die Option, Personenbezogene Daten beim Aufgeben einer Supportmeldung von der Übertragung auszuschließen. Falls diese Daten für den Incident-Management-Prozess erforderlich sind, kann der Auftraggeber diese Personenbezogenen Daten vor der Übermittlung der Störungsmeldung an SAP anonymisieren.

10. DEFINITIONEN

Hervorgehobene Begriffe, die hier nicht definiert werden, haben die ihnen in der Vereinbarung zugewiesene Bedeutung.

10.1 **"Verantwortlicher"** bezeichnet die natürliche oder juristische Person, öffentliche Behörde oder Agentur oder andere Stelle, die allein oder gemeinsam mit anderen die Zwecke und Mittel der Verarbeitung Personenbezogener Daten bestimmt; für die Zwecke dieses DPA gilt der Verantwortliche im Verhältnis zu SAP, wenn der Kunde als Auftragsverarbeiter für einen anderen Verantwortlichen handelt, als zusätzlicher und unabhängiger Verantwortlicher mit den entsprechenden Rechten und Pflichten eines Verantwortlichen gemäß diesem DPA.

10.2 **"Rechenzentrum"** bezeichnet den Standort, an dem die Produktivinstanz des Cloud Service für den Auftraggeber in seiner Region gehostet wird (siehe: http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html) bzw. den Standort, der dem Auftraggeber mitgeteilt wurde oder der in einer Order Form vereinbart wurde.

10.3 **"Datenschutzrecht"** bezeichnet die geltenden Rechtsvorschriften zum Schutz der Grundrechte und Freiheiten von Personen und deren Persönlichkeitsrecht in Bezug auf die Verarbeitung von Personenbezogenen Daten im Rahmen der Vereinbarung (und beinhaltet in Bezug auf die Beziehung zwischen den Parteien bezüglich der Verarbeitung Personenbezogener Daten durch

SAP im Auftrag des Auftraggebers, die DSGVO als Mindeststandard, unabhängig davon, ob die Personenbezogenen Daten der DSGVO unterliegen oder nicht.).

10.4 **"Betroffene Person"** bezeichnet eine identifizierte oder identifizierbare natürliche Person gemäß der Definition im Datenschutzrecht.

10.5 **"EWR"** bezeichnet den Europäischen Wirtschaftsraum, d. h. die Mitgliedsstaaten der EU sowie Island, Liechtenstein und Norwegen.

10.6 **"Europäischer Unterauftragsverarbeiter"** bezeichnet einen Unterauftragsverarbeiter, der mit der physischen Verarbeitung Personenbezogener Daten im EWR oder in der Schweiz beauftragt ist.

10.7 **"Personenbezogene Daten"** bezeichnet alle Informationen in Bezug auf eine Betroffene Person, die dem Schutz des Datenschutzrechts unterliegen. In diesem DPA sind darunter nur diejenigen personenbezogenen Daten zu verstehen, die (i) vom Auftraggeber oder dessen Autorisierten Nutzern im Cloud Service oder durch dessen Nutzung erfasst werden oder (ii) von SAP oder ihren Unterauftragsverarbeitern bereitgestellt werden oder auf die SAP oder ihre Unterauftragsverarbeiter zugreifen, um den Support gemäß der Vereinbarung zu leisten. Personenbezogene Daten sind eine Teilmenge der Auftraggeberdaten (gemäß der Definition der Vereinbarung).

10.8 **"Verletzung des Schutzes Personenbezogener Daten"** bezeichnet eine/n bestätigte/n (1) versehentliche oder widerrechtliche Vernichtung, Verlust, Veränderung, eine unbefugte Offenlegung von bzw. einen unbefugten Zugang Dritter zu Personenbezogenen Daten oder (2) einen vergleichbaren Vorfall mit Personenbezogenen Daten, bei denen der Verantwortliche in jedem Fall gemäß Datenschutzrecht zur Meldung an die zuständigen Datenschutzbehörden oder gegenüber den Betroffenen Personen verpflichtet ist.

10.9 **"Auftragsverarbeiter"** bezeichnet eine natürliche oder justische Person, öffentliche Behörde oder Agentur oder andere Stelle, die Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, sei es direkt als Auftragsverarbeiter eines Verantwortlichen oder indirekt als Unterauftragsverarbeiter eines Auftragsverarbeiters, der Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

10.10 **"Standardvertragsklauseln"** (auch als „EU-Modellklauseln" bezeichnet) bezeichnet die Standardvertragsklauseln (Auftragsverarbeiter) bzw. jegliche nachfolgenden von der Europäischen Kommission veröffentlichten Versionen dieser Klauseln (die automatisch gelten). Die bei Vertragsschluss geltenden Standardvertragsklauseln sind hierzu als Anhang 4 beigefügt.

10.11 **"Unterauftragsverarbeiter"** bezeichnet Verbundene Unternehmen der SAP, die SAP SE, sowie Verbundene Unternehmen der SAP SE, sowie Dritte, die von SAP, der SAP SE oder den Verbundenen Unternehmen der SAP SE zur Erbringung des Cloud Service eingesetzt werden, und die Personenbezogene Daten gemäß diesem DPA verarbeiten.

Anhang 1 zum DPA und, falls anwendbar, zu den Standardvertragsklauseln

Datenexporteur
Der Datenexporteur ist der Auftraggeber, der einen bestimmten Cloud Service bezieht, mit dem Autorisierte Nutzer Personenbezogene Daten erfassen, ändern, nutzen, löschen oder anderweitig verarbeiten können. Wenn der Auftraggeber anderen Verantwortlichen erlaubt, den Cloud-Service ebenfalls zu nutzen, sind diese anderen Verantwortlichen ebenfalls Datenexporteure.

Datenimporteur
SAP SE und ihre Unterauftragsverarbeiter erbringen den Cloud Service, der folgenden Support umfasst: Verbundene Unternehmen von SAP leisten von SAP-Einrichtungen in St.Leon/Rot (Deutschland), in Indien oder an anderen Standorten, an denen SAP Personal in der Organisation Operations/Cloud Delivery beschäftigt, aus Remote-Support für die Rechenzentren des SAP Cloud Service. Support beinhaltet:

- Überwachung des Cloud Service
- Sicherung und Wiederherstellung von im Cloud Service gespeicherten Auftraggeberdaten
- Release und Entwicklung von Korrekturen oder Upgrades des Cloud Service
- Überwachung, Fehlerbehebung und Verwaltung der dem Cloud Service zugrunde liegenden Infrastruktur und Datenbank
- Sicherheitsüberwachung, netzwerkbasierter Intrusion Detection Support, Penetrationstests

Verbundene Unternehmen von SAP SE leisten Support, wenn ein Auftraggeber eine Supportmeldung aufgibt, weil der Cloud Service nicht verfügbar ist oder für einige oder alle Autorisierten Nutzer nicht wie erwartet funktioniert. SAP nimmt Telefonanrufe entgegen, führt grundlegende Fehlerbehebungsmaßnahmen durch und bearbeitet Supportmeldungen in einem Tracking-System, das separat von der Produktivinstanz des Cloud Service betrieben wird.

Betroffene Personen
Sofern nicht anderweitig durch den Datenexporteur angegeben, lassen sich die übermittelten Personenbezogenen Daten in der Regel einer der folgenden Kategorien von Betroffenen Personen zuordnen: Mitarbeiter, Subunternehmer, Geschäftspartner oder sonstige Personen, deren Personenbezogene Daten im Cloud Service gespeichert werden.

Datenkategorien
Die übermittelten Personenbezogenen Daten betreffen die folgenden Datenkategorien:
Der Auftraggeber bestimmt die Kategorien von Daten pro bezogenem Cloud Service. Der Auftraggeber kann die Datenfelder während der Implementierung des Cloud Service oder wie anderweitig im Cloud Service zulässig konfigurieren. Die übermittelten Personenbezogenen Daten lassen sich in der Regel einer der folgenden Datenkategorien zuordnen: Name, Telefonnummer, E-Mail-Adresse, Zeitzone, Anschrift, Systemzugriff/-nutzung/-Berechtigungsdaten, Name des Unternehmens, Vertragsdaten, Rechnungsdaten und anwendungsspezifische Daten, die von den Autorisierten Nutzern des Auftraggebers im Cloud Service erfasst werden, wie beispielsweise Bankkontendaten sowie Kredit- oder Debitkartendaten.

Besondere Datenkategorien (falls zutreffend)
Die übermittelten Personenbezogenen Daten lassen sich den folgenden besonderen Datenkategorien zuordnen: wie in der Vereinbarung (insbes. der Order Form) dargelegt (sofern zutreffend).

Verarbeitungsvorgänge / Zwecke
Die übermittelten Personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen:

- Verwendung von Personenbezogenen Daten, um den Cloud Service einzurichten, zu betreiben, zu überwachen und bereitzustellen (einschließlich operativen und technischen Supports)
- Bereitstellung von Consulting Services
- Kommunikation mit Autorisierten Nutzern
- Speicherung von Personenbezogenen Daten in speziellen Rechenzentren (Multi-Tenant-Architektur)
- Upload von Korrekturen oder Upgrades in den Cloud Service
- Erstellen von Sicherungskopien der Personenbezogenen Daten
- Rechnergestützte Verarbeitung von Personenbezogenen Daten, einschließlich Datenübertragung, Abruf von Daten, Zugang zu Daten
- Netzwerkzugang, um die Übertragung von Personenbezogenen Daten zu ermöglichen
- Ausführung von Anweisungen des Auftraggebers gemäß der Vereinbarung

Anhang 2 zum DPA und, falls anwendbar, zu den Standardvertragsklauseln - Technische und organisatorische Maßnahmen

1. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

In den folgenden Abschnitten werden die aktuellen technischen und organisatorischen Maßnahmen der SAP definiert. SAP kann diese Maßnahmen jederzeit unangekündigt ändern, solange eine vergleichbare oder höhere Sicherheitsstufe aufrechterhalten wird. Einzelne Maßnahmen können durch neue Maßnahmen, die denselben Zweck erfüllen, ersetzt werden, ohne dass die Sicherheitsstufe beim Schutz Personenbezogener Daten verringert wird.

1.1 Zutrittskontrolle. Unbefugten wird der physische Zugang zu Einrichtungen, Gebäuden und Räumlichkeiten verwehrt, in denen sich Datenverarbeitungssysteme befinden, die Personenbezogene Daten verarbeiten oder nutzen.

Maßnahmen:

- SAP schützt Gebäude durch angemessene Maßnahmen basierend auf der SAP Security Policy.
- Im Allgemeinen sind Gebäude durch Zutrittskontrollsysteme (z. B. Zutritt per Chipkarte) gesichert.
- Als Mindestanforderung müssen die äußeren Zugänge eines Gebäudes mit einer zertifizierten Schließanlage ausgestattet sein, einschließlich einer modernen, aktiven Schlüsselverwaltung.
- Abhängig von der Sicherheitseinstufung werden Gebäude, einzelne Bereiche und das umliegende Gelände möglicherweise durch weitere Maßnahmen geschützt. Dazu gehören spezielle Zutrittsprofile, Videoüberwachung, Einbruchmeldeanlagen und biometrische Zutrittskontrollsysteme.
- Die Vergabe der Zutrittsrechte an die berechtigten Personen erfolgt auf individueller Basis gemäß den Maßnahmen zur System- und Datenzugriffskontrolle (siehe folgende Abschnitte 1.2 und 1.3). Dies gilt auch für den Zutritt von Besuchern. Gäste und Besucher in SAP-Gebäuden müssen sich namentlich an der Rezeption anmelden und von autorisiertem SAP-Personal begleitet werden.
- SAP-Personal und externes Personal müssen ihren Firmenausweis an allen SAP-Standorten tragen.

Zusätzliche Maßnahmen für Rechenzentren:

- Für alle Rechenzentren gelten strenge Sicherheitsmaßnahmen, die u. a. durch Wachpersonal, Überwachungskameras, Bewegungsmelder und Zugangskontrollmechanismen unterstützt werden, um Anlagen und Einrichtungen von Rechenzentren vor dem Zugriff Unbefugter zu schützen. Zu den Systemen und zur Infrastruktur der Rechenzentren haben ausschließlich autorisiertePersonen Zugang. Um die ordnungsgemäße Funktion zu schützen, werden Sicherheitsgeräte (Bewegungssensoren, Kameras usw.) in regelmäßigen Abständen gewartet.
- SAP sowie alle von Dritten betriebenen Rechenzentren protokollieren die Namen und Uhrzeiten von befugten Personen, die die nicht öffentlichen Bereiche von SAP innerhalb der Rechenzentren betreten.

1.2 Systemzugriffskontrolle. Datenverarbeitungssysteme, die zur Bereitstellung des Cloud Service genutzt werden, sind vor einer nicht autorisierten Nutzung zu schützen.

Maßnahmen:

- Die Gewährung des Zugriffs auf sensible Systeme, einschließlich der Systeme zur Speicherung und Verarbeitung Personenbezogener Daten, erfolgt über mehrere Berechtigungsstufen. Berechtigungen werden über definierte Prozesse gemäß der SAP Security Policy verwaltet.
- Alle Personen greifen mit einer eindeutigen Kennung (User-ID) auf die Systeme von SAP zu
- SAP hat Verfahren eingerichtet, so dass angeforderte Änderungen an Berechtigungen nur in Übereinstimmung mit der SAP Security Policy durchgeführt werden (beispielsweise werden keine

Rechte ohne entsprechende Berechtigung erteilt). Wenn ein Mitarbeiter das Unternehmen verlässt, werden dessen Zugriffsrechte aufgehoben.

- SAP hat eine Kennwortrichtlinie festgelegt, die die Weitergabe von Kennwörtern untersagt, regelt, wie vorzugehen ist, wenn ein Kennwort offengelegt wird, und erfordert, dass Kennwörter regelmäßig geändert und vorgegebene Kennwörter geändert werden. Zur Authentifizierung werden personalisierte Benutzerkennungen (User-IDs) zugewiesen. Alle Kennwörter müssen bestimmte Mindestbedingungen erfüllen und werden in verschlüsselter Form gespeichert. Im Fall von Domänenkennwörtern erzwingt das System alle sechs Monate eine Änderung des Kennworts, das den Anforderungen an komplexe Kennwörter entsprechen muss. Jeder Computer verfügt über einen kennwortgeschützten Bildschirmschoner.
- Das Unternehmensnetzwerk ist durch Firewalls vor dem öffentlichen Netzwerk geschützt.
- SAP verwendet aktuelle Virenscanner an den Übergängen zum Firmennetz (für E-Mail-Konten), sowie auf allen Fileservern und auf allen Einzelplatzcomputern.
- Das Sicherheitspatch-Management gewährleistet die Anwendung entsprechender regelmäßiger Sicherheits-Updates. Der vollständige Zugriff auf das SAP-Firmennetzwerk und die kritische Infrastruktur ist durch eine strenge Authentifizierung geschützt.

1.3 Datenzugriffskontrolle. Personen, die zur Nutzung von Datenverarbeitungssystemen berechtigt sind, erhalten nur Zugriff auf die Personenbezogenen Daten, für die sie Zugriffsrechte besitzen, und Personenbezogene Daten dürfen bei der Verarbeitung, Nutzung oder Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Maßnahmen:

- Im Rahmen der SAP Security Policy erfordern Personenbezogene Daten zumindest den gleichen Schutz wie „vertrauliche" Informationen im Sinne des SAP-Informationsklassifizierungsstandards.
- Der Zugriff auf Personenbezogene Daten wird nur bei entsprechender Notwendigkeit gewährt („Need-to-know"-Prinzip). Jeder Person wird der Zugriff nur auf diejenigen Informationen gewährt, die sie zur Erledigung ihrer Pflichten benötigt. SAP verwendet Berechtigungskonzepte, die die Zuweisungsprozesse und die zugewiesenen Rollen pro Account (User ID) dokumentieren.Alle Auftraggeberdaten werden gemäß der SAP Security Policy geschützt.
- Alle produktiven Server werden in den Rechenzentren oder in sicheren Serverräumen betrieben. Die Sicherheitsmaßnahmen zum Schutz der Anwendungen zur Verarbeitung Personenbezogener Daten werden in regelmäßigen Abständen geprüft. Zu diesem Zweck führt SAP interne und externe Sicherheitsüberprüfungen und Penetrationstests ihrer IT-Systeme durch.
- SAP erlaubt nicht die Installation eigener Software oder sonstiger Software, die nicht durch SAP genehmigter wurde.
- Durch einen entsprechenden SAP-Sicherheitsstandard wird geregelt, auf welche Weise Daten und Datenträger gelöscht oder vernichtet werden, wenn sie nicht mehr benötigt werden.

1.4 Datenübertragungskontrolle. Die Datenübertragungskontrolle gewährleistet, dass Personenbezogene Daten, außer soweit für die Erbringung der Cloud Services gemäß der Vereinbarung notwendig, bei der Übertragung oder Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Beim physischen Transport von Datenträgern werden bei SAP geeignete Maßnahmen getroffen, um die vereinbarten Service-Level zu gewährleisten (z. B. Verschlüsselung, mit Blei ausgekleidete Behälter).

Maßnahmen:

- Personenbezogene Daten sind bei der Übertragung über interne SAP-Netzwerke geschützt gemäß der SAP Security Policy geschützt.
- Im Hinblick auf die Übertragung der Daten zwischen SAP und ihren Auftraggebern werden die Sicherheitsmaßnahmen für die übertragenen Personenbezogenen Daten von den Parteien

vereinbart und zum Bestandteil der Vereinbarung. Dies gilt sowohl für die physische als auch für die netzwerkbasierte Datenübertragung. In jedem Fall übernimmt der Auftraggeber die Verantwortung für die Datenübertragung, sobald sie außerhalb der von SAP kontrollierten Systeme erfolgt (z. B. Daten, die außerhalb der Firewall des SAP-Rechenzentrums übertragen werden).

1.5 Dateneingabekontrolle. Es wird die Möglichkeit geschaffen, im Nachhinein zu untersuchen und festzustellen, ob und von wem Personenbezogene Daten erfasst, modifiziert oder aus den Datenverarbeitungssystemen der SAP entfernt wurden.
Maßnahmen:

- SAP gestattet ausschließlich befugten Personen im Rahmen ihrer Pflichten, auf Personenbezogene Daten zuzugreifen.
- SAP hat innerhalb des Cloud Service ein Protokollierungssystem für das Erfassen, Ändern und Löschen oder Sperren Personenbezogener Daten durch SAP oder ihre Unterauftragsverarbeiter im technisch möglichen Umfang implementiert.

1.6 Auftragskontrolle. Personenbezogene Daten, die im Auftrag verarbeitet werden (z. B. im Auftrag des Auftraggebers), werden ausschließlich in Übereinstimmung mit der Vereinbarung und den diesbezüglichen Weisungen des Auftraggebers verarbeitet.
Maßnahmen:

- SAP nutzt Kontrollen und Verfahren, um die Einhaltung der Verträge zwischen SAP und ihren Auftraggebern, Unterauftragsverarbeitern oder anderen Serviceanbietern zu überwachen.
- Im Rahmen der SAP Security Policy erfordern Personenbezogene Daten zumindest den gleichen Schutz wie „vertrauliche" Informationen im Sinne des SAP-Informationsklassifizierungsstandards.
- Sämtliche SAP-Mitarbeiter und Unterauftragsverarbeiter oder anderen Serviceanbieter werden vertraglich verpflichtet, die Geheimhaltungspflicht in Bezug auf alle sensiblen Informationen einschließlich Geschäftsgeheimnissen von Auftraggebern und Partnern der SAP einzuhalten.

1.7 Verfügbarkeitskontrolle. Personenbezogene Daten werden vor versehentlicher oder nicht autorisierter Vernichtung oder Verlust geschützt.
Maßnahmen:

- SAP verfügt über regelmäßige Backup-Prozesse zur Wiederherstellung der Verfügbarkeit geschäftskritischer Systeme bei Bedarf.
- SAP verwendet unterbrechungsfreie Stromversorgungen (USV, Batterien, Generatoren usw.), um die Stromversorgung für die Rechenzentren zu schützen.
- SAP hat Geschäftsnventualfallpläne für geschäftskritische Prozesse ausgearbeitet und kann Desaster Recovery Strategien für geschäftskritische Services anbieten, wie näher in der Dokumention beschrieben oder in der Order Form für den jeweiligen Cloud Service einbezogen.

- Notfallprozesse und -systeme werden regelmäßig getestet.

1.8 Trennungskontrolle. Personenbezogene Daten, die für unterschiedliche Zwecke erfasst werden, können getrennt verarbeitet werden.
Maßnahmen:

- SAP nutzt die technischen Möglichkeiten der implementierten Software (z. B. Multi-Tenancy- oder getrennte Systemlandschaften), um die Trennung von Personenbezogenen Daten zu ermöglichen, die von verschiedenen Auftraggebern stammen.
- Der Auftraggeber (einschließlich seiner Verantwortlichen) hat ausschließlich auf seine eigenen Daten Zugriff.

- Wenn zur Bearbeitung eines Supportfalls des Auftraggebers Personenbezogene Daten dieses Auftraggebers benötigt werden, werden die Daten dieser Meldung zugeordnet und nur zur Bearbeitung dieser Meldung verwendet; für die Bearbeitung anderer Meldungen findet kein Zugriff auf diese Daten statt. Diese Daten werden in dedizierten Support-Systemen gespeichert.

-

1.9 Datenintegritätskontrolle. Personenbezogene Daten bleiben während der Verarbeitungsaktivitäten unversehrt, vollständig und aktuell.

Maßnahmen:

SAP hat zum Schutz vor unautorisierten Änderungen eine mehrere Schichten umfassende Sicherheitsstrategie umgesetzt.

Insbesondere verwendet SAP die folgenden Mittel, um die obigen Abschnitte zu Kontrollen und Maßnahmen umzusetzen:

- Firewalls
- Security Monitoring Center
- Antivirensoftware
- Erstellen von Sicherungskopien und Wiederherstellung
- Externe und interne Penetrationstests
- Regelmäßige Prüfung der Sicherheitsmaßnahmen durch externe Prüfer

Anhang 3 zum DPA und, falls anwendbar, zu den Standardvertragsklauseln

Ausschließlich zur Veranschaulichung benennt die folgende Tabelle die einschlägigen Artikel der DSGVO und die entsprechenden Regelungen des DPA.

Artikel der DSGVO	Abschnitt des DPA	Mit Klick auf den Link zum jeweiligen Abschnitt
28(1)	2 und Anhang 2	SICHERHEIT DER VERARBEITUNG und Anhang 2 Technische und organisatorische Maßnahmen
28(2), 28(3) (d) und 28 (4)	6	UNTERAUFTRAGSVERARBEITER
28 (3) Satz 1	1.1 und Anhang 1, 1.2	Zweck und Anwendung., Anhang 1, Struktur.
28(3) (a) und 29	3.1 und 3.2	Weisungen des Auftraggebers. , Verarbeitung auf Basis rechtlicher Erfordernisse.
28(3) (b)	3.3	Befugte Personen.
28(3) (c) und 32	2 und Anhang 2	SICHERHEIT DER VERARBEITUNG und Anhang 2 Technische und organisatorische Maßnahmen
28(3) (e)	3.4	Kooperation.
28(3) (f) and 32-36	2 und Anhang 2, 3.5, 3.6	SICHERHEIT DER VERARBEITUNG und Anhang 2 Technische und organisatorische Maßnahmen Meldung von Verletzungen des Schutzes Personenbezogener Daten., Datenschutz-Folgenabschätzung.
28(3) (g)	4	DATEN-EXPORT UND LÖSCHUNG
28(3) (h)	5	ZERTIFIZIERUNGEN UND AUDITS
28 (4)	6	UNTERAUFTRAGSVERARBEITER
30	8	DOKUMENTATION; VERARBEITUNGSVERZEICHNIS
46(2) c)	7.2 und Anhang 4	Standardvertragsklauseln und Anhang 4 Standardvertragsklauseln (Auftragsverarbeiter)

Anhang 4 zum DPA

Standardvertragsklauseln (Auftragsverarbeiter)[1]

gemäß Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist

[...]

(In den Klauseln nachfolgend als „**Datenexporteur**" bezeichnet)

Und

[...]

(in den Klauseln nachfolgend als „**Datenimporteur**" bezeichnet)

(die „Partei", wenn eine dieser Organisationen gemeint ist, die „Parteien", wenn beide gemeint sind)

VEREINBAREN folgende Vertragsklauseln („Klauseln"), um angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bei der Übermittlung der in Anhang 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Datenexporteur an den Datenimporteur zu bieten.

Klausel 1

Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

a) die Ausdrücke „personenbezogene Daten", „besondere Kategorien personenbezogener Daten", „Verarbeitung", „für die Verarbeitung Verantwortlicher", „Auftragsverarbeiter", „betroffene Person" und „Kontrollstelle" entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (1);

b) der „Datenexporteur" ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt;

c) der „Datenimporteur" ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung nach dessen Anweisungen und den Bestimmungen der Klauseln in dessen Auftrag zu verarbeiten und der nicht einem System eines Drittlandes unterliegt, das angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;

d) der „Unterauftragsverarbeiter" ist der Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiters des Datenimporteurs tätig ist und sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs personenbezogene Daten ausschließlich zu dem Zweck entgegenzunehmen, diese nach der Übermittlung im Auftrag des Datenexporteurs nach dessen Anweisungen, den Klauseln und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;

e) der Begriff „anwendbares Datenschutzrecht" bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen

[1] Gemäß dem Beschluss der Kommission vom 5. Februar 2010 (2010/87/EU)

anzuwenden sind;

f) die „technischen und organisatorischen Sicherheitsmaßnahmen" sind die Maßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung schützen sollen.

Klausel 2

Einzelheiten der Übermittlung

Die Einzelheiten der Übermittlung, insbesondere die besonderen Kategorien personenbezogener Daten, sofern vorhanden, werden in Anhang 1 erläutert, der Bestandteil dieser Klauseln ist.

Klausel 3

Drittbegünstigtenklausel

(1) Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.

(2) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.

(3) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(4) Die Parteien haben keine Einwände dagegen, dass die betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

Klausel 4

Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:

a) die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und gegebenenfalls den zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur niedergelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;

b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der

Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und den Klauseln zu verarbeiten;

c) der Datenimporteur hinreichende Garantien bietet in Bezug auf die in Anhang 2 zu diesem Vertrag beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen;

d) die Sicherheitsmaßnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligem Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung geschützt sind;

e) er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt;

f) die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis gesetzt worden ist oder gesetzt wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;

g) er die gemäß Klausel 5 Buchstabe b sowie Klausel 8 Absatz 3 vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Kontrollstelle weiterleitet, wenn der Datenexporteur beschließt, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben;

h) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsmaßnahmen zur Verfügung stellt; außerdem stellt er ihnen gegebenenfalls die Kopie des Vertrags über Datenverarbeitungsdienste zur Verfügung, der gemäß den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;

i) bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter die Verarbeitung gemäß Klausel 11 erfolgt und die personenbezogenen Daten und die Rechte der betroffenen Person mindestens ebenso geschützt sind, wie vom Datenimporteur nach diesen Klauseln verlangt; und

j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

Klausel 5

Pflichten des Datenimporteurs [(2)]

Der Datenimporteur erklärt sich bereit und garantiert, dass:

a) er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer

solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

c) er vor der Verarbeitung der übermittelten personenbezogenen Daten die in Anhang 2 beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen ergriffen hat;

d) er den Datenexporteur unverzüglich informiert über

   i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;

   ii) jeden zufälligen oder unberechtigten Zugang und

   iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

e) er alle Anfragen des Datenexporteurs im Zusammenhang mit der Verarbeitung der übermittelten personenbezogenen Daten durch den Datenexporteur unverzüglich und ordnungsgemäß bearbeitet und die Ratschläge der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten befolgt;

f) er auf Verlangen des Datenexporteurs seine für die Verarbeitung erforderlichen Datenverarbeitungseinrichtungen zur Prüfung der unter die Klauseln fallenden Verarbeitungstätigkeiten zur Verfügung stellt. Die Prüfung kann vom Datenexporteur oder einem vom Datenexporteur ggf. in Absprache mit der Kontrollstelle ausgewählten Prüfgremium durchgeführt werden, dessen Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind;

g) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und gegebenenfalls einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden; Anhang 2 wird durch eine allgemeine Beschreibung der Sicherheitsmaßnahmen ersetzt, wenn die betroffene Person vom Datenexporteur keine solche Kopie erhalten kann;

h) er bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat;

i) der Unterauftragsverarbeiter die Datenverarbeitungsdienste in Übereinstimmung mit Klausel 11 erbringt;

j) er dem Datenexporteur unverzüglich eine Kopie des Unterauftrags über die Datenverarbeitung zuschickt, den er nach den Klauseln geschlossen hat.

Klausel 6

Haftung

(1) Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.

(2) Ist die betroffene Person nicht in der Lage, gemäß Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den

Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.

Der Datenimporteur kann sich seiner Haftung nicht entziehen, indem er sich auf die Verantwortung des Unterauftragsverarbeiters für einen Verstoß beruft.

(3) Ist die betroffene Person nicht in der Lage, gemäß den Absätzen 1 und 2 gegenüber dem Datenexporteur oder dem Datenimporteur wegen Verstoßes des Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 aufgeführte Pflichten Ansprüche geltend zu machen, weil sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, ist der Unterauftragsverarbeiter damit einverstanden, dass die betroffene Person im Zusammenhang mit seinen Datenverarbeitungstätigkeiten aufgrund der Klauseln gegenüber ihm statt gegenüber dem Datenexporteur oder dem Datenimporteur einen Anspruch geltend machen kann, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen. Eine solche Haftung des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach diesen Klauseln beschränkt.

Klausel 7

Schlichtungsverfahren und Gerichtsstand

(1) Für den Fall, dass eine betroffene Person gegenüber dem Datenimporteur Rechte als Drittbegünstigte und/oder Schadenersatzansprüche aufgrund der Vertragsklauseln geltend macht, erklärt sich der Datenimporteur bereit, die Entscheidung der betroffenen Person zu akzeptieren, und zwar entweder:

a) die Angelegenheit in einem Schlichtungsverfahren durch eine unabhängige Person oder gegebenenfalls durch die Kontrollstelle beizulegen oder

b) die Gerichte des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, mit dem Streitfall zu befassen.

(2) Die Parteien vereinbaren, dass die Entscheidung der betroffenen Person nicht die materiellen Rechte oder Verfahrensrechte dieser Person, nach anderen Bestimmungen des nationalen oder internationalen Rechts Rechtsbehelfe einzulegen, berührt.

Klausel 8

Zusammenarbeit mit Kontrollstellen

(1) Der Datenexporteur erklärt sich bereit, eine Kopie dieses Vertrags bei der Kontrollstelle zu hinterlegen, wenn diese es verlangt oder das anwendbare Datenschutzrecht es so vorsieht.

(2) Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Maße und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gemäß dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.

(3) Der Datenimporteur setzt den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des

Datenimporteurs oder von Unterauftragsverarbeitern gemäß Absatz 2 verhindern. In diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 Buchstabe b vorgesehenen Maßnahmen zu ergreifen.

Klausel 9

Anwendbares Recht

Für diese Klauseln gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist.

Klausel 10

Änderung des Vertrags

Die Parteien verpflichten sich, die Klauseln nicht zu verändern. Es steht den Parteien allerdings frei, erforderlichenfalls weitere, geschäftsbezogene Klauseln aufzunehmen, sofern diese nicht im Widerspruch zu der Klausel stehen.

Klausel 11

Vergabe eines Unterauftrags

(1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss [(3)]. Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.

(2) Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gemäß Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gemäß Klausel 6 Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(3) Für Datenschutzbestimmungen im Zusammenhang mit der Vergabe von Unteraufträgen über die Datenverarbeitung gemäß Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich: …

(4) Der Datenexporteur führt ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen Vereinbarungen, die vom Datenimporteur nach Klausel 5 Buchstabe j übermittelt wurden. Das Verzeichnis wird der Kontrollstelle des Datenexporteurs bereitgestellt.

Klausel 12

Pflichten nach Beendigung der Datenverarbeitungsdienste

(1) Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Datenverarbeitungsdienste je nach Wunsch des Datenexporteurs alle

übermittelten personenbezogenen Daten und deren Kopien an den Datenexporteur zurückschicken oder alle personenbezogenen Daten zerstören und dem Datenexporteur bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der der Datenimporteur unterliegt, diesem die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. In diesem Fall garantiert der Datenimporteur, dass er die Vertraulichkeit der übermittelten personenbezogenen Daten gewährleistet und diese Daten nicht mehr aktiv weiterverarbeitet.

(2) Der Datenimporteur und der Unterauftragsverarbeiter garantieren, dass sie auf Verlangen des Datenexporteurs und/oder der Kontrollstelle ihre Datenverarbeitungseinrichtungen zur Prüfung der in Absatz 1 genannten Maßnahmen zur Verfügung stellen.

---

(1) Die Parteien können die Begriffsbestimmungen der Richtlinie 95/46/EG in diese Klausel aufnehmen, wenn nach ihrem Dafürhalten der Vertrag für sich allein stehen sollte.

(2) Zwingende Erfordernisse des für den Datenimporteur geltenden innerstaatlichen Rechts, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft für den Schutz eines der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG aufgelisteten Interessen erforderlich ist, widersprechen nicht den Standardvertragsklauseln, wenn sie zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen erforderlich sind. Beispiele für zwingende Erfordernisse, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich ist, sind international anerkannte Sanktionen, Erfordernisse der Steuerberichterstattung oder Anforderungen zur Bekämpfung der Geldwäsche.

(3) Dies kann dadurch gewährleistet werden, dass der Unterauftragsverarbeiter den nach diesem Beschluss geschlossenen Vertrag zwischen dem Datenexporteur und dem Datenimporteur mitunterzeichnet.