SOLUTION PLUS
+49 176 47658461
info@solutionplus.io
solutionplus.io
Kollwitzstraße 76
10435 Berlin, Germany

Version 3.2 · November 2026

Vertrag über die Auftragsverarbeitung

gemäß Artikel 28 DSGVO, auf Grundlage der EU-Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter (Durchführungsbeschluss (EU) 2021/915 der Kommission)

geschlossen als Teil des [Vertrags / Angebots, Nummer und Datum] (der **„Hauptvertrag"**)

zwischen

[Firma des Kunden], [Anschrift]
– der **„Verantwortliche"** –

und

SolutionPlus UG (haftungsbeschränkt), Kollwitzstraße 76, 10435 Berlin, Amtsgericht Charlottenburg HRB 291768 B, vertreten durch den Geschäftsführer Saif Ur Rehman Qureshi
– der **„Auftragsverarbeiter"** –

– zusammen die „Parteien"; Kontaktdaten und Unterschriften in Anhang I –

Aufbau dieses Vertrags

Teil	Inhalt
Teil A	Die von der Europäischen Kommission erlassenen Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern (Durchführungsbeschluss (EU) 2021/915 vom 4. Juni 2021), **unverändert** wiedergegeben, mit Ausnahme der unten gewählten Optionen (Klausel 2 Buchstabe a).
Teil B	Ergänzende Regelungen nach Klausel 2 Buchstabe b: EU-Datengrenze und Zugriffsstufen, kontrollierter Fernzugriff der Stufe C (B.2a), Fristen, Kontrollen, Behördenanfragen, Löschung, Haftung, Recht und Gerichtsstand. Sie widersprechen Teil A nicht; sollte dies doch der Fall sein, hat Teil A Vorrang (Klausel 4).
Anhänge I–IV	Liste der Parteien, Beschreibung der Verarbeitung, technische und organisatorische Maßnahmen, Unterauftragsverarbeiter.
Anhang V	Zusammenfassung der Bewertung der Übermittlungsrisiken für die Unterauftragsverarbeiter in Pakistan und den Vereinigten Arabischen Emiraten (Klausel 7.8, Kapitel V DSGVO).

In Teil A gewählte Optionen

Klausel	Auswahl
1 a), 8 c) Nr. 4, 9.1, 9.2	Option 1: Verordnung (EU) 2016/679 (DSGVO)
5 (Kopplungsklausel)	Aufgenommen
7.7 a)	Option 2: allgemeine schriftliche Genehmigung; Zeitraum **30 Tage**

So arbeiten wir: auf einen Blick

- **Vertragspartner:** Die SolutionPlus UG in Berlin ist Ihr Auftragsverarbeiter und steht Ihnen gegenüber für alle ein, die an Ihrem Projekt arbeiten, auch für Unterauftragsverarbeiter (Klausel 7.7 d).
- **Ort:** Ihre Produktivsysteme und personenbezogenen Daten werden in der EU bzw. im EWR betrieben.
- **Stufe A:** Auf personenbezogene Daten greifen nur unsere Teammitglieder mit Sitz in der EU bzw. im EWR zu.
- **Stufe B:** Unser Lieferpartner in Pakistan und, soweit Anhang IV es nennt, unser verbundenes Unternehmen in den Vereinigten Arabischen Emiraten (Solution Plus Tech Consultancy FZE) arbeiten an Code und Testsystemen mit synthetischen oder anonymisierten Daten. Sie haben keinen Zugriff auf personenbezogene Daten und keinen Zugang zu Produktivsystemen. Es findet keine Übermittlung personenbezogener Daten statt.
- **Stufe C:** Zugriff durch eine benannte Person eines Unterauftragsverarbeiters außerhalb der EU bzw. des EWR nur auf Ihre dokumentierte Weisung, für eine Aufgabe und befristet, unter den Standardvertragsklauseln für Übermittlungen (Modul 3) und den Schutzmaßnahmen in Anhang V. Typischer Fall: ein Sicherheitsvorfall. Der Zugriff ist reine Anzeige, über ein verschlüsseltes VPN auf einen abgeschotteten virtuellen Desktop in der EU; Kopieren, Herunterladen und Drucken sind deaktiviert; jede Sitzung wird protokolliert und aufgezeichnet (B.2a).
- **Anwendbares Recht:** Für jede Verarbeitung nach diesem Vertrag gelten die DSGVO und das Bundesdatenschutzgesetz (BDSG). In Pakistan ist kein umfassendes Datenschutzgesetz in Kraft; in den Vereinigten Arabischen Emiraten gilt das Föderale Gesetzesdekret Nr. 45 von 2021 zum Schutz personenbezogener Daten (PDPL). Für keines der beiden Länder gibt es einen Angemessenheitsbeschluss der EU; deshalb ist Stufe B der Standard (Anhang V).
- **Fristen:** 30 Tage Vorankündigung neuer Unterauftragsverarbeiter; Meldung von Datenschutzverletzungen innerhalb von 24 Stunden; Löschung innerhalb von 30 Tagen nach Vertragsende.

Abbildungen 1 und 2 veranschaulichen Teil B, Abschnitt B.2. Verbindlich ist der Text der Teile A und B und der Anhänge.

ABBILDUNG 1 · DATENFLUSS UND EU-DATENGRENZE

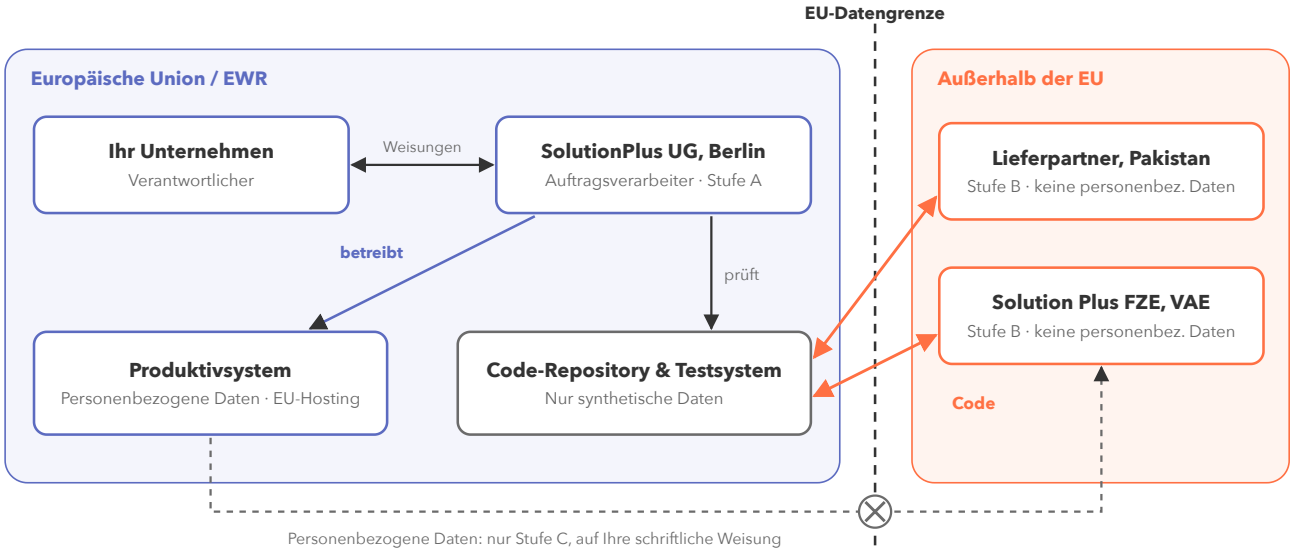
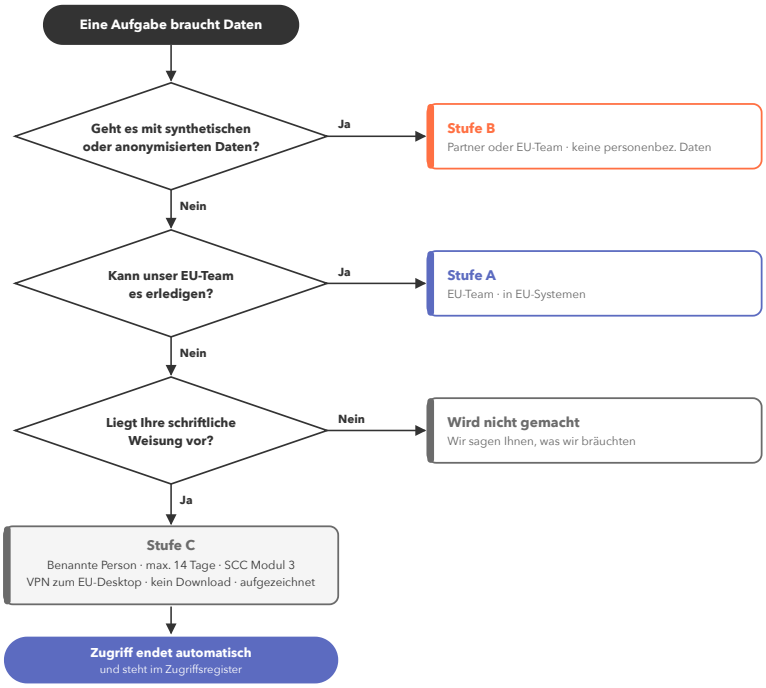


ABBILDUNG 2 · WER DARF PERSONENBEZOGENE DATEN SEHEN: DIE ENTSCHEIDUNG ÜBER DIE ZUGRIFFSSTUFE



Teil A – Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/915 der Kommission)

Wiedergegeben nach dem Amtsblatt (ABl. L 199 vom 7.6.2021, S. 18) ohne Änderungen, mit Ausnahme der auf Seite 1 gewählten Optionen (Klausel 2 Buchstabe a). Quelle: EUR-Lex, © Europäische Union, https://eur-lex.europa.eu.

ABSCHNITT I

Klausel 1 Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln") soll die Einhaltung von Artikel 28 Absätze 3 und 4 der 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 (Datenschutz-Grundverordnung) sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2 Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3 Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4 Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 – fakultativ Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 6 Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7 Pflichten der Parteien

7.1. Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

a) **ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG:** Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 30 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8 Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

   1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung"), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

   2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

   3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

   4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9 Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

   1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

   2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

   3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III – SCHLUSSBESTIMMUNGEN

Klausel 10 Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

   1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

   2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

   3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Teil B — Ergänzende Regelungen (Klausel 2 Buchstabe b)

B.1 Verhältnis zu Teil A und zum Hauptvertrag

1. Teil B ergänzt Teil A. Er ändert Teil A nicht und ist im Einklang mit ihm auszulegen. Bei Widersprüchen hat Teil A Vorrang (Klausel 4).
2. In Fragen des Datenschutzes geht dieser Vertrag dem Hauptvertrag vor. Er gilt, solange der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
3. Dieser Vertrag gilt nicht für personenbezogene Daten, die der Auftragsverarbeiter als eigener Verantwortlicher verarbeitet, etwa Kontaktdaten der Beschäftigten des Verantwortlichen für Vertragsverwaltung und Rechnungsstellung.

B.2 EU-Datengrenze und Zugriffsstufen

1. Personenbezogene Daten werden in der Europäischen Union oder im Europäischen Wirtschaftsraum gespeichert und verarbeitet. Die Hosting-Standorte sind in Anhang IV aufgeführt.
2. Der Auftragsverarbeiter organisiert den Zugriff auf personenbezogene Daten in drei Stufen (Abbildungen 1 und 2):
   a. **Stufe A – EU-Team.** Zugriff auf Produktivsysteme, auf personenbezogene Daten und auf Bildschirme, die personenbezogene Daten zeigen (einschließlich Support-Sitzungen, Bildschirmfreigaben und Besprechungen), haben nur Beschäftigte und freie Mitarbeitende des Auftragsverarbeiters, die sich zum Zeitpunkt des Zugriffs in der EU bzw. im EWR befinden, und nur soweit erforderlich (Klausel 7.4 b).
   b. **Stufe B – außerhalb der EU bzw. des EWR, ohne personenbezogene Daten.** Der Lieferpartner in Pakistan und, soweit Anhang IV es nennt, das verbundene Unternehmen des Auftragsverarbeiters in den Vereinigten Arabischen Emiraten arbeiten an Quellcode, Design, Dokumentation sowie an Entwicklungs- und Testsystemen, die ausschließlich synthetische oder anonymisierte Daten enthalten. Personen der Stufe B haben weder Konten auf noch Zugriff auf noch technische Zugangswege zu Produktivsystemen oder anderen Systemen mit personenbezogenen Daten des Verantwortlichen und erhalten keine Kopien davon. Informationen, die sich nicht auf eine identifizierbare natürliche Person beziehen, sind keine personenbezogenen Daten (Erwägungsgrund 26 DSGVO); ihre Nutzung ist keine Übermittlung im Sinne von Kapitel V DSGVO.
   c. **Stufe C – Ausnahme auf Weisung.** Zugriff auf personenbezogene Daten durch Personen außerhalb der EU bzw. des EWR erfolgt nur auf dokumentierte Weisung des Verantwortlichen (Klauseln 7.1 und 7.8 a) für eine bestimmte Aufgabe, durch benannte Personen und für einen in der Weisung genannten Zeitraum, unter den Bedingungen nach B.2a und den Schutzmaßnahmen nach B.4 und Anhang V. Der Zugriff endet mit Ablauf des Zeitraums automatisch.

3. Personen der Stufe A dürfen unter den Maßnahmen in Anhang III im Homeoffice oder auf Reisen innerhalb der EU bzw. des EWR arbeiten. Greift eine Person der Stufe A während eines vorübergehenden Aufenthalts außerhalb der EU bzw. des EWR auf personenbezogene Daten zu, bedarf dies der vorherigen Zustimmung des Verantwortlichen in Textform.
4. Der Auftragsverarbeiter erfasst jeden Zugriff der Stufe C (wer, welche Daten, wann, wozu, auf wessen Weisung) in einem Zugriffsregister und stellt es dem Verantwortlichen auf Anfrage zur Verfügung.

B.2a Stufe C: kontrollierter Fernzugriff

1. **Zweck und Ausnahme.** Stufe C ist eine Ausnahme. Sie ist nur zulässig, wenn sich eine bestimmte Aufgabe nicht in der erforderlichen Zeit auf Stufe A oder B erledigen lässt, insbesondere um eine Verletzung des Schutzes personenbezogener Daten, einen Sicherheitsvorfall oder eine ausnutzbare Schwachstelle zu untersuchen, einzudämmen oder zu beheben, oder um einen Fehler zu analysieren, der nur mit Produktivdaten auftritt. Für Routineentwicklung, Tests oder Support wird Stufe C nicht genutzt.
2. **Freigabe in Textform.** Ohne vorherige Stufe-C-Freigabe findet kein Zugriff der Stufe C statt. Diese Regel gilt ausnahmslos, auch bei dringenden Vorfällen und außerhalb der Geschäftszeiten.
   a. Eine Stufe-C-Freigabe ist eine dokumentierte Weisung des Verantwortlichen (Klauseln 7.1 und 7.8 a) in Textform (§ 126b BGB; E-Mail oder Ticket genügt) durch eine in Anhang I als weisungsberechtigt genannte Person.
   b. Sie nennt: die Aufgabe und ihren Zweck; die betroffenen Systeme und Kategorien personenbezogener Daten; den Unterauftragsverarbeiter (der in Anhang IV genehmigt sein muss) und die benannten Personen; ob Änderungen zulässig sind (Nr. 9 a); ob sensible Daten einbezogen sind (Nr. 9 c); Beginn und Ende des Zugriffszeitraums sowie etwaige weitere Bedingungen.
   c. Der Zugriffszeitraum ist so kurz, wie die Aufgabe es erfordert, höchstens 14 Tage. Er wird nur durch eine neue Freigabe verlängert.
   d. Der Auftragsverarbeiter kann eine Freigabe vorschlagen und begründet im Vorschlag, warum Stufe A oder B nicht ausreicht und welches Restrisiko bleibt (Nr. 11 c). Der Verantwortliche entscheidet frei und kann ablehnen.
   e. Bis eine Freigabe vorliegt, setzt der Auftragsverarbeiter die Arbeit nur auf Stufe A oder B fort. Der Verantwortliche kann dafür in Anhang I einen Notfallkontakt benennen.
   f. Hat der Auftragsverarbeiter Anlass, an der Echtheit einer Freigabe zu zweifeln, etwa weil das E-Mail-System des Verantwortlichen vom Vorfall betroffen ist, bestätigt er sie vor der Freischaltung durch Rückruf unter der Prüfnummer in Anhang I.

3. **Widerruf und Ablehnung.** Der Verantwortliche kann eine Freigabe jederzeit in Textform ohne Angabe von Gründen widerrufen oder einschränken. Der Auftragsverarbeiter beendet dann offene Sitzungen und sperrt die Konten unverzüglich, spätestens innerhalb von 24 Stunden, und bestätigt dies in Textform. Der Auftragsverarbeiter führt keinen Zugriff der Stufe C durch, wenn die Bedingungen dieses Abschnitts nicht erfüllt werden können, und informiert den Verantwortlichen.
4. **Zugangsweg.** Zugriff der Stufe C erfolgt ausschließlich wie folgt:
   a. *Verschlüsselter Tunnel.* Die freigegebene Person verbindet sich über einen verschlüsselten, beidseitig authentifizierten VPN-Tunnel mit einem VPN-Gateway in der EU bzw. im EWR. Das Gateway betreibt der Auftragsverarbeiter, der Verantwortliche oder ein in Anhang IV genannter Anbieter. Der Auftragsverarbeiter dokumentiert das verwendete Protokoll und die Konfiguration.
   b. *EU-Sitzungsrechner.* Vom Gateway aus erreicht die Person nur einen gehärteten virtuellen Desktop oder Sitzungs-Proxy in der EU bzw. im EWR (den „EU-Sitzungsrechner"), mit persönlichem Konto und Mehr-Faktor-Authentifizierung (Authenticator-App oder Hardware-Schlüssel, nicht SMS). Alle für die Aufgabe genutzten Werkzeuge (Kommandozeile, Datenbank-Client, Administrationskonsole) laufen auf dem EU-Sitzungsrechner. Eine direkte Verbindung vom Gerät der Person zu einem Produktivsystem, einer Datenbank oder einer Schnittstelle ist nicht möglich.
   c. *Nur Anzeige.* Personenbezogene Daten werden nur auf Systemen in der EU bzw. im EWR gespeichert und verarbeitet. An das Gerät der Person wird nur das Bildschirmbild übertragen, zurück nur Tastatur- und Mauseingaben.
   d. *Keine Kopierfunktionen.* Zwischenablage, Dateiübertragung sowie Laufwerks-, Drucker- und USB-Umleitung sind auf dem EU-Sitzungsrechner deaktiviert. Seine ausgehenden Verbindungen sind auf die in der Freigabe genannten Systeme beschränkt, sodass er keine E-Mail-, Messaging-, Filesharing- oder sonstigen Internetdienste erreichen kann.
   e. *Gerät und Ort.* Der Zugriff erfolgt von einem firmeneigenen Gerät des Unterauftragsverarbeiters mit vollständiger Festplattenverschlüsselung, unterstütztem und aktuellem Betriebssystem, Virenschutz und automatischer Bildschirmsperre, an einem nicht öffentlichen Ort. Der Unterauftragsverarbeiter bestätigt dies für jede benannte Person vor dem ersten Zugriff in Textform.
5. **Konten und Fristen.** Konten der Stufe C sind persönlich, standardmäßig gesperrt und werden von einer Person der Stufe A des Auftragsverarbeiters nur für den Zugriffszeitraum freigeschaltet. Sie sind auf die für die Aufgabe nötigen Systeme und Rechte beschränkt, laufen mit Ende des Zeitraums automatisch ab und werden früher gesperrt, sobald die Aufgabe erledigt ist. Inaktive Sitzungen werden automatisch getrennt.
6. **Protokollierung und Aufzeichnung.**
   a. Gateway und EU-Sitzungsrechner protokollieren jede Sitzung der Stufe C: Person, Beginn und Ende, Quell-IP-Adresse und aufgerufene Systeme. Zusätzlich wird die Sitzung aufgezeichnet (Bildschirmaufzeichnung oder Protokoll der Befehle und Abfragen), sofern der Verantwortliche in der Freigabe nicht darauf verzichtet.

b. Protokolle und Aufzeichnungen werden in der EU bzw. im EWR an einem Ort gespeichert, an dem die freigegebenen Personen und der Unterauftragsverarbeiter keine Schreib- oder Löschrechte haben.

c. Sitzungsprotokolle werden 12 Monate, Aufzeichnungen 90 Tage aufbewahrt, sofern der Verantwortliche keine andere Frist bestimmt oder sie für eine laufende Untersuchung benötigt werden. Danach werden sie gelöscht.

d. Protokolle und Aufzeichnungen werden nur zur Kontrolle der Einhaltung und zur Untersuchung von Vorfällen verwendet. Zugriff haben nur Personen der Stufe A und der Verantwortliche. Der Auftragsverarbeiter stellt sie dem Verantwortlichen auf Anfrage innerhalb von 5 Arbeitstagen zur Verfügung.

e. Die freigegebenen Personen werden vorab darüber informiert, dass Sitzungen protokolliert und aufgezeichnet werden.

f. Jede Freigabe und jede Sitzung wird im Zugriffsregister (B.2 Nr. 4) erfasst.

7. **Ende des Zugriffs.** Innerhalb von 5 Arbeitstagen nach Ende des Zugriffszeitraums bestätigt der Auftragsverarbeiter dem Verantwortlichen in Textform, dass die Konten gesperrt sind, und fasst die durchgeführten Sitzungen und Tätigkeiten zusammen.
8. **Behördliche Anfragen und Rechtsänderungen.** B.7 gilt. Wendet sich eine Behörde während oder nach einem Zugriffszeitraum der Stufe C wegen der Daten des Verantwortlichen an den Unterauftragsverarbeiter oder eine freigegebene Person, oder erfährt der Auftragsverarbeiter von einer Änderung von Recht oder Praxis, die die Bewertung in Anhang V berührt, setzt er den Zugriff der Stufe C sofort aus und informiert den Verantwortlichen (B.4 Nr. 3).
9. **Datenminimierung.**
   a. Zugriffsrechte sind nur lesend, sofern die Freigabe Änderungen nicht ausdrücklich erlaubt.
   b. Wo die Aufgabe es zulässt, werden maskierte oder pseudonymisierte Ansichten genutzt.
   c. Sensible Daten (Klausel 7.5) sind ausgeschlossen, sofern die Freigabe sie nicht ausdrücklich einbezieht.
   d. Auf Wunsch des Verantwortlichen beaufsichtigt eine Person der Stufe A die Sitzung live.
10. **Verstöße.** Der Auftragsverarbeiter behandelt als Sicherheitsvorfall: jeden Zugriff der Stufe C ohne gültige Freigabe oder außerhalb des Zugangswegs nach Nr. 4, jeden Versuch, diese Maßnahmen zu umgehen, sowie jeden Verlust oder jede Kompromittierung eines Geräts oder Zugangs, der für Stufe C genutzt wird. In jedem dieser Fälle setzt er den Zugriff der Stufe C aus, informiert den Verantwortlichen innerhalb der Frist nach B.5 und behandelt den Vorgang nach Klausel 9.2, soweit eine Verletzung des Schutzes personenbezogener Daten vorliegt. Der Verantwortliche kann die betroffenen Personen oder den Unterauftragsverarbeiter von weiteren Zugriffen der Stufe C ausschließen.
11. **Rechtliche Einordnung.**

a. Die Parteien sind sich einig, dass ein Fernzugriff aus einem Drittland, einschließlich der Anzeige auf einem Bildschirm, eine Übermittlung personenbezogener Daten im Sinne von Kapitel V DSGVO ist, auch wenn die Daten nicht außerhalb der EU bzw. des EWR gespeichert werden.

b. Zugriff der Stufe C erfolgt daher nur nach B.4 Nr. 2 und mit den Maßnahmen in Anhang V. Dieser Abschnitt ergänzt Teil A und die Standardvertragsklauseln nach B.4 Nr. 2 und schränkt sie nicht ein.

c. Die Maßnahmen nach Nr. 4 sollen das Kopieren, Herunterladen und Weiterleiten personenbezogener Daten verhindern. Sie können nicht verhindern, dass eine Person das Angezeigte liest, notiert oder fotografiert. Dieses Restrisiko wird verringert durch die Beschränkung auf benannte, schriftlich zur Vertraulichkeit verpflichtete Personen, durch Datenminimierung nach Nr. 9 und durch Protokollierung und Aufzeichnung nach Nr. 6.

d. Der Verantwortliche bleibt dafür verantwortlich, Übermittlungen der Stufe C in seinem Verzeichnis von Verarbeitungstätigkeiten und in seinen Datenschutzinformationen abzubilden. Der Auftragsverarbeiter stellt die dafür nötigen Informationen bereit.

12. **Weitergabe der Pflichten.** Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter, der Zugriff der Stufe C erhalten kann, die Pflichten dieses Abschnitts schriftlich auf (Klausel 7.7 b) und bleibt dem Verantwortlichen für deren Erfüllung voll verantwortlich (Klausel 7.7 d).

B.3 Weisungen

Der Hauptvertrag und dieser Vertrag sind die anfänglichen dokumentierten Weisungen des Verantwortlichen. Weitere Weisungen erteilen die in Anhang I genannten Personen in Textform (z. B. E-Mail oder Ticket). Mündliche Weisungen werden unverzüglich in Textform bestätigt. Der Auftragsverarbeiter nutzt personenbezogene Daten nicht für eigene Zwecke, nicht zum Training von KI-Modellen und nicht für Werbung.

B.4 Unterauftragsverarbeiter und Übermittlungen

1. Die Unterrichtung nach Klausel 7.7 a) erfolgt mindestens 30 Tage im Voraus in Textform und nennt Name, Standort, Leistungen und Zugriffsstufe des Unterauftragsverarbeiters. Der Verantwortliche kann innerhalb dieser Frist aus berechtigten datenschutzrechtlichen Gründen widersprechen. Einigen sich die Parteien nicht, kann der Verantwortliche die betroffenen Leistungen zu dem Zeitpunkt kündigen, zu dem die Änderung wirksam würde; bis dahin setzt der Auftragsverarbeiter den neuen Unterauftragsverarbeiter nicht für personenbezogene Daten des Verantwortlichen ein.

2. Ein Zugriff der Stufe C durch einen Unterauftragsverarbeiter außerhalb der EU bzw. des EWR erfolgt erst, nachdem der Auftragsverarbeiter (Datenexporteur) und dieser Unterauftragsverarbeiter (Datenimporteur) die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer, Modul 3 (Auftragsverarbeiter an Auftragsverarbeiter), Durchführungsbeschluss (EU) 2021/914 der Kommission, abgeschlossen haben (Klausel 7.8 b). Der Auftragsverarbeiter hat Recht und Praxis in Pakistan und in den Vereinigten Arabischen Emiraten bewertet und wendet die zusätzlichen Maßnahmen in Anhang V an. Die vollständige Bewertung stellt er dem Verantwortlichen auf Anfrage zur Verfügung.
3. Wird ein Übermittlungsinstrument unwirksam oder kann es nicht mehr eingehalten werden, stellt der Auftragsverarbeiter die Übermittlung unverzüglich ein und informiert den Verantwortlichen. Die betroffenen Arbeiten werden bis zu einer Einigung der Parteien nur auf Stufe A oder B fortgeführt.
4. Die Verträge mit Unterauftragsverarbeitern enthalten die nach Klausel 7.7 e) erforderliche Drittbegünstigtenklausel.

B.5 Verletzungen des Schutzes personenbezogener Daten

Die Meldung nach Klausel 9.2 erfolgt unverzüglich, spätestens **innerhalb von 24 Stunden**, nachdem der Auftragsverarbeiter von der Verletzung Kenntnis erlangt hat, an die in Anhang I genannte Kontaktstelle. Die Meldung an die Aufsichtsbehörde und die Benachrichtigung der betroffenen Personen bleiben Entscheidung des Verantwortlichen.

B.6 Kontrollen (Klausel 7.6)

1. Der Auftragsverarbeiter beantwortet zunächst Sicherheitsfragebögen des Verantwortlichen und stellt Unterlagen bereit. Reicht dies nicht aus, kann der Verantwortliche oder ein zur Verschwiegenheit verpflichteter unabhängiger Prüfer Kontrollen einschließlich Inspektionen durchführen, in der Regel einmal je Kalenderjahr, mit mindestens 30 Tagen Vorlauf, zu den Geschäftszeiten und ohne unzumutbare Störung des Betriebs. Bei Anhaltspunkten für Verstöße, nach einer Datenschutzverletzung oder auf Verlangen einer Aufsichtsbehörde sind Kontrollen jederzeit mit angemessenem Vorlauf möglich.
2. Kontrollen beim Lieferpartner können aus der Ferne durchgeführt werden.
3. Jede Partei trägt ihre eigenen Kosten einer Kontrolle. Ergibt eine Kontrolle einen wesentlichen Verstoß des Auftragsverarbeiters gegen diesen Vertrag, trägt er die angemessenen Kosten der Kontrolle.

B.7 Anfragen von Behörden

Verlangt eine Behörde eines Drittlands vom Auftragsverarbeiter oder einem Unterauftragsverarbeiter Zugang zu personenbezogenen Daten des Verantwortlichen, wird der Auftragsverarbeiter (und vertraglich der Unterauftragsverarbeiter), soweit rechtlich zulässig, den Verantwortlichen unverzüglich informieren, die Rechtmäßigkeit der Anfrage prüfen, sie bei begründeten Zweifeln anfechten, nur das gesetzlich erforderliche Minimum offenlegen und die Anfrage dokumentieren.

B.8 Rückgabe und Löschung (Klausel 10 d)

Nach Ende der Leistungen gibt der Auftragsverarbeiter die personenbezogenen Daten nach Wahl des Verantwortlichen innerhalb von **30 Tagen** zurück oder löscht sie, einschließlich der Kopien bei Unterauftragsverarbeitern, sofern nicht nach Unionsrecht oder dem Recht der Mitgliedstaaten eine Speicherpflicht besteht. Sicherungskopien werden im regulären Zyklus überschrieben, spätestens innerhalb von 90 Tagen. Der Auftragsverarbeiter bestätigt die Löschung in Textform. Quellcode und Dokumentation ohne personenbezogene Daten richten sich nach dem Hauptvertrag.

B.9 Kosten der Unterstützung

Unterstützung nach den Klauseln 8 und 9 erfolgt ohne gesonderte Vergütung, soweit sie aus der Sphäre des Auftragsverarbeiters oder aus seinen gesetzlichen Pflichten folgt. Sonstige Unterstützung kann nach vorheriger Ankündigung zu den Sätzen des Hauptvertrags berechnet werden.

B.10 Haftung

Für die Haftung gegenüber betroffenen Personen gilt Artikel 82 DSGVO. Im Verhältnis der Parteien gilt der Hauptvertrag, soweit zwingendes Recht nichts anderes bestimmt.

B.11 Schlussbestimmungen

1. Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform (§ 126b BGB) und müssen ausdrücklich auf diesen Vertrag Bezug nehmen. Die Anhänge I und IV können durch Mitteilung nach B.4 aktualisiert werden.
2. Dieser Vertrag kann in elektronischer Form geschlossen werden (Artikel 28 Absatz 9 DSGVO).
3. Ist eine Bestimmung von Teil B unwirksam, bleiben die übrigen Bestimmungen wirksam.
4. Für Teil B gilt deutsches Recht. Ist der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder hat er keinen allgemeinen Gerichtsstand in Deutschland, ist Gerichtsstand Berlin.

Anhang I – Liste der Parteien

Verantwortlicher	
Name	[Firma des Kunden]
Anschrift	[Anschrift]
Kontaktperson, Funktion, Kontaktdaten	[Name, Funktion, E-Mail, Telefon]
Weisungsberechtigte Personen	[Name, E-Mail]; Vertretung [Name, E-Mail]
Datenschutzbeauftragte/r (falls vorhanden)	[Name, E-Mail]
Kontaktstelle für Datenschutzverletzungen (B.5)	[E-Mail, Telefon]
Stufe C: Notfallkontakt und Prüfnummer (B.2a Nr. 2 e–f)	[Name, E-Mail, rund um die Uhr erreichbare Telefonnummer – oder „Stufe C wird nicht genutzt“]

Auftragsverarbeiter	
Name	SolutionPlus UG (haftungsbeschränkt), Amtsgericht Charlottenburg HRB 291768 B
Anschrift	Kollwitzstraße 76, 10435 Berlin
Kontaktperson, Funktion, Kontaktdaten	Saif Ur Rehman Qureshi, Geschäftsführer, info@solutionplus.io, +49 176 47658461
Weisungsempfänger	Saif Ur Rehman Qureshi; Vertretung: die im Hauptvertrag genannte Projektleitung
Datenschutzbeauftragte/r	Nicht erforderlich (§ 38 BDSG: weniger als 20 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt). Ansprechpartner Datenschutz: info@solutionplus.io
Kontaktstelle für Datenschutzverletzungen (B.5)	info@solutionplus.io, +49 176 47658461

Ort, Datum

Ort, Datum

Verantwortlicher – Name, Funktion

Auftragsverarbeiter – Saif Ur Rehman Qureshi, Geschäftsführer, SolutionPlus UG (haftungsbeschränkt)

Anhang II – Beschreibung der Verarbeitung

Punkt	**Angaben**
Kategorien betroffener Personen	☐ Kunden und Endnutzer des Verantwortlichen ☐ Beschäftigte des Verantwortlichen ☐ Interessenten ☐ Lieferanten und Geschäftspartner ☐ Sonstige: […]
Kategorien personenbezogener Daten	☐ Identifikations- und Kontaktdaten ☐ Konto- und Anmeldedaten ☐ Nutzungs- und Protokolldaten (IP-Adresse, Gerät, Zeitstempel) ☐ Vertrags- und Zahlungsdaten ☐ von Nutzern eingegebene Inhalte ☐ Kommunikationsdaten ☐ Standortdaten ☐ Sonstige: […]

Punkt	Angaben
Sensible Daten (Klausel 7.5) und Schutzmaßnahmen	☐ keine ☐ Gesundheitsdaten ☐ Sonstige: […] Falls angekreuzt: Zugriff auf Stufe A nur durch benannte Personen; Stufe C ausgeschlossen, sofern der Verantwortliche für diese Kategorie nicht ausdrücklich anders anweist; Anonymisierung vor jeder Nutzung in Testsystemen; Zugriffe im Zugriffsregister erfasst.
Art der Verarbeitung	☐ Entwicklung und Test ☐ Bereitstellung und Betrieb ☐ Wartung und Fehlerbehebung ☐ technischer Support ☐ Datenmigration ☐ Hosting ☐ KI-Funktionen (Anbieter in Anhang IV) ☐ Sonstige: […]
Zweck(e)	Erbringung der Leistungen nach dem Hauptvertrag: [Kurzbeschreibung, z. B. Entwicklung und Betrieb der Webanwendung „…“]
Dauer	Laufzeit des Hauptvertrags zuzüglich der Frist für Rückgabe und Löschung (B.8).
Genutzte Zugriffsstufen (B.2)	☑ Stufe A ☐ Stufe B ☐ Stufe C geplant für: [Aufgabe, Zeitraum]
Verarbeitung durch Unterauftragsverarbeiter	Lieferpartner: Stufe B, keine personenbezogenen Daten; Stufe C nur auf dokumentierte Weisung für die darin genannte Aufgabe und Dauer. Hosting und weitere Anbieter: wie in Anhang IV, für die Laufzeit des Hauptvertrags.

Anhang III – Technische und organisatorische Maßnahmen

Nr.	Maßnahme	Umsetzung
1	EU-Datengrenze und Zugriffsstufen	Produktivsysteme und personenbezogene Daten in der EU bzw. im EWR. Zugriff je Stufe (B.2): Stufe A für benannte Personen in der EU; Personen der Stufe B ohne Konten auf Systemen mit personenbezogenen Daten; Stufe C nur auf dokumentierte Weisung, befristet, namentlich und protokolliert. Zugriffslisten bei Projektbeginn und -ende sowie mindestens vierteljährlich geprüft.
2	Pseudonymisierung und Verschlüsselung	TLS 1.2 oder höher für alle Verbindungen; vom Hosting-Anbieter angebotene Verschlüsselung ruhender Daten aktiviert; vollständige Festplattenverschlüsselung aller Arbeitsgeräte; pseudonymisierte Kennungen in Protokollen und Testdaten, wo möglich.
3	Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit	Getrennte Entwicklungs-, Test- und Produktivumgebungen mit getrennten Zugangsdaten; Rollen nach dem Minimalprinzip; Produktivrechte nur für die Personen, die das System betreiben; Prüfung von Abhängigkeiten und Schwachstellen; Hosting bei etablierten Anbietern (Anhang IV).

Nr.	Maßnahme	Umsetzung
4	Wiederherstellung der Verfügbarkeit nach einem Zwischenfall	Betreibt der Auftragsverarbeiter das Hosting: automatische Sicherungen in der EU mit festgelegter Aufbewahrung und getestetem Wiederherstellungsverfahren. Betreibt der Verantwortliche das Hosting, ist er für Sicherungen verantwortlich; Code und Konfiguration liegen in der Versionsverwaltung, sodass die Anwendung neu bereitgestellt werden kann.
5	Regelmäßige Überprüfung und Bewertung	Überprüfung dieser Maßnahmen mindestens einmal jährlich und nach wesentlichen Änderungen (neue Werkzeuge, personelle Wechsel, Vorfälle); Zugriffsprüfungen wie unter Nr. 1.
6	Identifizierung und Autorisierung	Nur persönliche Konten, keine geteilten Konten; Mehr-Faktor-Authentifizierung, wo unterstützt; Passwortmanager; Entzug der Zugänge innerhalb von 24 Stunden, wenn eine Person das Projekt verlässt; Zugangsdaten in einem Secrets-Speicher, nie im Quellcode, Rotation bei Ausscheiden.
7	Schutz bei der Übermittlung	Keine personenbezogenen Daten per unverschlüsselter E-Mail, Chat oder Wechseldatenträger. Datenaustausch (z. B. Migrationsexporte) nur über mit dem Verantwortlichen abgestimmte verschlüsselte Wege, Löschung nach Gebrauch.
8	Schutz bei der Speicherung	Keine lokalen Kopien von Produktivdaten; eine unvermeidbare temporäre Kopie für eine Aufgabe der Stufe A ist verschlüsselt, auf das Nötige beschränkt und wird nach der Aufgabe gelöscht. Keine personenbezogenen Daten in Quellcode, Tickets oder Screenshots.
9	Physische Sicherheit	Abschließbare Büros und Heimarbeitsplätze; Geräte nicht unbeaufsichtigt an öffentlichen Orten; Rechenzentrumssicherheit der Hosting-Anbieter gemäß deren Zertifizierungen.
10	Protokollierung	Zugriffe auf Produktivsysteme werden von der jeweiligen Plattform protokolliert (z. B. Cloud-Audit-Logs); Zugriffe der Stufe C zusätzlich im Zugriffsregister (B.2 Nr. 4); Aufbewahrung der Protokolle mindestens 6 Monate, sofern der Verantwortliche nichts anderes vorgibt.
11	Systemkonfiguration einschließlich Standardkonfiguration	Gehärtete Standardkonfiguration der Arbeitsgeräte (aktuelles Betriebssystem, automatische Updates, Bildschirmsperre, Endpoint-Schutz, keine Standardpasswörter); Anwendungskonfiguration versioniert; Änderungen geprüft.
12	Interne IT- und IT-Sicherheits-Governance	Benannte Verantwortung für Zugriffsverwaltung und Gerätesicherheit; schriftliche interne Regeln zu Passwörtern, Umgang mit Kundendaten, Meldung von Vorfällen und Nutzung von KI-Werkzeugen; Code-Review (Vier-Augen-Prinzip) vor jedem Release.

Nr.	Maßnahme	Umsetzung
13	Zertifizierung und Qualitätssicherung	Der Auftragsverarbeiter ist derzeit nicht zertifiziert. Hosting-Anbieter werden nach anerkannten Zertifizierungen (z. B. ISO/IEC 27001) ausgewählt. Der Auftragsverarbeiter beantwortet Sicherheitsfragebögen und lässt Kontrollen zu (B.6).
14	Datenminimierung	Entwicklung und Test mit synthetischen oder anonymisierten Daten; Zugriff nur auf die für eine Aufgabe erforderlichen personenbezogenen Daten; keine zusätzlichen Kopien.
15	Datenqualität	Validierungs- und Plausibilitätsprüfungen in der Anwendung wie mit dem Verantwortlichen festgelegt; im Support bemerkte Unrichtigkeiten werden dem Verantwortlichen gemeldet (Klausel 8 c) Nr. 3).
16	Begrenzte Speicherdauer	Aufbewahrungs- und Löschregeln des Produktivsystems legt der Verantwortliche fest; sie werden wie vorgegeben umgesetzt; temporäre Daten auf Arbeitsgeräten werden nach der Aufgabe, spätestens bei Projektende gelöscht; Löschung nach B.8.
17	Rechenschaftspflicht	Dokumentation der Zugriffsrechte, Weisungen, des Zugriffsregisters der Stufe C und dieser Maßnahmen; schriftliche Vertraulichkeitsverpflichtung und Unterweisung jeder Person (Klausel 7.4 b); Auffrischung mindestens einmal jährlich.
18	Datenübertragbarkeit und Löschung	Export- und Löschfunktionen in der Anwendung wie mit dem Verantwortlichen festgelegt; Rückgabe oder Löschung der beim Auftragsverarbeiter vorhandenen personenbezogenen Daten nach B.8.
19	Nutzung von KI-Werkzeugen	KI-Werkzeuge nur mit Einstellungen oder Verträgen, die die Nutzung von Eingaben zum Training ausschließen; personenbezogene Daten des Verantwortlichen nur in KI-Dienste, die in Anhang IV aufgeführt sind.
20	Unterstützung des Verantwortlichen (Klausel 8)	Anträge betroffener Personen werden innerhalb von 2 Arbeitstagen weitergeleitet; technische Unterstützung bei Auskunft, Berichtigung, Export und Löschung in der Anwendung; Informationen für Datenschutz-Folgenabschätzungen auf Anfrage.
21	Meldung von Datenschutzverletzungen (Klausel 9)	Meldung innerhalb von 24 Stunden (B.5) mit, soweit verfügbar: Zeitpunkt und Art des Vorfalls, betroffene Systeme und Daten, ungefähre Zahl betroffener Personen und Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen, Ansprechpartner; Ergänzungen unverzüglich.

Nr.	Maßnahme	Umsetzung
22	Kontrollierter Fernzugriff (Stufe C)	Nur aufgrund einer Freigabe des Verantwortlichen in Textform (B.2a): Benannte Personen verbinden sich per verschlüsseltem VPN und Mehr-Faktor-Authentifizierung mit einem virtuellen Desktop oder Sitzungs-Proxy in der EU bzw. im EWR; Zwischenablage, Datei-, Laufwerks-, Drucker- und USB-Umleitung deaktiviert, ausgehende Verbindungen beschränkt, kein direkter Weg zu Produktivsystemen. Konten standardmäßig gesperrt und befristet (höchstens 14 Tage); Sitzungen werden in einem EU-Speicher protokolliert und aufgezeichnet, den die zugreifenden Personen nicht verändern können (Protokolle 12 Monate, Aufzeichnungen 90 Tage).

Anhang IV – Unterauftragsverarbeiter

Der Verantwortliche genehmigt die folgenden Unterauftragsverarbeiter (Klausel 7.7 a), Option 2). Die in diesem Projekt genutzten Zeilen ankreuzen; Hosting- und Dienstanbieter des Projekts ergänzen.

Nutzung	Name und Anschrift	Ort der Verarbeitung	Beschreibung der Verarbeitung	Zugriffsstufe / Übermittlungsinstrument
☐	Tecsofiy Solutions (Pvt.) Ltd., [Sitzanschrift], Lahore, Pakistan	Pakistan	Lieferpartner: Softwareentwicklung, Design und Qualitätssicherung auf Entwicklungs- und Testsystemen	Stufe B: keine personenbezogenen Daten, keine Übermittlung. Stufe C nur auf Weisung: SCC Modul 3 (B.4, Anhang V)
☐	Solution Plus Tech Consultancy FZE, Business Centre, Sharjah Publishing City Free Zone, Sharjah, Vereinigte Arabische Emirate (verbundenes Unternehmen)	Vereinigte Arabische Emirate	[Rolle in diesem Projekt]	Stufe B: keine personenbezogenen Daten, keine Übermittlung. Stufe C nur auf Weisung: SCC Modul 3 (B.4, Anhang V)
☐	Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg	EU, Region [z. B. eu-central-1, Frankfurt]	Cloud-Hosting, Datenbanken, Speicher	EU; AV-Vertrag des Anbieters

Nutzung	Name und Anschrift	Ort der Verarbeitung	Beschreibung der Verarbeitung	Zugriffsstufe / Übermittlungsinstrument
☐	Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	EU	E-Mail und Zusammenarbeit (Microsoft 365) für die Projektkommunikation	EU; AV-Vertrag des Anbieters
☐	[Name, Anschrift]	[…]	[…]	[…]

Anhang V – Bewertung der Übermittlungsrisiken: Zusammenfassung

Weder für Pakistan noch für die Vereinigten Arabischen Emirate gibt es einen Angemessenheitsbeschluss der EU. Beide Unterauftragsverarbeiter außerhalb der EU bzw. des EWR arbeiten deshalb standardmäßig auf Stufe B: Sie haben weder Konten auf noch technische Zugangswege zu Systemen mit personenbezogenen Daten des Verantwortlichen, sodass keine personenbezogenen Daten an sie übermittelt werden. Dieser Anhang regelt nur eine Ausnahme der Stufe C.

Punkt	Pakistan (Lieferpartner)	Vereinigte Arabische Emirate (verbundenes Unternehmen)
Angemessenheitsbeschluss (Art. 45 DSGVO)	Keiner.	Keiner (Liste der Angemessenheitsbeschlüsse der Europäischen Kommission, geprüft am 17. November 2026).
Lokales Datenschutzrecht	Kein umfassendes Datenschutzgesetz in Kraft; die Personal Data Protection Bill ist vom Parlament nicht verabschiedet (Stand geprüft am 16. November 2026: Chambers, *Data Protection & Privacy 2026 – Pakistan*; ICLG, *Data Protection Laws and Regulations 2026 – Pakistan*). Behördliche Zugriffe richten sich insbesondere nach dem Prevention of Electronic Crimes Act 2016.	Föderales Gesetzesdekret Nr. 45 von 2021 zum Schutz personenbezogener Daten (PDPL). Es gilt in der Sharjah Publishing City Free Zone, weil es nur Freizonen mit eigener Datenschutzgesetzgebung ausnimmt, etwa DIFC und ADGM (Artikel 2). Die Ausführungsverordnung war noch nicht erlassen (Chambers, *Data Protection & Privacy 2026 – UAE*, geprüft am 17. November 2026). Die EU hat das PDPL nicht als im Wesentlichen gleichwertig anerkannt; der Auftragsverarbeiter stützt den Schutz der personenbezogenen Daten des Verantwortlichen nicht darauf.

Punkt	Pakistan (Lieferpartner)	Vereinigte Arabische Emirate (verbundenes Unternehmen)
Was als Übermittlung gilt	Das Bereitstellen personenbezogener Daten an ein anderes Unternehmen in einem Drittland, einschließlich Fernzugriff und Anzeige auf einem Bildschirm (EDSA-Leitlinien 05/2021 zum Zusammenspiel von Artikel 3 und Kapitel V DSGVO, Version 2.0 vom 14. Februar 2023). Das verbundene Unternehmen ist eine eigene juristische Person; ein Zugriff durch es ist eine Übermittlung wie ein Zugriff durch den Lieferpartner.	
Bewertung	Der Auftragsverarbeiter geht nicht davon aus, dass vertragliche Garantien allein für einen Zugriff auf Klardaten aus einem der beiden Länder ein im Wesentlichen gleichwertiges Schutzniveau sichern (vgl. EDSA-Empfehlungen 01/2020, Version 2.0). Er arbeitet daher für beide standardmäßig auf Stufe B: Es gelangen keine personenbezogenen Daten zum Lieferpartner oder zum verbundenen Unternehmen, und es findet keine Übermittlung statt.	
Übermittlungsinstrument für Stufe C	Standardvertragsklauseln, Modul 3, Durchführungsbeschluss (EU) 2021/914 der Kommission, zwischen dem Auftragsverarbeiter (Exporteur) und dem jeweiligen Unterauftragsverarbeiter (Importeur). Vor ihrem Abschluss findet kein Zugriff der Stufe C statt.	
Zusätzliche Maßnahmen für Stufe C	Zugriff nur aufgrund einer Stufe-C-Freigabe in Textform für eine bestimmte Aufgabe und einen Zeitraum von höchstens 14 Tagen, durch benannte Personen (B.2a). Der Zugriff ist reine Anzeige, über ein verschlüsseltes VPN und einen virtuellen Desktop oder Sitzungs-Proxy in der EU bzw. im EWR, mit Mehr-Faktor-Authentifizierung. Kopier-, Dateiübertragungs- und Druckfunktionen sind deaktiviert und ausgehende Verbindungen beschränkt, sodass der Importeur keine gespeicherte Kopie der Daten besitzt, die herausgegeben oder beschlagnahmt werden könnte. Wo die Aufgabe es zulässt, werden maskierte oder pseudonymisierte Ansichten genutzt, mit Zuordnungsschlüsseln in der EU; sensible Daten sind ausgeschlossen, sofern nicht ausdrücklich freigegeben. Sitzungen werden in der EU protokolliert und aufgezeichnet und im Zugriffsregister erfasst. Der Zugriff wird sofort ausgesetzt bei Ablauf des Zeitraums, bei Widerruf, bei jeder behördlichen Anfrage (B.7) oder bei einer relevanten Rechtsänderung. Restrisiko: Angezeigte Daten sind für die benannten Personen im Klartext lesbar und können notiert oder fotografiert werden; der Verantwortliche wird vor jeder Freigabe darauf hingewiesen und entscheidet, ob er es akzeptiert.	
Von Stufe C ausgeschlossen, sofern nicht ausdrücklich angewiesen	Sensible Daten (Klausel 7.5).	
Überprüfung	Mindestens jährlich und bei jeder Änderung der Rechtslage in Pakistan oder den Vereinigten Arabischen Emiraten, insbesondere wenn Pakistan ein Datenschutzgesetz erlässt oder die VAE die Ausführungsverordnung zum PDPL erlassen.	