AUFTRAGSVERARBEITUNGSVEREINBARUNG

Hinweis 1: Alle der nachfolgenden Personenbezeichnungen beziehen sich auf alle Geschlechter und ihre Sprachformen und verstehen sich stets mit dem Zusatz „(w/m/d)".

Hinweis 2: Die nachfolgende Vertragsurkunde beruht auf einem Muster der EU-Kommission, die exakt diese Vertragsurkunde als rechtmäßig ansieht. Dazu hat die EU-Kommission extra einen Durchführungsbeschluss über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28(7) DS-GVO und Artikel 29(7) der Verordnung (EU) 2018/1725 gefasst. Der Durchführungsbeschluss kann hier eingesehen werden: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021D0915. Er darf nicht mit den Standardvertragsklauseln i.S.v. Artikel 46 DSGVO, die eine Drittlandübermittlung regeln, verwechselt werden.

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln") soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG sichergestellt werden.

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

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

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

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

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

Klausel 2

Unabänderbarkeit der Klauseln

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

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

Klausel 3

Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.
c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

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

Klausel 5

Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.
b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.
c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II – PFLICHTEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

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

Klausel 7

Pflichten der Parteien

7.1 Weisungen

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

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

7.2 Zweckbindung

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

7.3 Dauer der Verarbeitung personenbezogener Daten

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

7.4 Sicherheit der Verarbeitung

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

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

7.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das

Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien

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) 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 drei Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

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

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich

personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

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

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

7.8 Internationale Datenübermittlungen

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

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

Klausel 8

Unterstützung des Verantwortlichen

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

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

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

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

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

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

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

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

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

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

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

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

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

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

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

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

3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen. Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

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

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

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

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt. Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

ABSCHNITT III – SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

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

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

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

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

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

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

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

ANHANG I – LISTE DER PARTEIEN

Verantwortliche(r):

Verantwortliche und Auftragsverarbeiterin sind unabhängig von dieser Auftragsverarbeitungsvereinbarung Vertragsparteien eines schuldrechtlichen Hauptvertrages über die Bereitstellung des Dienstes „Onepage“ (vgl. https://onepage.io/de/auth/registration). Verantwortliche ist das Unternehmen, das diesen Dienst bucht, egal, ob kostenfreie Testversion oder kostenpflichtige Version. Das Beitrittsdatum ist identisch mit dem Datum der ersten Buchung des Dienstes.

Auftragsverarbeiter:

Name: Onepage GmbH
Anschrift: Hanauer Landstraße 172, 60314 Frankfurt am Main
Name, Funktion und Kontaktdaten der Kontaktperson: Marcel Knopf, Geschäftsführung, erreichbar wie oben unter dem Adresszusatz „persönlich – vertraulich – Geschäftsführung“
Das Beitrittsdatum ist identisch mit dem Datum der ersten Buchung des Dienstes.

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Vorbemerkung

Die Auftragsverarbeiterin stellt ihren unternehmerischen Kunden die SaaS-Plattform „Onepage“ zur Verfügung. Mithilfe dieser Plattform ist es möglich, Internetseiten (einschl. Landingpages) zu erstellen, fortlaufend zu gestalten und darüber erhobenen Daten (sog. Leads) zu verwalten. Hierfür stellt sie ihren Kunden ein Webportal zur browserbasierten Nutzung in einem ausschließlich für registrierte Nutzer zugänglichen Bereich zur Verfügung, ebenso wie Speicherplatz auf Servern der Unterauftragsverarbeiter (ANHANG III), die sich ausschließlich in der EU befinden. Die Verantwortliche ist Kundin und somit Nutzerin der Plattform.

Dies vorausgeschickt kann die Auftragsverarbeitung wie folgt beschrieben werden:

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- aktuelle und ehemalige Besucher*innen der mit Onepage generierten Internetseiten
- Bewerber*innen der Verantwortlichen
- aktuelle und ehemalige Beschäftigte der Verantwortlichen
- potenzielle, aktuelle und ehemalige Kund*innen der Verantwortlichen
- potenzielle, aktuelle und ehemalige Lieferant*innen der Verantwortlichen

Kategorien personenbezogener Daten, die verarbeitet werden

<u>Daten der aktuellen und ehemaligen Besucher*innen der mit Onepage generierten Internetseiten</u>

- Technische Zugriffsdaten: IP-Adresse der Besucher:innen, Datum und Uhrzeit des Zugriffs. abgerufene URL/Seite, Referrer-URL (zuvor besuchte Seite), HTTP-Statuscode, übertragene Datenmenge, Browsertyp und -version, Betriebssystem, Spracheinstellungen, Gerätetyp
- *nur, sofern, solange und soweit von der Verantwortlichen aktiviert:* Cookie- und Trackingdaten Cookie-IDs und ähnliche Identifikatoren
    - besuchte Unterseiten, Verweildauer, Klicks, Scrollverhalten, ggf. Marketing-/Tracking-Daten, wie z. B. UTM-Parameter, Kampagnenzuordnung, „tagging-pixel-basierte Daten
- *nur, sofern, solange und soweit von der Verantwortlichen aktiviert:* Inhalts- und Formulardaten bei Kontakt-/Lead-Formularen
    - von Besucher*innen eingegebene Daten, z. B. Name, E-Mail-Adresse, Telefonnummer, weitere Formularinhalte, wie Freitext-Nachrichten, Interessensangaben, Terminwünsche, Auswahloptionen in Formularen. Opt-in-/Einwilligungsstatus, wie Zeitpunkt, Inhalt der Einwilligung, Nachweis der Zustimmung zu Newslettern o. Ä.

Daten der anderen Betroffenenkategorien

- alle Daten, die auch von Besucher*innen der mit Onepage generierten Internetseiten verarbeitet werde
- Kommunikations- und Interaktionsdaten
    - Inhalte von Anfragen über Kontaktformulare (z. B. Support-, Beratungs- oder Buchungsanfragen), ggf. Kommentare/Bewertungen, wenn solche Funktionen eingebunden werden (einschließlich Name, Kommentartext).
- Vertrags- und Abrechnungsdaten (nur falls über die Landingpage Verträge/Bestellungen angebahnt oder abgeschlossen werden)
- Basisdaten zu Anfragen, Buchungen oder Bestellungen (z. B. gewähltes Angebot, Datum der Anfrage).
- ggf. Zahlungs- oder Rechnungsinformationen (werden oft über externe Payment-Provider abgewickelt, dabei aber als Zweck über die Landingpage initiiert).

Art der Verarbeitung

Die Daten werden auf den mit Onepage generierten Internetseiten erhoben, in einer Cloudumgebung gespeichert und der Verantwortlichen zum Abruf bereitgestellt. Bei Weisung und/oder Ende des Hauptvertrages werden die Daten gelöscht.

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

Die Verarbeitung dient der Bereitstellung von Internetauftritten, werblichen Ansprache und Analyse des Nutzungsverhaltens.

Dauer der Verarbeitung

Bei Weisung und/oder Ende des Hauptvertrages werden die Daten gelöscht.

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

I

Allgemeine Maßnahmen

Maßnahmen zur dauerhaften Gewährleistung der Sicherheit (Nachhaltigkeitskontrolle)

Datenschutz als Compliance-Ziel

Die Achtung kern- und nebendatenschutzrechtlicher Regelungen ist ein formuliertes Compliance Ziel des Auftragsverarbeiterin. Die organisatorische Hoheit zur Sicherstellung der Datenschutzkonformität liegt qua Amt bei der Geschäftsleitung.

Revisionsfrequenz 18 Monate

Es wird im Abstand von 18 Monaten anlasslos kontrolliert, ob die hier dokumentierten Maßnahmen noch ergriffen werden (Prüfungspunkt 1) und ob die Maßnahmen noch genügen, um die festgestellten Risiken hinreichend zu minimieren (Prüfungspunkt 2). Es wird dokumentiert, ob die Prüfungspunkte bejaht oder verneint werden. Sollte mindestens einer der beiden Prüfungspunkte zu verneinen sein, werden neue Maßnahmen definiert und umgesetzt. Anlassbezogene Kontrollen sind jederzeit möglich und werden ebenfalls dokumentiert.

Schulungs- und Awareness-Maßnahmen

Die Beschäftigten werden regelmäßig (i.d.R. einmal jährlich) geschult. Zum Schulungskonzept ist folgendes auszuführen:

- Ziel der Schulung ist, die Beschäftigten (m/w/d) mit den Grundlagen und Grundbegriffen des Datenschutzrechts vertraut zu machen. Insbesondere sollen die Beschäftigten (m/w/d) anschließend in der Lage sein, anhand des Verbots mit Erlaubnisvorbehalts die grundlegende Frage zu beantworten, wann die Verarbeitung personenbezogener Daten rechtmäßig und wann sie rechtswidrig ist. Ferner sollen sie die erforderlichen technischen und organisatorischen Maßnahmen kennen und wissen, wie sie bei der Umsetzung in ihrem Unternehmen daran mitwirken können und müssen. Ferner soll ein Überblick über die sonstigen datenschutzrechtlichen Pflichten erfolgen, insbesondere jene nach DSGVO und BDSG2018. Insbesondere erfolgt eine Belehrung über das Datengeheimnis.
- Zum Aufbau ist insbesondere auszuführen:
    - Block 1 beginnt mit einer groben Einführung, bei der ein Überblick über die kommende Schulung verschafft wird.
    - Block 2 beginnt mit einer Einführung in das Datenschutzrecht. Es werden die Grundbegriffe geschult, insbesondere die Begriffe „personenbezogene Daten“, „Verarbeitung“, „Einwilligung“, „Rechtsvorschrift.“. Die Schulung orientiert sich an den Legaldefinitionen der DSGVO und des BDSG2018. Es wird das Verbot mit

Erlaubnisvorbehalt erläutert. Werden die Rechtmäßigkeitsvoraussetzungen für die Einwilligung besprochen. Anschließend werden die wichtigsten, einwilligungsunabhängigen Rechtsvorschriften erläutert, insbesondere § 26 BDSG2018 (Beschäftigtendatenschutz), Artikel 6 Absatz 1 lit. b DSGVO (Kundendatenschutz) und Artikel 6 Absatz 1 lit. f DSGVO (berechtigtes Interesse). Zu jeder Erlaubnisnorm wird mindestens ein Beispielsfall mit den Schulungsteilnehmern (m/w/d) diskutiert, um sicherzustellen, dass alle mit den Normen umgehen können. Außerdem werden die Voraussetzungen der Einwilligung erläutert.

- Block 3 beginnt mit einer Einführung zu den technischen und organisatorischen Maßnahmen nach Artikel 32 DSGVO. Hierbei wird v.a. erläutert, dass und welche Risiken zu analysieren sind. Dann wird erklärt, dass diese Risiken mit technischen und organisatorischen Maßnahmen zu minimieren sind. Ferner wird auf die Nachweispflicht eingegangen. Sodann werden die wichtigsten technischen und organisatorischen Maßnahmen im Unternehmen besprochen. Abschließend wird hier der Projektplan „Datenschutzorganisation“ geschult.
- Block 4 beschäftigt sich mit spezifischen Fragen des Datenschutzrechts im Anwendungsbereich der Auftragsverarbeitung.

DSB ernannt

Die Verantwortliche hat einen Datenschutzbeauftragten ernannt.

Organisatorische Maßnahmen, Dokumentation und Rechtmäßigkeit von Weisungen

Die Hiesige Auftragsverarbeiterin führt ein umfassendes Verzeichnis von Verarbeitungstätigkeiten. Sie führt insbesondere die Verzeichnisse i.S.v. Artikel 30 Absatz 2 DSGVO mit allen gesetzlichen Pflichtangaben. Kommen Beschäftigte zum Ergebnis, dass eine Weisung gegen die DSGVO verstößt, konsultieren sie im Zweifelsfall den externen Datenschutzbeauftragten, der erforderlichenfalls mit dem hiesigen Verantwortlichen/Auftraggeber Kontakt aufnimmt und die Rechtmäßigkeit der Weisung klärt. Sie unterstützt sie den hiesigen Verantwortlichen/Auftraggeber bei Datenschutzfolgeabschätzungen; dies in Erfüllung ihrer Pflichten als Auftragsverarbeiterin. Allerdings erbringt sie keine Rechtsberatung. Weisungen des hiesigen Verantwortlichen/Auftraggebers werden in Textform dokumentiert.

II
Vertraulichkeit

Maßnahmen der Anonymisierung

Technik der Löschung

Daten, die zur Löschung anstehen, werden anonymisiert.

Maßnahmen der Verschlüsselung

Die auftragsgegenständliche Verarbeitung findet nicht auf Servern der Auftragsverarbeiterin statt, sondern bei ihren Unterauftragsverarbeitern.

Verschlüsselung bei AWS

Die Unterauftragsverarbeiterin verschlüsselt Daten bei Speicherung („at rest“) standardisiert mit branchenüblichen Algorithmen wie AES-256. Die Verschlüsselung erfolgt beispielsweise in Diensten wie Amazon S3, Amazon RDS, Amazon EBS und Amazon Glacier. Für die Verwaltung der Schlüssel werden zentrale Systeme wie der AWS Key Management Service (KMS) und dedizierte Hardware-Sicherheitsmodule (HSM, etwa „AWS CloudHSM“) eingesetzt. Kund*innen haben die Möglichkeit, Schlüssel selbst zu verwalten oder von der Unterauftragsverarbeiterin generieren und schützen zu lassen. Ohne die erforderlichen Zugangsschlüssel sind gespeicherte Daten für Dritte und die Unterauftragsverarbeiterin nicht im Klartext zugänglich. Für Daten in Übertragung („in transit“) setzt die Unterauftragsverarbeiterin standardmäßig Transportverschlüsselung mit SSL/TLS ein. Alle Schnittstellen und API-Endpunkte unterstützen HTTPS (TLS), so dass Kommunikation zwischen Kund*innen und der AWS-Cloud durchgängig geschützt ist. Zusätzlich werden bei der Übertragung zwischen AWS-Rechenzentren und innerhalb virtueller privater Netzwerke (VPCs) Netzwerkverschlüsselungen (z.B. IPsec) implementiert.

Verschlüsselung bei Google

Die Unterauftragsverarbeiterin verschlüsselt sämtliche Kundendaten im Ruhezustand („at rest“) auf Datenträgern und Backup-Medien mithilfe starker Algorithmen wie AES-128 oder AES-256. Die Verschlüsselung erfolgt automatisch ohne Zutun der Kund*innen für alle Daten in den Workspace-Kernanwendungen (beispielsweise Gmail, Drive, Docs, Sheets, Meet). Google-eigene Schlüsselverwaltungsmechanismen im Rechenzentrum schützen die Schlüssel, wobei physische und technische Schutzsysteme für Datenträger und Schlüsselmaterial eingesetzt werden. Für die Übertragung („in transit“) schützt die Unterauftragsverarbeiterin Kundendaten mit Transportverschlüsselung nach Industriestandard, insbesondere HTTPS (TLS), was für alle Nutzer*innen und Schnittstellen standardmäßig aktiviert ist. Zusätzlich erfolgt die Verschlüsselung der Kommunikation zwischen Google-Rechenzentren und für Übertragungen im öffentlichen Internet.

Maßnahmen der Zutrittskontrolle

Innerhalb der Büroräume der hiesigen Auftragsverarbeiterin befinden sich ohnehin keine permanenten Hardware-Komponenten, insbesondere kein Server. Ferner wird dort in der Regel keine auftragsgegenständliche Tätigkeit ausgeführt, sondern lediglich geschäftsführende-administrative Tätigkeiten sowie die Entgegennahme von Post. Daher sind physische Sicherheitsmaßnahmen nur von geringer Bedeutung. Gleichwohl werden hierfür seitens der Auftragsverarbeiterin folgende, ergänzende Maßnahmen ergriffen:

Gebäude, verschlossene Tür (mechanischer Schlüssel)

Das Gebäude, in dem sich die für die Datenverarbeitung maßgebliche Betriebsstätte befindet, ist verschlossen. Der Zutritt ist wie folgt möglich: Entweder eine Person innerhalb des Hauses öffnet die Zugangstür von innen oder eine Person öffnet die Zugangstür mit einem gesonderten Zugangsmittel (hier: mechanischer Schlüssel).

Büro, verschlossene Tür (mechanischer Schlüssel)
Die Büroräume sind verschlossen. Der Zutritt ist wie folgt möglich: Entweder eine Person innerhalb der Büroräume öffnet die jeweilige Zugangstür von innen oder eine Person öffnet die jeweilige Zugangstür mit einem gesonderten Zugangsmittel (hier: mechanischer Schlüssel).

Dienstanweisung, sichere Räume
Die Beschäftigten sind per Dienstanweisung verpflichtet, remote-Arbeit nur in sicheren Räumen zu verrichten. Sichere Räume sind solche, die in der Regel nicht von unbekannten Dritten betreten werden können, nicht von außerhalb des jeweiligen Hauses leicht einsehbar sind und von Besucher*innen in der Regel nicht betreten werden.

Dienstanweisung, Meldung Zutrittsverletzung
Die Beschäftigten sind per Dienstanweisung verpflichtet, den Verdacht auf meldepflichtige Fälle i.S.d. Artikel 33, 34 DSGVO im Zusammenhang mit Zutrittsverletzungen zu melden. Die gleiche Verpflichtung gilt, wenn nicht nur ein Verdacht, sondern Gewissheit hierüber herrscht.

Maßnahmen der Zugangskontrolle

Innerhalb der Büroräume der hiesigen Auftragsverarbeiterin befinden sich ohnehin keine permanenten Hardware-Komponenten, insbesondere kein Server. Ferner wird dort in der Regel keine auftragsgegenständliche Tätigkeit ausgeführt, sondern lediglich geschäftsführende-administrative Tätigkeiten sowie die Entgegennahme von Post. Daher sind physische Sicherheitsmaßnahmen nur von geringer Bedeutung. Gleichwohl werden hierfür seitens der Auftragsverarbeiterin folgende, ergänzende Maßnahmen ergriffen:

Dienstanweisung, eingeschränkter Zugang
Die Beschäftigten sind per Dienstanweisung verpflichtet, Dritten, einschl. Familienangehörigen, keinen oder nur einen unbedingt notwendigen Zugriff auf die Datenverarbeitungsmittel im Betriebseigentum zu gewähren.

Dienstanweisung, Meldung Zugangsverletzung
Die Beschäftigten sind per Dienstanweisung verpflichtet, den Verdacht auf meldepflichtige Fälle i.S.d. Artikel 33, 34 DSGVO im Zusammenhang mit Zugangsverletzungen zu melden. Die gleiche Verpflichtung gilt, wenn nicht nur ein Verdacht, sondern Gewissheit hierüber herrscht.

Dienstanweisung, übergreifende Maßnahmen
Die Beschäftigten sind per Dienstanweisung verpflichtet, die nachfolgend näher bezeichneten „übergreifenden Maßnahmen“ auch während der remote-Arbeit zu ergreifen.

Übergreifende Maßnahmen

Folgende Maßnahmen werden ergriffen, unabhängig davon, ob die Datenverarbeitung remote oder in Präsenz erfolgt (übergreifende Maßnahmen):

Änderung von Standard- und Leerpasswörtern

Nach Installation neuer Software bzw. Inbetriebnahme neuer Hardware werden Standard- und Leerpasswörter geändert.

passwortgeschützte clients

Alle clients sind passwortgeschützt.

individuelle Passwörter

Alle Berechtigten haben individuelle Passwörter.

eingeschränkte Nutzung von Admin-Zugängen

Die sog. Admin-Zugänge werden nur für Admin-Tätigkeiten genutzt. Personen, die über Admin-Rechte verfügen, nutzen gesonderte Zugänge für Nicht-Admin-Tätigkeiten.

eingeschränkter Gesamtzugriff auf Passwörter

Nur ein eng begrenzter Personenkreis hat einen Gesamtzugriff auf alle Zugangsdaten.

Betriebssysteme, Sicherheitspatches

Mit Blick auf die eingesetzten Betriebssysteme werden alle verfügbaren Sicherheitspatches eingespielt.

Betriebssysteme, Updates

Mit Blick auf die eingesetzten Betriebssysteme werden alle verfügbaren Updates installiert.

Web-Browser, Sicherheitspatches

Mit Blick auf die eingesetzten Web-Browser werden alle verfügbaren Sicherheitspatches eingespielt.

Web-Browser, Updates

Mit Blick auf die eingesetzten Web-Browser werden alle verfügbaren Updates installiert.

Virenschutz auf allen clients

Alle clients und server verfügen über Virenschutz.

Virenprüfungen

Die eingesetzten Virenschutzprogramme führen automatisierte, regelmäßige Virenprüfungen durch.

Virenschutzprogramme, Updates

Mit Blick auf die eingesetzten Virenschutzprogramme werden alle verfügbaren Updates installiert.

Freigabeerfordernis für neue Software
Neue Software kann nur installiert werden, wenn sie vorher zentral freigegeben wurde.

Softwarefreigabe erst nach Kenntnisnahme der Handbücher
Neue Software kann nur installiert werden, wenn das Handbuch entweder bekannt ist oder gelesen wurde.

Freigabeerfordernis für neue Hardware
Neue Hardware kann nur in Betrieb genommen werden, wenn sie vorher zentral freigegeben wurde.

Hardwarefreigabe erst nach Kenntnisnahme der Handbücher
Neue Hardware kann nur in Betrieb genommen werden, wenn das Handbuch entweder bekannt ist oder gelesen wurde.

Maßnahmen der Zugriffskontrolle

Zentrale Rechtevergabe
Die Zugriffsrechte auf personenbezogene Daten werden zentral vergeben.

need-to-know-Prinzip
Die Zugriffsrechte auf personenbezogene Daten werden nach dem need-to-know-Prinzip vergeben.

Anpassungen bei Rechtevergabe
Verändern sich die Aufgaben einer berechtigten Person, werden die Zugriffsrechte, soweit erforderlich, nach dem need-to-know-Prinzip angepasst.

Entzug der Rechte
Endet die Tätigkeit einer berechtigten Person, werden die Zugriffsrechte umgehend und vollständig entzogen.

Maßnahmen der Weitergabekontrolle

Bezugnahme Verschlüsselung
Es wird auf die Maßnahmen zur Verschlüsselung Bezug genommen.

Maßnahmen der Eingabekontrolle

Eingaben werden geloggt
Eingaben, so sie im auftragsrelevanten Bereich überhaupt manuell getätigt werden, werden geloggt.

Maßnahmen der Auftragskontrolle

Artikel 28 DSGVO

Vor jeder Unterbeauftragung wird geprüft, ob die gesetzlichen Voraussetzungen erfüllt sind, insbesondere, ob eine Vertragsurkunde nach Artikel 28 Absatz 3 DSGVO vorhanden ist und ob das zu beauftragende Unternehmen hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Nur bei positivem Ergebnis erfolgt die Beauftragung. Das Ergebnis wird in jedem Fall protokolliert.

Artikel 44 DSGVO

Für den Fall, dass die Unterbeauftragung eine Übermittlung in ein Drittland i.S.v. Artikel 44 DSGVO mit sich bringt, wird geprüft, ob das zu beauftragende Unternehmen die im 5. Kapitel der DSGVO (Artikel 44 bis 50 DSGVO) niedergelegten Bedingungen einhält und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten aus dem betreffenden Drittland oder der betreffenden internationalen Organisation an ein anderes Drittland oder eine andere internationale Organisation. Nur bei positivem Ergebnis erfolgt die Beauftragung. Das Ergebnis wird in jedem Fall protokolliert.

Artikel 46 DSGVO - TIA

Für den Fall, dass die Beauftragung eine Übermittlung in ein Drittland i.S.v. Artikel 44 DSGVO mit sich bringt und das zu beauftragende Unternehmen sich gemäß den Standardvertragsklauseln i.S.v. Artikel 46 DSGVO verpflichtet, wird ein sog. Transfer Impact Assessment durchgeführt. Nur bei positivem Ergebnis erfolgt die Beauftragung. Das Ergebnis wird in jedem Fall protokolliert.

Artikel 35 DSGVO

Für den Fall, dass die Beauftragung selbst oder die beauftragte Datenverarbeitung in den Anwendungsbereich des Artikels 35 DSGVO fällt, wird eine Datenschutzfolgeabschätzung durchgeführt. Nur bei positivem Ergebnis erfolgt die Beauftragung. Das Ergebnis wird in jedem Fall protokolliert.

Nachkontrollen

Die vorgenannten Kontrollen werden in regelmäßigen Abständen anlasslos wiederholt, solange die Beauftragung andauert.

Zuständigkeiten

Für die vorgenannten Maßnahmen gelten folgende Zuständigkeiten:

Geschäftsleitung

Datenschutzbeauftragte

Soweit nach der AVV erforderlich, auch die Verantwortliche (Auftraggeberin)

Maßnahmen der Trennungskontrolle

ausdifferenziertes Ordner- und Zugriffsmodell
Elektronisch gespeicherten Daten sind durch ein ausdifferenzierten Ordner- und Zugriffsmodell getrennt.

III
Verfügbarkeit, Wiederherstellbarkeit, Belastbarkeit

Maßnahmen der Verfügbarkeitskontrolle

Die auftragsgegenständliche Verarbeitung findet nicht auf Servern der Auftragsverarbeiterin statt, sondern bei ihren Unterauftragsverarbeitern.

Verfügbarkeit bei AWS
Die Unterauftragsverarbeiterin ist nach ISO/IEC 27018:2014 und nach ISO 27001 zertifiziert. Der Anbieter ergreift in concreto folgende Maßnahmen: Rechenzentren sind in Clustern in verschiedenen globalen Regionen aufgebaut. Alle Rechenzentren sind online und bedienen Kunden. Kein Rechenzentrum ist "kalt". Im Fehlerfall verlagern automatisierte Prozesse den Kundendatenverkehr aus dem betroffenen Bereich. Es ist sichergestellt, dass im Falle eines Rechenzentrumsausfalls genügend Kapazität zur Verfügung steht, um den Lastausgleich für die verbleibenden Standorte zu kompensieren. Ferner differenziert der Anbieter zwischen verschiedenen Verfügbarkeitszonen. Jede Verfügbarkeitszone ist als unabhängige Fehlerzone ausgelegt. Dies bedeutet, dass die Verfügbarkeitszonen innerhalb einer typischen Metropolregion räumlich getrennt sind und sich in Niedrigwasser-Überschwemmungsgebieten befinden (die spezifische Kategorisierung der Überschwemmungsgebiete variiert je nach Region). Zusätzlich zur unterbrechungsfreien Stromversorgung und zu den Onsite-Backup-Generatoren wird die Energiezufuhr über verschiedene Netze von unabhängigen Versorgungsunternehmen gespeist, um einzelne Fehlerquellen weiter zu reduzieren. Verfügbarkeitszonen sind alle redundant verbunden.

Verfügbarkeit bei Google
Die Unterauftragsverarbeiterin ist nach ISO 27001 zertifiziert. Ergänzend ist hierzu folgendes auszuführen: Google speichert die Daten in einer geschützten Umgebung von eigenen Servern. Daten, die Services-Datenbank und die Dateisystemarchitektur werden zwischen mehreren geografisch verteilten Rechenzentren repliziert, wobei sichergestellt ist, dass die Vertraulichkeit und Trennung der Daten gewährleistet ist. Die hierfür verwendeten Infrastruktursysteme sind in der Lage, einzelne Fehlerquellen zu eliminieren und die Auswirkungen von zu erwartenden Umweltrisiken zu minimieren. Zweifache Schaltkreise, Schalter, Netzwerke oder andere notwendige Geräte tragen dazu bei, diese Redundanz bereitzustellen. Hierbei ist sichergestellt, dass Google bestimmte Risiken früh erkennen und

minimieren kann. Die hierfür erforderliche Wartung kann i.d.R. störungsfrei verlaufen. Hier gibt es dokumentierte, präventive Wartungsverfahren. Die vorbeugende Wartung der Rechenzentrumsausrüstung erfolgt auf Grundlage eines standardisierten Änderungsprozesses. Die Stromversorgungssysteme des Rechenzentrums sind so konzipiert, dass sie redundant und wartungsfähig sind, ohne den kontinuierlichen Betrieb zu beeinträchtigen, 24 Stunden am Tag und 7 Tage die Woche. In den meisten Fällen wird für kritische Infrastrukturkomponenten im Rechenzentrum sowohl eine primäre als auch eine alternative Stromquelle mit jeweils gleicher Kapazität bereitgestellt. Backup-Strom wird durch verschiedene Mechanismen wie unterbrechungsfreie Stromversorgungen zur Verfügung gestellt, die einen konsistent zuverlässigen Stromschutz während Versorgungsspannungsabfällen, Stromausfällen, Überspannung, Unterspannung und außerhalb der Toleranz liegenden Frequenzbedingungen liefern. Wenn die Netzstromversorgung unterbrochen wird, ist die Notstromversorgung so ausgelegt, dass das Rechenzentrum bei voller Auslastung für bis zu 10 Minuten mit Strom versorgt wird, bis die Dieselgeneratorsysteme die Stromversorgung übernehmen. Die Dieselgeneratoren sind in der Lage, innerhalb von Sekunden automatisch hochzufahren, um genügend Notstrom zu liefern, um das Rechenzentrum typischerweise über einen Zeitraum von mehreren Tagen mit voller Kapazität zu betreiben.

Maßnahmen für die rasche Wiederherstellbarkeit

Durch die o.g. Maßnahmen der Verfügbarkeitskontrolle ist sichergestellt, dass eine rasche Wiederherstellbarkeit gegeben ist. Es ist ein Notfallkonzept für Vorfälle des Datenverlustes oder der eingeschränkten Verfügbarkeit implementiert.

Maßnahmen für die Sicherstellung der Belastbarkeit

Es findet ein durchgehendes Systemmonitoring statt.

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER:

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

AWS

Name: Amazon Web Services EMEA S.à.r.l.

Anschrift: 38 Avenue John F. Kennedy, L-1855 Luxemburg, Großherzogtum Luxemburg

Name, Funktion und Kontaktdaten der Kontaktperson:

- Datenschutzbeauftragter / Data Protection Officer: dpo@amazon.com (siehe AWS DSGVO-Datenverarbeitungsvereinbarung)
- Allgemeine Kontaktmöglichkeiten sowie aktuelle Ansprechpartner über die AWS-Kontaktseite: https://aws.amazon.com/compliance/contact/

Drittlandstatus: n/a, da Luxemburg (EU) – Es wird nicht verkannt, dass dieser Unterauftragsverarbeiter eine Muttergesellschaft in den USA hat. Allerdings hat dieser Unterauftragsverarbeiter der hiesigen Auftragsverarbeiterin vertraglich zugesichert, die Daten ausschließlich innerhalb der EU zu verarbeiten. Hierauf darf die hiesige Auftragsverarbeiterin auch vertrauen. Dies entspricht der Rechtsprechung der Gerichte innerhalb der EU. Beispielsweise hat das Oberlandesgericht Karlsruhe mit Beschluss vom 7. September 2022 zum Az. 15 Verg 8/22 gerade erst folgendes entschieden: „*Sie hat in diesem Zuge zugesichert, dass personenbezogene Gesundheitsdaten ausschließlich an die A. S.à.r.l., L., übermittelt werden und auch zu ihrer Verarbeitung die EU nicht verlassen, sondern nur in Deutschland verarbeitet werden. Zudem hat die Beigeladene erklärt, dass die A. S.à.r.l., L. ihr gegenüber zugesichert habe, dass alle Daten der Beigeladenen in Deutschland verarbeitet werden und in der mündlichen Verhandlung vor dem Senat zudem bestätigt, dass sie bis zur Angebotsverwirklichung sämtliche intern notwendigen Verträge mit A. schließen wird, die ihre Zusagen, wie sie im Angebot gemacht werden, umsetzen. Im Sinne einer solchen bindenden Zusicherung haben die Antragsgegnerinnen die Erklärungen der Beigeladenen in den Vergabeunterlagen auch verstanden. Auf dieses Leistungsversprechen dürfen die Antragsgegnerinnen vertrauen.*“

Beschreibung der Verarbeitung: Speicherung und Verarbeitung personenbezogener Daten im Auftrag der Auftragverarbeiterin (Cloud-Storage, Infrastrukturleistungen).

Google Workspace

Name: Google Cloud EMEA Limited

Anschrift: 70 Sir John Rogerson’s Quay, Dublin 2, Irland

Name, Funktion und Kontaktdaten der Kontaktperson:

- Datenschutzbeauftragte: Kristie Chon Flynn, erreichbar über das Datenschutzteam via https://support.google.com/a/contact/googlecloud_dpr (Nutzer am besten über das Administratorkonto); Allgemeine Informationen: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland.

Drittlandstatus: n/a, da Irland (EU) – Es wird nicht verkannt, dass dieser Unterauftragsverarbeiter eine Muttergesellschaft in den USA hat. Allerdings hat dieser Unterauftragsverarbeiter der hiesigen

Auftragsverarbeiterin vertraglich zugesichert, die Daten ausschließlich innerhalb der EU zu verarbeiten. Hierauf darf die hiesige Auftragsverarbeiterin auch vertrauen. Dies entspricht der Rechtsprechung der Gerichte innerhalb der EU. Beispielsweise hat das Oberlandesgericht Karlsruhe mit Beschluss vom 7. September 2022 zum Az. 15 Verg 8/22 gerade erst folgendes entschieden: „*Sie hat in diesem Zuge zugesichert, dass personenbezogene Gesundheitsdaten ausschließlich an die A. S.à.r.l., L., übermittelt werden und auch zu ihrer Verarbeitung die EU nicht verlassen, sondern nur in Deutschland verarbeitet werden. Zudem hat die Beigeladene erklärt, dass die A. S.à.r.l., L. ihr gegenüber zugesichert habe, dass alle Daten der Beigeladenen in Deutschland verarbeitet werden und in der mündlichen Verhandlung vor dem Senat zudem bestätigt, dass sie bis zur Angebotsverwirklichung sämtliche intern notwendigen Verträge mit A. schließen wird, die ihre Zusagen, wie sie im Angebot gemacht werden, umsetzen. Im Sinne einer solchen bindenden Zusicherung haben die Antragsgegnerinnen die Erklärungen der Beigeladenen in den Vergabeunterlagen auch verstanden. Auf dieses Leistungsversprechen dürfen die Antragsgegnerinnen vertrauen.*“

Beschreibung der Verarbeitung: Speicherung und Verarbeitung personenbezogener Daten im Auftrag der Auftragverarbeiterin (Cloud-Storage, Infrastrukturleistungen).

Cloudflare

Name: Cloudflare, Inc.

Anschrift: 101 Townsend Street, San Francisco, CA 94107, USA

Name, Funktion und Kontaktdaten der Kontaktperson:

- Datenschutzbeauftragte / Data Protection Officer: privacyquestions@cloudflare.com; Weitere Kontaktdaten lt. DPA/AVV: +44 (0) 20 3514 6970

Drittlandstatus: USA, Artikel 45 DSGVO (EU-U.S. DPF)

Beschreibung der Verarbeitung: Erbringung von Webhosting-, Reverse Proxy-, DNS- sowie Content Delivery Network (CDN)-Leistungen; Auslieferung und Zwischenspeicherung von Website-Inhalten, Sicherheits- und Schutzfunktionen (z.B. vor DDoS-Angriffen), sowie Protokollierung von Zugriffen zur Analyse und Optimierung der Verfügbarkeit und Performance; bei der Auslieferung und Zwischenspeicherung können personenbezogene Daten (z.B. IP-Adressen, Zugriffszeitpunkte oder Logdaten) verarbeitet und über weltweit verteilte Server transportiert werden