**Standardvertragsklauseln 2021/915**

**Verantwortlicher zu Auftragsverarbeiter**

**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.

(b) 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**

**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.

**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 dreißig 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.

**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.

**ANHANG I**

**Liste der Parteien**

**Verantwortliche(r):** **[Name und Kontaktdaten des/der Verantwortlichen und gegebenenfalls des Datenschutzbeauftragten des Verantwortlichen**]

**Verantwortliche Nummer** d

Name: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Anschrift: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Name, Funktion und Kontaktdaten der Kontaktperson: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Gegebenenfalls der Datenschutzbeauftragter des Verantwortlichen: Bitte klicken Sie hier, um einen Text hinzuzufügen.

|  |  |
| --- | --- |
| Beitrittsdatum: Bitte klicken Sie hier, um einen Text hinzuzufügen.  Vor- und Nachname (vollständig ausgeschrieben):  Bitte klicken Sie hier, um einen Text hinzuzufügen. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Unterschrift |

**Auftragsverarbeiter:** [**Name und Kontaktdaten des/der Auftragsverarbeiter/s und gegebenenfalls des Datenschutzbeauftragten des Auftragsverarbeiters**]

**Auftragsverarbeiter Nummer**: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Name: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Anschrift: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Name, Funktion und Kontaktdaten der Kontaktperson: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Gegebenenfalls der Datenschutzbeauftragter des Auftragsverarbeiters: Bitte klicken Sie hier, um einen Text hinzuzufügen.

|  |  |
| --- | --- |
| Beitrittsdatum: Bitte klicken Sie hier, um einen Text hinzuzufügen.  Vor- und Nachname (vollständig ausgeschrieben):  Bitte klicken Sie hier, um einen Text hinzuzufügen. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Unterschrift |

**ANHANG II**

**Beschreibung der Verarbeitung**

**Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden**

Kunden  Veranstaltungsteilnehmer

Angehörige der Mitarbeiter  Interessenten

Besucher  Bewerber

Mitarbeiter  Geschäftspartner

Auszubildende  Lieferanten

Kommunikationsteilnehmer  Praktikanten

Dienstleister  Berater

Studenten  Vertretungsberechtigte

Gesellschafter  Ansprechpersonen

Abonnenten

Andere. Bitte spezifizieren: Bitte klicken Sie hier, um einen Text hinzuzufügen.

**Kategorien der personenbezogenen Daten, die verarbeitet werden**

Namen  Merkmale, die Ausdruck der physischen Identität sind

Kennnummer  Merkmale, die Ausdruck der physiologischen Identität sind

Standortdaten  Merkmale, die Ausdruck der genetischen Identität sind

Online-Kennung  Merkmale, die Ausdruck der psychischen Identität sind

Merkmale, die Ausdruck der wirtschaftlichen Identität sind

Merkmale, die Ausdruck der kulturellen Identität sind

Merkmale, die Ausdruck der sozialen Identität sind

Kundendaten  Daten von Veranstaltungsteilnehmern

Daten von Angehörigen (Mitarbeiter)  Interessentendaten

Besucherdaten  Bewerberdaten

Mitarbeiterdaten  Geschäftspartner-Daten

Daten von Auszubildenden  Lieferantendaten

Daten von Kommunikationsteilnehmern  Praktikantendaten

Dienstleisterdaten  Beraterdaten

Daten von Studenten  Daten von Vertretungsberechtigten

Gesellschafterdaten  Daten von Ansprechpersonen

Abonnentendaten

Andere. Bitte spezifizieren: Bitte klicken Sie hier, um einen Text hinzuzufügen.

**Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen**

**Verarbeitete sensible Daten**

Rassische Herkunft  Ethnische Herkunft

Politische Meinung  Religiöse Überzeugung

Weltanschauliche Überzeugung  Gewerkschaftszugehörigkeit

Genetische Daten  Biometrische Daten

Gesundheitsdaten  Daten zum Sexualleben

Daten zur sexuellen Orientierung  Daten über strafrechtliche Verurteilungen

Daten über Straftaten

Bitte klicken Sie hier, um einen Text hinzuzufügen.

**Angewandte Beschränkungen oder Garantien**

Strenge Zweckbindung

Zugangsbeschränkungen

Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben

Aufzeichnungen über den Zugang zu den Daten

Beschränkungen für Weiterübermittlungen

Zusätzliche Sicherheitsmaßnahmen. Bitte spezifizieren: Bitte klicken Sie hier, um einen Text hinzuzufügen.

**Art der Verarbeitung**

Erheben  Anpassung  Offenlegung durch Übermittlung

Einschränkung  Erfassen  Veränderung

Verbreitung  Löschen  Organisation

Auslesen  and. Form d. Bereitstellung  Vernichtung

Ordnen  Abfragen  Abgleich

Speicherung  Verwendung  Verknüpfung

Bitte klicken Sie hier, um einen Text hinzuzufügen.

**Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden**

Bitte klicken Sie hier, um einen Text hinzuzufügen.

**Dauer der Verarbeitung**

Die Daten werden einmalig verarbeitet.

Die Daten werden langfristig verarbeitet.

Andere. Bitte spezifizieren: Bitte klicken Sie hier, um einen Text hinzuzufügen.

**Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.**

**Gegenstand der (Unter-)Auftragsverarbeitung:** Bitte klicken Sie hier, um einen Text hinzuzufügen.

**Art der (Unter-)Auftragsverarbeitung:** Bitte klicken Sie hier, um einen Text hinzuzufügen.

**Dauer der (Unter-)Auftragsverarbeitung:** Bitte klicken Sie hier, um einen Text hinzuzufügen.

**ANHANG III**

**Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten**

Beschreibung der von dem/den Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen.

**Bei den bereits angekreuzten technischen und organisatorischen Sicherheitsmaßnahmen handelt es sich um den Mindeststandard, den Sie bei einer Zusammenarbeit mit dem Verantwortlichen einhalten müssen. Sind diese technischen und organisatorischen Sicherheitsmaßnahmen bei Ihnen nicht umgesetzt, so informieren Sie den Verantwortlichen bitte umgehend. Alle zusätzlich von Ihnen getroffenen technischen und organisatorischen Sicherheitsmaßnahmen müssen Sie ergänzen!**

1. **Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten**

☒ Pseudonymisierung von nicht mehr im Klartext  Richtlinie zur Pseudonymisierung

benötigten personenbezogenen Daten  Verschlüsselung von Datenträgern

Pseudonymisierung von Daten in Testsystemen ☒ Verschlüsselung von Webseiten (SSL)

Verschlüsselung von Datenbanken ☒ E-Mail-Verschlüsselung (TLS 1.2 oder 1.3)

Verschlüsselung von Passwörtern und Schlüsseln  Verschlüsselung mobiler Geräte

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung**

☒ Vertraulichkeitsvereinbarungen mit Mitarbeitern ☒ NDAs mit Dritten

☒ Datenschutzverpflichtung der Mitarbeiter  Externer Speicher / Backup-Server

Supportverträge mit Dritten  Daten-Outsourcing-Vereinbarungen

Nutzung der zertifizierten Microsoft Cloud  Nutzung der zertifizierten Google Cloud

Nutzung der zertifizierten Amazon Cloud  Nutzung zertifizierter Cloud-Anbieter

☒ Firewall ☒ Antivirenprogramm

☒ Regelmäßige Datensicherungen  Redundante Systeme

Überwachung von Systemen und Diensten  RAID-Systeme

Netzgebundener Speicher (NAS)  Wartungsverträge

Regelmäßige IT-Störfalltests  Interne Speicherung von Kopien / Backups

Unterbrechungsfreie Stromversorgung (UPS)  Brand- und Rauchmeldeanlagen

Geräte zur Überwachung von Temperaturen  Ausrüstung zur Brandbekämpfung

Alarmwarnung bei unberechtigtem Zugriff  Load-Balancing

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen**

☒ Regelmäßige Backups des gesamten Systems  Speicherung auf mehreren Systemen

Erstellung eines Datensicherungskonzepts ☒ Regelmäßiger Test Backup/Recovery

Hardware-Support- und Serviceverträge  Notfallvorsorgekonzept

Ausgelagerte Datensicherung ☒ Regelmäßige Schulung des IT-Personals

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung**

☒ Interne Kontrollen ☒ Regelmäßige Überprüfung der IT-Prozesse

☒ Regelmäßige Audits (z.B. durch den DSB)  Regelmäßige Überprüfung der Verfahren

TOM-Audit durch den DSB  Regelmäßige Checks der Mitarbeiter

Durchführung von Folgenabschätzungen  Check Technikgestaltung / Voreinstellungen

Einführung eines Datenschutzmanagementsystems (DPMS) / Datenschutzhandbuch

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen zur Identifizierung und Autorisierung der Nutzer**

Zwei-Faktor-Authentifizierung ☒ Auth. mit Benutzername / Passwort

Rollentrennung von Test- und Produktivsystem ☒ Regelm. Prüfung von Berechtigungen

BIOS-Passwörter  Erstellung eines Berechtigungskonzepts

Richtlinie zur Verwaltung mobiler Geräte  Erstellung von Benutzerprofilen

☒ Passwort-Richtlinie ☒ Begrenzung der Anzahl der Admins

Identifikation von neuen Mitarbeitern  Trennung der Benutzerrollen

Automatische Verriegelungsmechanismen  Identifikation Externer mit Ausweisen

☒ Verwaltung der Rechte durch einen Admin ☒ Unterscheidung zwischen Berechtigungen

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen zum Schutz der Daten während der Übermittlung**

☒ Einsatz von Verschlüsselungstechnologien  VPN

☒ Protokollierung von Aktivitäten und Ereignissen  Transport über eine private Cloud

Dokumentation der Datenempfänger ☒ E-Mail-Verschlüsselung (TLS 1.2 oder 1.3)

Verifizierung der Identität des Empfängers ☒ Verwendung nicht öffentlicher Laufwerke

Physischer Transport: sichere Transportbehälter  Sorgfältige AuswahlTransportpersonal

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen zum Schutz der Daten während der Speicherung**

Verschlüsselung von Datenträgern  Datenklassifizierung

Erstellung eines Berechtigungskonzepts  Zugriffsbeschränkung

☒ Protokollierung von Aktionen und Ereignissen  Sicherheitstüren

☒ Begrenzung der Anzahl der Administratoren  Schlüsselkarte / RFID-Zugang

Anonymisierung von Daten  Pseudonymisierung von Daten

Sichere Aufbewahrung von Datenträgern ☒ Firewall

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden**

Alarmanlage  Personenkontrolle / Pförtner

Schutz von Gebäudeschächten  Protokollierung der Besucher

Automatische Zugangskontrolle  Sorgfältige Auswahl des Reinigungspersonals

Chipkarten, Transponder  Sorgfältige Auswahl des Sicherheitspersonals

Schließsystem mit Codeschloss  Pflicht zum Tragen von Berechtigungsausweisen

☒ Manuelles Schließsystem  Zugriffskonzept

Biometrische Zugangssperre  Abschließbare Server-Schränke

Videoüberwachung der Eingänge  Türen mit einem Knauf auf der Außenseite

Lichtschranken / Bewegungsmelder  Besucher: Nur in Begleitung von Mitarbeitern

☒ Sicherheitsschlösser  Klingelanlage mit Kamera

☒ Verfahren zur Schlüsselausgabe  Büroräume mit Knauf von außen

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen**

Einsatz einer automatischen Protokollierung  Ereignisbericht-Erstellung

Benachrichtigung mit Echtzeit-Alarm ☒ Protokollierung auf Applikationsebene

Automatische Prüfung von Protokollen  Synchronisation der Systemuhren

☒ Regelmäßige manuelle Überprüfung der Protokolle  Autom. Konsolidierung von Ereignissen

Protokolle werden in der Anwendung gespeichert und automatisch an einen anderen Ort gesendet

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration**

Konfigurationsmanagement-Richtlinie vorhanden ☒ Prozess zu Konfigurationsänderungen

☒ Datenschutzgerechte Voreinstellungen  Check der Standardkonfigurationen

DSB an Konfiguration beteiligt  Definition von Standardkonfigurationen

IT-Sicherheitsbeauftragter an Konfiguration beteiligt ☒ Konfiguration durch Systemadministrator

Protokollierung von Konfigurationsänderungen ☒ Regelmäßige Schulung der IT-Mitarbeiter

Beachtung der Empfehlungen des Herstellers

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit**

☒ IT-Sicherheitsrichtlinie  IT-Administrationsrichtlinie

Regelmäßige Compliance-Audits / Überprüfungen  IT-Anlagenverzeichnis

☒ Schulung der Mitarbeiter zur Datensicherheit  Regelmäßige Systemprüfung/ -bewertung

☒ IT-Team mit klaren Rollen / Verantwortlichkeiten  Richtlinien für Ereignis-Management

Risikobewertung und Maßnahmen zum Risikomanagement auf allen Stufen und Ebenen

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten**

Einführung der ISO 9001 - Qualitätsmanagement

Einführung der ISO 27001 - Informationssicherheitsmanagement

Implementierung der ISO 27701 - Datenschutz-Informationsmanagement

DS-GVO-Zertifizierung – Datenschutzmanagement

☒ Klarer Überblick über die für Produkte/Dienstleistungen/Prozesse geltenden Bestimmungen

Identifikation von branchenspezifischen Standards

☒ Regelmäßige interne und/oder externe Audits

☒ Zuweisung von Audit-Verantwortlichkeiten an zertifizierte Experten

Regelmäßige Überprüfung auf neue Voraussetzungen und Erneuerung von Zertifikaten

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen zur Gewährleistung der Datenminimierung**

☒ Identifikation des Zwecks der Verarbeitung

☒ Bewertung des Zusammenhangs zwischen Verarbeitung und Zweck

Beurteilung des Umfangs und der Qualität der verarbeiteten Daten in Bezug auf den Zweck

☒ Identifikation der geltenden Aufbewahrungsfristen

☒ Sichere Löschung der Daten nach Ablauf der Aufbewahrungsfrist

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen zur Gewährleistung der Datenqualität**

Datenprofilierung und –klassifizierung  Kontrolle eingehender oder neuer Daten

☒ Protokollierung Eingabe/Änderung Daten ☒ Rechtevergabe zur Dateneingabe

Aufbewahrung von Protokollen ☒ Nachvollziehbarkeit der Benutzer bei Eingabe,

Vermeidung von doppelten Daten Änderung von Daten (keine Benutzergruppen)

Identifizierung von Anforderungen an Daten  Anwendung von Maßnahmen zur Datenqualität

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung**

Aufbewahrungsrichtlinie mit Rollen  Trennung der Daten nach Aufbewahrungsfristen

DSB berät zu Datenspeicherfristen ☒ Regelmäßige Schulungen

☒ Regelmäßige Prüfung und Bewertung der gespeicherten Daten

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen zur Gewährleistung der Rechenschaftspflicht**

☒ Schulungen / Sensibilisierung ☒ Regelmäßige Kontrollen und Prüfungen

Aufbau eines Datenschutzteams  Anleitung und Unterstützung f. Mitarbeiter

☒ Angemessene Richtlinien zum Datenschutz ☒ Abschluss von Standardvertragsklauseln

Vereinbarungen über gemeins. Verantwortlichkeit  Beantwortung von Anfragen Betroffener

Transparenzdokument (Art.13 / 14 DSGVO) ☒ Sichere Datenlöschung

☒ Rechtsgrundlage besteht für alle Aktivitäten ☒ Dokumentierte Datenschutzerklärung

Auditberichte und Maßnahmen sind dokumentiert  Ordnungsgemäße Einbeziehung des DSB

Spezifisches Einwilligungsverfahren / Aufbewahren von Einwilligungsprotokollen

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung**

☒ Speicherung in einem strukturiertem Format ☒ Überwachung gesetzlicher Fristen

Übertragung per End-to-End-Verschlüsselung ☒ Einhaltung von Aufbewahrungsfristen

☒ Ermöglichung der Datenübertragbarkeit ☒ Richtiger Umgang mit Betroffenenrechten

☒ Sichere Datenlöschung gewährleistet durch Beauftragung der Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Deutschland, E-Mail: info@notebook12.com (zertifiziertes Datenlöschungszertifikat).

☒ Sichere Datenträgervernichtung gewährleistet durch Beauftragung der Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, E-Mail: info@notebook12.com (zertifizierter Datenvernichtungsnachweis).

Bitte klicken Sie hier, um einen Text hinzuzufügen.

1. **Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-) Auftragsverarbeiter zur Unterstützung des Verantwortlichen und (bei Datenübermittlungen von einem Auftragsverarbeiter an einen Unterauftragsverarbeiter) zur Unterstützung des Datenexporteurs ergreifen muss.**

Standardvertragsklauseln (SCCs) werden unterzeichnet oder vereinbart

Implementierung der ISO 9001 - Qualitätsmanagement durch (Unter-) Auftragsverarbeiter

Implementierung der ISO 27001 - Management der Informationssicherheit durch (Unter-) Auftragsverarbeiter

Implementierung der ISO 27701 - Datenschutz Informationsmanagement durch (Unter-) Auftragsverarbeiter

DSGVO-Zertifizierung - Datenschutzmanagement durch (Unter-) Auftragsverarbeiter

☒ Sichere Datenlöschung gewährleistet durch Beauftragung von Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Deutschland, E-Mail: info@notebook12.com (zertifiziertes Datenlöschungszertifikat).

☒ Sichere Datenträgervernichtung gewährleistet durch Beauftragung von Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, E-Mail: info@notebook12.com (zertifizierter Datenvernichtungsnachweis).

☒ Vertraglich vereinbarte, wirksame Kontrollrechte

☒ Vertraglich vereinbarte Unterstützung des Verantwortlichen

Bitte klicken Sie hier, um einen Text hinzuzufügen.

**ANHANG IV**

**Liste der Unterauftragsverarbeiter**

ERLÄUTERUNG**:**

Dieser Anhang muss im Falle einer gesonderten Genehmigung von Unterauftragsverarbeitern ausgefüllt werden (**Klausel 7.7 Buchstabe a, Option 1**).

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt**:**

Name: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Anschrift: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Name, Funktion und Kontaktdaten der Kontaktperson: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden): Bitte klicken Sie hier, um einen Text hinzuzufügen.

Name: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Anschrift: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Name, Funktion und Kontaktdaten der Kontaktperson: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden): Bitte klicken Sie hier, um einen Text hinzuzufügen.

Name: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Anschrift: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Name, Funktion und Kontaktdaten der Kontaktperson: Bitte klicken Sie hier, um einen Text hinzuzufügen.

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden): Bitte klicken Sie hier, um einen Text hinzuzufügen.