Vereinbarung zur Auftragsverarbeitung

ABSCHNITT I

1. Zweck und Anwendungsbereich

1.1. 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 sichergestellt werden.

1.2. 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.

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

1.4. Die Anhänge I bis IV sind Bestandteil der Klauseln.

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

1.6. 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.

2. Unabänderbarkeit der Klauseln

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

2.2. 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.

3. Auslegung

3.1. 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.

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

3.3. 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.

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.

5. Kopplungsklausel

5.1. 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.

5.2. Nach Ausfüllen und Unterzeichnen der unter 5.1 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.

5.3. 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

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.

7. Pflichten der Parteien

7.1. Weisungen

7.1.1. 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.

7.1.2. 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

7.4.1. 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.

7.4.2. 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 zusätzliche Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

7.6.1. Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

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

7.6.3. 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.

7.6.4. 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.

7.6.5. 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

7.7.1. 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.

7.7.2. 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.

7.7.3. 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.

7.7.4. 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.

7.7.5. 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

7.8.1. 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.

7.8.2. Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß 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.

8. Unterstützung des Verantwortlichen

8.1. 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.

8.2. 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 8.1 und 8.2 befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

8.3. Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß 8.2 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:

8.3.1. 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;

8.3.2. 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;

8.3.3. 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;

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

8.4. 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.

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:

9.1.1. 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);

9.1.2. 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:

9.1.2.1. 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;

9.1.2.2. die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

9.1.2.3. 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;

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:

9.2.1. 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);

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

9.2.3. 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

10. Verstöße gegen die Klauseln und Beendigung des Vertrags

10.1. 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.

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

10.2.1. der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß 10.1 ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

10.2.2. 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;

10.2.3. 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.

10.3. 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 7.1.2 verstoßen.

10.4. 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

1. Verantwortliche(r)

Der Verantwortliche ist der jeweilige Kunde; Name, Anschrift und Kontaktdaten ergeben sich aus den im Rahmen der Registrierung oder Vertragsbeziehung hinterlegten Daten.

2. Auftragsverarbeiter

Evolo Software GmbH, Görrestraße 48, 80797 München. Ansprechpartner: info@pictomento.com

Datenschutzkontakt des Auftragsverarbeiters

Für Anfragen zur Auftragsverarbeitung, zum Datenschutz sowie zur Unterstützung bei datenschutzrechtlichen Anliegen des Verantwortlichen kann der Auftragsverarbeiter unter der hierfür benannten Kontaktadresse kontaktiert werden:

Evolo Software GmbH
Görrestraße 48
80797 München
E-Mail: info@pictomento.com

Datenschutzbeauftragter des Auftragsverarbeiters
Der Auftragsverarbeiter hat einen Datenschutzbeauftragten benannt.
Dieser ist unter folgenden Kontaktdaten erreichbar:

Evolo Software GmbH
Datenschutzbeauftragter
Görrestraße 48
80797 München
E-Mail: info@pictomento.com

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

Nutzer, Besucher, Fotografen, Kunden der Fotografen, abgebildete Personen (Gäste).

Kategorien personenbezogener Daten, die verarbeitet werden

Name, E-Mail-Adresse, Nutzerverhalten, IP-Adresse, Logdaten, Authentifizierungsdaten, Profildaten, Abrechnungsdaten, Galeriemetadaten, Medien- und Inhaltsdaten (Fotos/Videos), EXIF-Metadaten, Gesichtserkennungsdaten.

Verarbeitete sensible Daten und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen

Verarbeitete sensible Daten
Biometrische Daten in Form von Gesichtserkennungsdaten, Embeddings sowie daraus abgeleiteten Zuordnungsinformationen.

Angewandte Beschränkungen oder Garantien
PictoMento kann eine optionale Funktion zur gesichtsbezogenen Zuordnung von Inhalten bereitstellen. Sofern diese Funktion durch den Kunden für eine bestimmte Galerie aktiviert wird, können eingeladenen Personen bevorzugt solche Inhalte angezeigt werden, auf denen sie voraussichtlich abgebildet sind.

Die Aktivierung der Funktion erfolgt ausschließlich auf Veranlassung des Kunden für die jeweilige Galerie. Mit der Aktivierung bestätigt der Kunde, dass für die damit verbundene Verarbeitung eine geeignete datenschutzrechtliche Grundlage besteht und – soweit erforderlich – wirksame Einwilligungen oder sonstige erforderliche Erlaubnistatbestände vorliegen.

Der Kunde ist dafür verantwortlich, Erklärungen betroffener Personen, insbesondere Widerrufe erteilter Einwilligungen oder Widersprüche gegen die Verarbeitung, zu berücksichtigen und die sich daraus ergebenden Maßnahmen unverzüglich umzusetzen oder gegenüber dem Auftragsverarbeiter zu veranlassen.

Soweit die Funktion deaktiviert wird oder die zugrunde liegende Galerie gelöscht wird, werden die zugehörigen Gesichtserkennungsdaten nach Maßgabe der technischen und organisatorischen Prozesse des Auftragsverarbeiters gelöscht, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Art der Verarbeitung
Erheben, Speichern, Auslesen, Zuordnen, Priorisieren der Anzeige von Inhalten, Übermitteln, Löschen, Gesichtserkennung.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden
Bereitstellung einer SaaS-Software zur Erstellung, Verwaltung und zum Teilen von Online-Galerien für Fotografen, einschließlich der optionalen Funktion, eingeladenen Personen vorrangig Inhalte anzuzeigen, auf denen sie abgebildet sind.

Dauer der Verarbeitung
für die Dauer des Hauptvertrags

Zugriff auf Inhalte und Supportfälle

Der Auftragsverarbeiter verarbeitet personenbezogene Daten grundsätzlich nur in dem Umfang, wie dies für die Bereitstellung, den technischen Betrieb, die Absicherung, die Wartung und die vertragsgemäße Durchführung des Dienstes erforderlich ist.

Ein routinemäßiger inhaltlicher Zugriff auf vom Verantwortlichen gespeicherte Foto-, Video- oder Galeriedaten erfolgt nicht. Soweit ein Zugriff im Einzelfall zur Fehleranalyse, Störungsbeseitigung, Missbrauchsabwehr, Sicherheitsüberprüfung oder zur Erfüllung einer Weisung des Verantwortlichen erforderlich ist, erfolgt dieser ausschließlich durch entsprechend berechtigte Personen und beschränkt auf das zur Zweckerreichung notwendige Maß.

Soweit technisch vorgesehen und zumutbar, werden solche Vorgänge intern nachvollziehbar dokumentiert. Der Auftragsverarbeiter stellt durch organisatorische und technische Maßnahmen sicher, dass Unterstützungsleistungen mit möglicher Einsicht in Inhalte auf Ausnahmefälle begrenzt bleiben.

Umgang mit Anfragen betroffener Personen

Soweit betroffene Personen sich unmittelbar an den Auftragsverarbeiter wenden, wird der Auftragsverarbeiter solche Anfragen unverzüglich an den Verantwortlichen weiterleiten, sofern eine eigenständige Bearbeitung nicht gesetzlich vorgeschrieben ist. Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen der vertraglichen und gesetzlichen Pflichten bei der Bearbeitung solcher Anfragen.

Verarbeitung durch (Unter-)Auftragsverarbeiter

Gegenstand der (Unter-)Auftragsverarbeitung: Bereitstellung von Cloud-Infrastruktur, Zahlungsabwicklung und Buchhaltungsdienstleistungen.

Art der (Unter-)Auftragsverarbeitung: Payment (mollie), billing (sevdesk), storing (Storj)

Bis zum Ende des Vertrags

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten

Verschlüsselung bei der Übertragung (TLS/SSL), Verschlüsselung sensibler Datenfelder sowie Passwort-Hashing nach dem Stand der Technik (Argon2).

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

Einsatz von Verschlüsselung, Monitoring- und Alarmierungsmechanismen, rollenbasierten Zugriffskonzepten sowie regelmäßigen Datensicherungen.

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

Regelmäßige Datensicherungen; Verfahren zur Wiederherstellung von Daten und Systemen werden in angemessenen Abständen überprüft oder testweise verifiziert, um eine Wiederherstellung innerhalb angemessener Zeit zu ermöglichen.

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

Regelmäßige interne Überprüfung der technischen Ausgestaltung, laufendes Monitoring sicherheitsrelevanter Ereignisse sowie bedarfsbezogene Anpassung bestehender Schutzmaßnahmen.

Maßnahmen zur Identifizierung und Autorisierung der Nutzer

Zugänge zu produktiven Systemen werden personenbezogen vergeben und nach einem rollenbasierten Berechtigungskonzept verwaltet. Administrative oder sonstige besonders privilegierte Zugänge werden, soweit technisch vorgesehen, zusätzlich durch einen zweiten Authentifizierungsfaktor oder eine vergleichbare verstärkte Authentifizierung abgesichert. Berechtigungen werden in angemessenen Abständen überprüft und bei Wegfall des Erfordernisses unverzüglich angepasst oder entzogen.

Maßnahmen zum Schutz der Daten während der Übermittlung

Verschlüsselung bei der Übertragung (TLS/SSL) für öffentlich erreichbare Endpunkte; interne Systemkommunikation erfolgt innerhalb eines technisch abgeschotteten Netzwerks oder gleichwertig geschützter Infrastruktur.

Maßnahmen zum Schutz der Daten während der Speicherung

Verschlüsselung sensibler Datenfelder, sicheres Geheimnis- und Schlüsselmanagement sowie Passwort-Hashing nach dem Stand der Technik.

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

Die Verarbeitung erfolgt in technisch abgesicherten Betriebsumgebungen. Soweit externe Rechenzentren oder Infrastrukturdienstleister eingesetzt werden, erfolgt deren physische Absicherung im Verantwortungsbereich der jeweiligen Anbieter nach marktüblichen Sicherheitsstandards.

Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen

Monitoring und Alarmierung via Grafana.

Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

Sicherheitsrelevante Systemereignisse sowie Zugriffe auf administrative Funktionen werden, soweit technisch vorgesehen, protokolliert und zur Erkennung von Störungen, Fehlkonfigurationen, unberechtigten Zugriffen oder Missbrauch ausgewertet.

Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit

Interne Vorgaben zur Verwaltung von Zugängen, Rollen, Geheimnissen und sicherheitsrelevanten Konfigurationen; Überprüfung und Fortentwicklung der technischen und organisatorischen Maßnahmen nach Bedarf.

Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten

Soweit vorhanden, werden Prüfberichte, Sicherheitsnachweise oder sonstige geeignete Unterlagen zur internen Qualitätssicherung herangezogen. Eine bestimmte Zertifizierung wird hierdurch nicht zugesichert.

Maßnahmen zur Gewährleistung der Datenminimierung

Es werden nur solche personenbezogenen Daten verarbeitet, die für die Bereitstellung, Sicherheit, Wartung und Durchführung des Dienstes erforderlich sind.

Maßnahmen zur Gewährleistung der Datenqualität

Plausibilitätsprüfungen, technische Validierungen und anlassbezogene Korrekturprozesse unterstützen die Richtigkeit und Aktualität der verarbeiteten Daten.

Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

Automatisierte oder organisatorisch gesteuerte Löschroutinen sowie Beschränkung der Datenerhebung und Speicherung auf das für den jeweiligen Verarbeitungszweck erforderliche Maß.

Maßnahmen zur Gewährleistung der Rechenschaftspflicht

Interne Dokumentation der technischen und organisatorischen Maßnahmen, regelmäßige Überprüfung der Sicherheitskonzepte sowie dokumentierte Prozesse zur Bewertung und Anpassung der Schutzmaßnahmen.
Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

Bereitstellung in einem strukturierten Format, soweit technisch vorgesehen oder vertraglich geschuldet, sowie Umsetzung von Löschprozessen nach Maßgabe vertraglicher, technischer und gesetzlicher Vorgaben.

Beschreibung der spezifischen technischen und organisatorischen Maßnahmen, die der (Unter-)Auftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss

Abschluss von Auftragsverarbeitungsverträgen mit relevanten Dienstleistern, angemessene Prüfung deren technischer und organisatorischer Maßnahmen sowie regelmäßige Überprüfung der eingebundenen Dienstleister.

Fortentwicklung der technischen und organisatorischen Maßnahmen

Der Auftragsverarbeiter ist berechtigt, die in diesem Anhang beschriebenen technischen und organisatorischen Maßnahmen weiterzuentwickeln, anzupassen oder durch gleichwertige Maßnahmen zu ersetzen, sofern das insgesamt geschuldete Schutzniveau hierdurch nicht unterschritten wird. Über wesentliche Änderungen mit Relevanz für die Sicherheit der Verarbeitung informiert der Auftragsverarbeiter den Verantwortlichen auf Anfrage oder in sonst geeigneter Form.

ERGÄNZENDE VERFAHRENSREGELUNGEN

Durchführung von Prüfungen und Nachweisen

Die Ausübung von Prüf- und Nachweisrechten durch den Verantwortlichen erfolgt unter Berücksichtigung der gesetzlichen Anforderungen, der Vertraulichkeitsinteressen anderer Kunden, der Integrität der Systeme des Auftragsverarbeiters sowie der betrieblichen Abläufe des Auftragsverarbeiters.

Soweit geeignet, erfolgt der Nachweis der Einhaltung datenschutzrechtlicher Pflichten zunächst durch die Bereitstellung von Unterlagen, Selbstauskünften, Beschreibungen der technischen und organisatorischen Maßnahmen, Zertifikaten, Prüfberichten oder vergleichbaren geeigneten Nachweisen.

Vor-Ort-Prüfungen kommen insbesondere dann in Betracht, wenn ein gleichwertiger Nachweis auf andere Weise nicht möglich oder nicht ausreichend ist oder konkrete Anhaltspunkte für erhebliche Pflichtverletzungen vorliegen. Solche Prüfungen sind mit angemessener Frist anzukündigen, während der üblichen Geschäftszeiten durchzuführen und auf den erforderlichen Umfang zu beschränken. Mehr als eine anlasslose Vor-Ort-Prüfung pro Kalenderjahr soll in der Regel nicht erfolgen.

Rückgabe und Löschung nach Vertragsende

Nach Beendigung des Vertragsverhältnisses erfolgt die Rückgabe oder Löschung der im Auftrag verarbeiteten personenbezogenen Daten nach Maßgabe der Weisung des Verantwortlichen und im Rahmen der technischen Möglichkeiten des bereitgestellten Dienstes, soweit keine gesetzlichen Aufbewahrungspflichten oder sonstige gesetzlich zulässige Gründe für eine befristete eingeschränkte Vorhaltung entgegenstehen.

Soweit eine Rückgabe vorgesehen ist, stellt der Auftragsverarbeiter die Daten über ein angemessen gesichertes Verfahren in einem üblichen strukturierten Format zur Verfügung. Sofern für den Abruf Zugangsdaten erforderlich sind, werden diese getrennt übermittelt oder auf anderem geeigneten Weg bereitgestellt.

Der Auftragsverarbeiter bestätigt auf Anforderung die durchgeführte Löschung in geeigneter Form. Dokumentationen, die dem Nachweis einer ordnungsgemäßen und auftragsgemäßen Verarbeitung dienen, dürfen im gesetzlich zulässigen Umfang über das Vertragsende hinaus aufbewahrt werden.

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Name: Storj Labs Inc.

Anschrift: 1870 The Exchange SE Ste 220 PMB 75268, Atlanta, GA 30339-2171, USA

Name, Funktion und Kontaktdaten der Kontaktperson: legal@storj.io

Beschreibung der Verarbeitung: Objekt-Storage für Fotos, Profilbilder sowie für Datenbank- und Log-Backups.

Name: Mollie B.V.; Anschrift: Keizersgracht 126, 1015 CW Amsterdam, Niederlande; Beschreibung der Verarbeitung: Zahlungsdienstleister zur Abwicklung von Zahlungen. Name: sevDesk GmbH; Anschrift: Im Unteren Angel 1, 77652 Offenburg, Deutschland; Beschreibung der Verarbeitung: Buchhaltungs- und Rechnungsstellungstool.