ANHANG [●]

**Standardvertragsklauseln**

ABSCHNITT I

*Klausel 1*

***Zweck und Anwendungsbereich***

1. 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.
2. 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.
3. Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.
4. Die Anhänge I bis IV sind Bestandteil der Klauseln.
5. Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.
6. 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***

1. Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.
2. 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***

1. 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.
2. Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.
3. 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 - fakultativl*

***Kopplungsklausel***

1. 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.
2. 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.
3. 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**

1. 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.
2. 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**

1. 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.
2. 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**

1. Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
2. Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
3. 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.
4. 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.
5. 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**

|  |
| --- |
|[ ]  OPTION 1: VORHERIGE GESONDERTE GENEHMIGUNG: Der Auftragsverarbeiter darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag des Verantwortlichen gemäß diesen Klauseln durchführt, ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen an einen Unterauftragsverarbeiter untervergeben. Der Auftragsverarbeiter reicht den Antrag auf die gesonderte Genehmigung mindestens Choose an item. vor der Beauftragung des betreffenden Unterauftragsverarbeiters zusammen mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Verantwortlichen genehmigten Unterauftragsverarbeiter findet sich in Anhang IV. Die Parteien halten Anhang IV jeweils auf dem neuesten Stand.. |
|[ ]  OPTION 2: 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 Choose an item. 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. |

1. 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.
2. 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.
3. 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.
4. 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**

1. 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.
2. 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***

1. 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.
2. 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.
3. 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.

1. 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:

1. 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);
2. 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;

1. 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:

1. 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);
2. Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
3. 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***

1. 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.
2. 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.

1. 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.
2. 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*

**Vertragsparteien**

**Für die Verarbeitung Verantwortliche(r):** [*Identität und Kontaktdaten des/der für die Verarbeitung Verantwortlichen und ggf. des Datenschutzbeauftragten des für die Verarbeitung Verantwortlichen*].

Name: Click or tap here to enter text.

Anschrift: Click or tap here to enter text.

Name, Position und Kontaktdaten der Kontaktperson: Click or tap here to enter text.

Unterschrift: Click or tap here to enter text.

Datum: Click or tap to enter a date.

\* \* \* \*

**Auftragsverarbeiter:** *[Identität und Kontaktdaten des/der Auftragsverarbeiter(s) und ggf. des Datenschutzbeauftragten des Auftragsverarbeiters].*

Name: Click or tap here to enter text.

Anschrift: Click or tap here to enter text.

Name, Position und Kontaktdaten der Kontaktperson: Click or tap here to enter text.

Unterschrift: Click or tap here to enter text.

Datum: Click or tap to enter a date.

\* \* \* \*

 *ANHANG II*

**Beschreibung der Verarbeitung**

*Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden*

[ ]  Bewerber

[ ]  Verbraucher

[ ]  Vertreter von Händlern

[ ]  Mitarbeiter

[ ]  Familienangehörige von Arbeitnehmern

[ ]  Ehemalige Mitarbeiter

[ ]  Gäste

[ ]  Journalisten

[ ]  Mitglieder der Unternehmensorgane

[ ]  Inhaber von Vollmachten

[ ]  Vertreter von Lieferanten (Berater, Auftragnehmer, Agenten)

[ ]  Besucher

*Kategorien personenbezogener Daten, die verarbeitet werden*

[ ]  Informationen zur Identifizierung, bitte spezifizieren:

[ ]  Kontaktinformationen, bitte spezifizieren:

[ ]  Angaben zur Familie, bitte spezifizieren:

[ ]  Berufliche Informationen, bitte spezifizieren:

[ ]  Finanzielle Informationen, bitte präzisieren:

[ ]  Digitale Informationen, bitte spezifizieren:

[ ]  Sensible Informationen, bitte unten angeben (falls zutreffend):

[ ]  Andere Informationen, bitte spezifizieren:

*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*

*Art der Verarbeitung*

Erbringung der vertragsgemäßen Leistungen.

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

*Dauer der Verarbeitung*

Bis zur Beendigung der Dienstleistungen, sofern von Pirelli nicht schriftlich anders angegeben.

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

Erbringung der Dienstleistungen gemäß der Vereinbarung und bis zu deren Beendigung, sofern von Pirelli nicht schriftlich anders angegeben.

*Bei Übermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-)Auftragsverarbeiter treffen muss, um den für die Verarbeitung Verantwortlichen unterstützen zu können.*

[*Falls zutreffend]*

*ANHANG III*

**Technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit**

Im Folgenden sind die grundlegenden technischen und organisatorischen Maßnahmen aufgeführt, die Pirelli von Lieferanten, die als Auftragsverarbeiter ("**Lieferanten**") tätig sind, verlangt, um ein angemessenes Sicherheitsniveau der personenbezogenen Daten von Pirelli ("**personenbezogene Daten von Pirelli**") zu gewährleisten. Die nachstehende Liste ist zusammen mit allen anderen technischen Dokumenten, Checklisten oder Zertifizierungen zu lesen, die zwischen Pirelli und dem Lieferanten in Bezug auf technische und organisatorische Maßnahmen für die Verarbeitung personenbezogener Daten von Pirelli bestehen.

Falls Änderungen an den unten aufgeführten technischen und organisatorischen Basismaßnahmen erforderlich werden, muss der Lieferant Pirelli unverzüglich schriftlich über diese Änderungen informieren. Alle Änderungen müssen mit den unten aufgeführten grundlegenden Sicherheitsmaßnahmen übereinstimmen und dürfen niemals zu einer Verschlechterung dieser Maßnahmen führen.

## **RICHTLINIEN UND VERFAHREN**

Der Lieferant muss über Richtlinien und/oder Verfahren für die unten aufgeführten Bereiche verfügen. Diese Richtlinien und/oder Verfahren sind regelmäßig zu überprüfen.

**1.1 Rechenschaftspflicht**

Der Lieferant muss einen *"Ansprechpartner"* bestimmen, der für die IT-Sicherheit der Anlagen und Systeme, die zur Verarbeitung personenbezogener Daten von Pirelli verwendet werden, zuständig ist, und Pirelli die entsprechenden Einzelheiten mitteilen. Der Lieferant muss Pirelli außerdem im Voraus die Kontaktdaten des für die Meldung von Verletzungen des Schutzes personenbezogener Daten zuständigen Personals mitteilen. Soweit möglich, sollte der Lieferant auch die ständige Erreichbarkeit dieses Personals rund um die Uhr sicherstellen - insbesondere in Notfällen.

**1.2 Geschäftskontinuität**

Es müssen Sicherheitsanforderungen zur Gewährleistung von System-Backups und zur Planung der Geschäftskontinuität vorhanden sein, insbesondere in Bezug auf Anlagen, die zur Verarbeitung personenbezogener Daten von Pirelli verwendet werden. Insofern muss der Lieferant in der Lage sein, die Verfügbarkeit und den Zugang zu den personenbezogenen Daten von Pirelli rechtzeitig wiederherzustellen, um eine Unterbrechung des Dienstes zu vermeiden.

**1.3 Sicherheitsschulung und Anweisungen**

Es müssen gezielte Schulungsmaßnahmen zur Verbesserung des IT-Sicherheitsbewusstseins innerhalb der Unternehmensstruktur des Lieferanten durchgeführt werden. Die Mitarbeiter des Lieferanten erhalten detaillierte Anweisungen zur Geheimhaltung und Integrität ihrer Zugangsberechtigungen sowie zur sorgfältigen Verwahrung und zum Schutz der ihnen zugewiesenen Geräte, Werkzeuge und Systeme - unter besonderer Berücksichtigung derjenigen, die zur Verarbeitung personenbezogener Daten von Pirelli verwendet werden.

**1.4 Protokollierung und Überwachung**

Die vom Lieferanten zur Verarbeitung personenbezogener Daten von Pirelli verwendeten Systeme und Tools müssen über Protokollierungs- und Überwachungsmechanismen verfügen. Was die Protokollierung betrifft, so muss der Lieferant Protokolle erstellen und für den Zeitraum aufbewahren, der nach geltendem Recht vorgeschrieben ist (oder anderweitig mit Pirelli vereinbart wurde), und diese Protokolle in jedem Fall mindestens 6 (sechs) Monate nach ihrer Erstellung aufbewahren. Im Hinblick auf die Überwachung muss der Lieferant die Rückverfolgbarkeit aller Vorgänge, die mit den personenbezogenen Daten von Pirelli über seine Systeme und Instrumente durchgeführt werden, durch die Annahme und Umsetzung angemessener Rückverfolgungsmaßnahmen sicherstellen.

**1.5 Vermeidung von Datenverlusten**

Der Lieferant muss über Strategien und/oder Verfahren verfügen, die einen Datenexport außerhalb des Netzes des Lieferanten verhindern. Im Falle der Weitergabe personenbezogener Daten von Pirelli muss der Lieferant angemessene Vertraulichkeitsmaßnahmen ergreifen.

**1.6 Umgang mit Verletzungen des Schutzes personenbezogener Daten**

Der Lieferant muss über Richtlinien und/oder Verfahren für den Umgang mit Verletzungen des Schutzes personenbezogener Daten verfügen. Diese Richtlinien und Verfahren sollten dem Personal des Lieferanten bekannt sein und von ihm regelmäßig überprüft und kontrolliert werden.

## **2. ANLAGENVERWALTUNG**

**2.1 Anlagenverzeichnis**

Der Lieferant muss ein Inventar aller für die Verarbeitung personenbezogener Daten von Pirelli genutzten Anlagen vorhalten und auf dem neuesten Stand halten.

**2.2 Anlagenschutz**

Der Lieferant muss die zur Verarbeitung personenbezogener Daten von Pirelli verwendeten Anlagen gemäß internationalen Industriestandards und bewährten Verfahren schützen. Die Schutzmaßnahmen umfassen mindestens die Verwendung von Antivirus-Software, Firewalls, IDS/IPS-Modulen und Anti-Spam-Lösungen.

**2.3 Lifecycle Management**

Der Lieferant muss sicherstellen, dass alle Anlagen, die personenbezogene Daten von Pirelli verarbeiten, sowie alle Cybersicherheitslösungen, die für die Erbringung von Pirelli-Diensten erforderlich sind (z. B. Virenschutz, Firewalls, IDS/IPS-Module), stets auf die letzte verfügbare Softwareversion aktualisiert werden. Wenn Aktualisierungen nicht möglich sind oder noch nicht angewendet werden, muss der Lieferant einen Aktualisierungsplan und einen Gesamtplan zur Risikominderung festlegen, um alle relevanten Risiken im Zusammenhang mit der Veralterung des Systems zu bewältigen (z. B. Umsetzung der Trennung, Überwachung usw.).

**2.4 Cyber security Risikobewertung**

Der Lieferant führt eine Risikobewertung der IT-Systeme durch, die zur Erbringung der Dienstleistungen für Pirelli verwendet werden, und berücksichtigt dabei insbesondere alle Risiken, die mit der Verarbeitung personenbezogener Daten von Pirelli verbunden sind. Eine solche Risikobewertung erfolgt entweder jährlich oder wenn die geltenden Gesetze und Vorschriften dies vorschreiben.

## **3. VERSCHLÜSSELUNG**

**3.1 Verschlüsselungsmaßnahmen**

Unter Berücksichtigung des Stands der Technik und der Verschlüsselungstechniken wird der Lieferant die Verschlüsselung auf verschiedenen Ebenen durchführen:

* **Verschlüsselung im Ruhezustand:** Der Lieferant muss über geeignete Verschlüsselungstechniken verfügen, um die Vertraulichkeit der personenbezogenen Daten von Pirelli im Ruhezustand auf verschiedenen Ebenen zu schützen (z. B. vollständige Festplattenverschlüsselung auf Massenlaufwerken, transparente Datenverschlüsselung auf Datenbanken, Verschlüsselung auf Dateiebene).
* **Verschlüsselung während der Übertragung:** Der Lieferant muss über geeignete Verschlüsselungstechniken verfügen, um die Vertraulichkeit der personenbezogenen Daten von Pirelli während der Übertragung zu schützen (z. B. Netzwerkverschlüsselung, Anwendungsverschlüsselung usw.).
* **Verwaltung der Verschlüsselungsschlüssel**: Der Lieferant muss über geeignete Lösungen und ein definiertes Verfahren für die Verwaltung von Verschlüsselungsschlüsseln verfügen, die zumindest eine Trennung von Schlüsselbesitzern und Datenbesitzern gewährleisten.
* **Verwaltung von Verschlüsselungszertifikaten:** Der Lieferant muss über geeignete Lösungen und einen klaren und dokumentierten Prozess für die Verwaltung von Verschlüsselungszertifikaten verfügen. Dieses Verfahren ist entsprechend den in internationalen Industrienormen festgelegten Anforderungen (z. B. Mindestlänge der Verschlüsselungsschlüssel) zu entwickeln.

## **4. IDENTITÄTS- UND ZUGANGSMANAGEMENT**

**4.1 Zugang zu personenbezogenen Daten von Pirelli**

Der Lieferant gewährleistet, dass nur befugtes Personal mit entsprechender Sachkenntnis und Erfahrung in Datenschutzfragen Zugang zu den personenbezogenen Daten von Pirelli hat und dass dieses Personal zur Vertraulichkeit verpflichtet ist.

Der Lieferant führt eine Liste aller Personen (einschließlich aller Angestellten, Bevollmächtigten oder Auftragnehmer), die unter seiner Aufsicht oder unter der Aufsicht von Unterauftragsverarbeitern handeln und Zugang zu den personenbezogenen Daten von Pirelli haben oder diese anderweitig verarbeiten, und aktualisiert diese regelmäßig.

**4.2 Maßnahmen und Grundsätze zur Identifizierung und Autorisierung von Benutzern**

Der Lieferant muss Systeme für die Benutzerauthentifizierung und das Berechtigungsmanagement einrichten. Der Lieferant muss die Mindestzugriffsrechte auf personenbezogene Pirelli-Daten nach den Grundsätzen des "Least privilege and Need-to-know" vergeben (d. h. er darf nur auf die Daten zugreifen, die für die Erfüllung der jeweiligen Arbeitsfunktion erforderlich sind). Der Lieferant prüft auch die den Nutzern zu erteilenden Berechtigungen auf der Grundlage ihrer Rolle bei der Verarbeitung personenbezogener Pirelli-Daten sowie im Hinblick auf geltende rechtliche Anforderungen an das Identitäts- und Zugangsmanagement der Nutzer.

**4.3 Profil-Überprüfung**

Der Lieferant überprüft mindestens einmal jährlich die Konsistenz und das Vorhandensein von Benutzerautorisierungsprofilen und führt Buch über diese Aktivitäten, wenn sie sich auf persönliche Daten von Pirelli beziehen.

**4.4 Sicherheit der Zugangsberechtigungen**

Der Lieferant muss internationale Standards und bewährte Verfahren für die Sicherheitsanforderungen an alle Anlagen, die zur Verarbeitung personenbezogener Daten von Pirelli verwendet werden, übernehmen.

**4.5 Individuelle Zugangsberechtigungen**

Der Lieferant darf für alle Anlagen, die zur Verarbeitung personenbezogener Daten von Pirelli verwendet werden, nur individuelle Zugangsberechtigungen vergeben (insbesondere solche mit hohen Berechtigungen für Systeme und Anwendungen). Die Zuweisung und Verwendung von gemeinsam genutzten Zugangsberechtigungen ist strengstens untersagt.

**4.6 Gültigkeitsdauer der Zugangsberechtigungen**

Der Lieferant muss über ein klares Verfahren für die Gültigkeitsdauer der Zugangsberechtigungen verfügen. Dieses Verfahren muss sicherstellen, dass alle Zugangsdaten, die für den Zugriff auf Anlagen zur Verarbeitung personenbezogener Daten von Pirelli verwendet werden, automatisch nach einem bestimmten Zeitraum der Nichtnutzung durch die Nutzer ablaufen.

**5. PHYSISCHE SICHERHEIT**

**5.1 Sicherheit von Rechenzentren**

Der Lieferant muss über physische Sicherheitsmaßnahmen verfügen, die gemäß den wichtigsten Industriestandards und bewährten Praktiken entwickelt wurden, wie z. B. mindestens die Installation von Einbruchalarmanlagen und Videoüberwachungssystemen, sowohl für die Räumlichkeiten als auch für die Eingänge zu den Rechenzentren. Der Lieferant muss außerdem über Verfahren verfügen, die den physischen Zugang zu den Rechenzentren begrenzen (z. B. einbruchsichere Drehkreuze), unbefugte Aktivitäten verhindern und Zugangsaktivitäten melden (z. B. mehrere fehlgeschlagene Zugangsversuche).

**5.2 Standort von Rechenzentren**

Der Lieferant teilt Pirelli auf Anfrage die Standorte der Rechenzentren mit, die zur Verarbeitung der personenbezogenen Daten von Pirelli verwendet werden. Pirelli muss im Voraus über jede Änderung des Standorts der Rechenzentren informiert werden.

**6. SICHERHEITSMASSNAHMEN**

**6.1 Anlagensicherheit**

Der Lieferant muss geeignete Maßnahmen ergreifen, um die Schwachstellen der für die Verarbeitung personenbezogener Daten von Pirelli verwendeten Anlagen zu verringern, indem er angemessene Konfigurationen durchsetzt und unbefugte Änderungen vermeidet (z. B. Kontrolle von Wechseldatenträgern).

**6.2 Softwareentwicklung**

Bei der Entwicklung von Software, die zur Verarbeitung personenbezogener Daten von Pirelli verwendet wird, muss der Lieferant Richtlinien für die Erstellung sicheren Codes anwenden.

**6.3 Security patch management**

Der Lieferant muss die Installation und Deinstallation von Patches mit einem Verfahren verwalten, das nach den besten Praktiken und Standards der Branche entwickelt wurde und die Rückverfolgbarkeit und den zeitlichen Ablauf der Patching-Aktivitäten gewährleistet.

**6.4 Schwachstellenbewertung**

Der Lieferant muss einen Nachweis über die an seinen Systemen durchgeführten Schwachstellenbewertungen oder Penetrationstests vorlegen.

**7. DATENSCHUTZVERLETZUNG**

**7.1 Mitteilung an Pirelli**

Im Falle einer Verletzung des Schutzes personenbezogener Daten von Pirelli muss der Lieferant Pirelli unverzüglich über Personal\_Data\_Breach@pirelli.com benachrichtigen. Der Zeitplan für die Benachrichtigung über die Verletzung ist wie folgt:

1. **Wichtige Informationen** (einfache E-Mail-Mitteilung, die zumindest die in den einschlägigen Klauseln beschriebenen Elemente enthält): spätestens 12 Stunden, nachdem der Verstoß bekannt geworden ist.
2. **Vollständiger Bericht** (auf der Grundlage des Berichts über den Sicherheitsvorfall, der unter diesem [Link](https://psi-dotcom-prd.s3.eu-west-1.amazonaws.com/suppliers-portal/de-de/Security_Incident_Report_DE.docx) verfügbar ist, oder alternativ in einem speziellen Format des Lieferanten, das die im Pirelli-*Bericht über den Sicherheitsvorfall* geforderten Informationen enthält): spätestens 48 Stunden nach der Mitteilung der oben genannten Schlüsselinformationen.

*ANHANG IV*

**Liste der Unterauftragsverarbeiter**

Der für die Verarbeitung Verantwortliche hat den Einsatz der folgenden Unterauftragsverarbeiter genehmigt:

Name: Click or tap here to enter text.

Anschrift: Click or tap here to enter text.

Name, Position und Kontaktdaten der Kontaktperson: Click or tap here to enter text.

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter zugelassen sind):

Click or tap here to enter text.

\* \* \* \*