Daten-Transfer-Folgenabschätzung / Data Transfer Impact Assessment (TiA)

Rechenschaftsbericht gem. § 5 Abs 2 DSGVO zur Prüfung von eingesetzten Verfahren und Werkzeugen im Onlinebereich. Die Evaluierung im Rahmen des TiA orientiert sich an den Grundsätzen von Art. 45 Abs. 2DSGVO unter Berücksichtigung der Kriterien der Empfehlungen des Europäischen Datenschutzausschusses (EDPB) 02/2020 zu den europäischen Grundgarantien für Überwachungsmaßnahmen vom 10. November 2020 sowie im Fall des Einsatzes von Standardvertragsklauseln am Art. 46 Abs. 1 lit d) DSGVO i.V.m. Klausel 14 des Beschlusses (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer.

Angaben zum Verantwortlichen

Fa./Adresse des Verantwortlichen	Susell GmbH Rosenthaler Str. 38 10178 Berlin
Datenschutzbeauftragter	datenschutz@susell.io
Zuständige Aufsichtsbehörde	Berliner Beauftragte für Datenschutz und Informationsfreiheit Friedrichstr. 219 10969 Berlin Tel.: +49 30 13889-0 Fax: +49 30 2155050 E-Mail: mailbox@datenschutz-berlin.de https://www.datenschutz-berlin.de/impressum

Angaben zum Prüfungszeitraum

Zeitpunkt Prüfung der sachlichen Richtigkeit/ Funktionsfähigkeit URL dieser Prüfung:	12.09.2022
Prüfungsdatum (TT.MM.YYYY):	12.09.2022, 13.09.2022

Angaben zum Verfahren/Dienst/Anbieter sowie Nutzungsgrundlagen

Name des Verfahrens/ Dienstes/ Werkzeugs (kurz „Verfahren“, dessen „Anbieter“ im Hinblick auf Drittlandtransfers als „Datenempfänger“ bezeichnet werden kann). Bitte (auch) im Auftrag für Kunden eingesetzte Dienste bezeichnen:	**Einsatz bzw. Nutzung von Amazon Web Services zur Datenverarbeitung (Speicherung, Verarbeitung und Bereitstellung von Diensten [e.g. Amazon S3, Amazon Simple Email Service (SES)] und insbesondere elektronischer Kommunikation)**
Adresse:	Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxemburg; Muttergesellschaft: Amazon Web Services, Inc., 410 Terry Avenue North, Seattle WA 98109, USA
Evtl. Kontaktinformationen:	
Einsatzzeitraum:	☒ Bereits im Einsatz. ☐ nein
Wird der Dienst in den eigenen Datenschutzerklärung des Verantwortlichen aufgeführt?	URL: https://www.reteach.io/datenschutz/ ☒ ja ☐ nein
URL AGB des Verfahrens/Anbieters:	URL: https://d1.awsstatic.com/legal/awsserviceterms/AWS_Service_Terms_German_Translation_2022-08-11.pdf ☒ als PDF-Datei gesichert/beiliegend.
URL Datenschutzerklärung des Verfahrens/Anbieters:	URL: https://d1.awsstatic.com/legal/privacypolicy/AWS_Privacy_Notice__German_Translation.pdf ☒ als PDF-Datei gesichert/beiliegend.

Art der Beauftragung (ggf. gemischt):	☒ Gemeinsam Verantwortlicher ☒ Auftragsverarbeiter. ☐ Dritter ☐ Nicht an der Datenverarbeitung beteiligt (z.B. Hosting auf eigenem Server **AWS als Auftragsverarbeiter:** Wenn Kunden AWS-Services verwenden, um personenbezogene Daten in den Inhalten zu verarbeiten, die sie in die AWS-Services hochladen, fungiert AWS als Auftragsverarbeiter. Kunden können die in den AWS-Services verfügbaren Kontrollen, einschließlich der Sicherheitskonfigurationskontrollen, für den Umgang mit personenbezogenen Daten nutzen. Unter diesen Umständen kann der Kunde selbst als Verantwortlicher oder Auftragsverarbeiter fungieren, während AWS als Auftragsverarbeiter oder Unterauftragsverarbeiter fungiert. AWS bietet ein DSGVO-konformes AWS GDPR Data Processing Addendum (AWS GDPR DPA), das die Verpflichtungen von AWS als Auftragsverarbeiter beinhaltet. Die AWS GDPR DPA mit Standardvertragsklauseln ist Teil der AWS-Servicebedingungen und ist automatisch für alle Kunden verfügbar, die sie zur Erfüllung der DSGVO benötigen. **AWS als Verantwortlicher**: Wenn AWS personenbezogene Daten erhebt und die Zwecke und Mittel der Verarbeitung dieser personenbezogenen Daten festlegt – zum Beispiel, wenn AWS Kontoinformationen (z. B. E-Mail-Adressen, die bei der Kontoregistrierung angegeben wurden) für die Kontoregistrierung, Verwaltung, den Zugriff auf Services speichert, oder Kontaktinformationen für das AWS-Konto, um Hilfe bei Kundensupportaktivitäten zu leisten – handelt AWS als Verantwortlicher. Weitere Informationen zur Verarbeitung personenbezogener Daten durch AWS als Verantwortlicher finden Sie im AWS-Datenschutzhinweis.
URL Datenschutzvereinbarungen (AV-Vertrag/ Vereinbarung gemeinsame Verantwortlichkeit):	URL: Data Processing Agreement: https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf Standardvertragsklauseln Modul 2 (Controller to Processor): https://d1.awsstatic.com/Controller_to_Processor_SCCs.pdf Standardvertragsklauseln Modul 3 (Processor to Processor): https://d1.awsstatic.com/Processor_to_Processor_SCCs.pdf ☒ als PDF-Datei gesichert/beiliegend.
Auskünfte/ Korrespondenz mit Anbieter im Hinblick auf den Datenschutz:	Technische und organisatorische Maßnahmen: https://aws.amazon.com/de/compliance/bsi-c5/ Liste der Unterauftragnehmer: https://aws.amazon.com/de/compliance/sub-processors/ ☒ als PDF-Datei gesichert/beiliegend.
Beschreibung der Funktionsweise/ Zwecks:	☒ Bereitstellung der AWS-Services ☐ Eigene Angaben: [ ].

Verarbeitete Datenkategorien:	☒ Bestandsdaten (Namen, Adressen) Nutzer. (Begriff Nutzer umfasst auch Kunden). ☒ E-Mail-Adressen. ☒ Andere Kontaktdaten der Nutzer. ☒ Vertragsdaten. ☒ Zahlungsdaten Nutzer. ☐ Angaben zu Mitarbeitern (Namen, Adressen, E-Mailadressen). ☐ Weitere Beschäftigtendaten: [ ]. ☒ Login-Informationen von Beschäftigten. ☒ Login-Informationen von Nutzern. ☒ IP-Adressen. ☒ User IDs/ Cookie IDs / Werbe IDs. ☒ Device ID (zB IMEI). ☒ Mac Adresse. ☒ Browsertyp /-version. ☒ Gerätedaten. ☒ Systemdaten. ☒ Standortdaten. ☒ Verhaltensbezogene Daten (geklickte Elemente, Besuchszeitraum, etc.). ☒ Interessensbezogene Daten (Arten aufgerufener Inhalte, Interesse an Angeboten). ☒ Texteingaben. ☒ Fotografien. ☒ Videoaufnahmen. ☒ Audioaufnahmen. ☒ Log-Daten. ☐ Eigene Angaben: [ ].
Betroffene Personen:	☒ Webseitenbesucher. ☒ Geschäftspartner. ☒ Freie Mitarbeiter. ☒ Beschäftigte. ☐ Bewerber. ☐ Eigene Angaben: [ ].
Besondere Kategorien personenbezogenen Daten:	☐ ja (☐ Biometrische Daten ☐ Gesundheitsdaten ☐ Gewerkschaftszugehörigkeit ☐ politische Meinung ☐ Rassische und ethnische Herkunft ☐ Religiöse oder weltanschauliche Überzeugung ☐ Sexualleben /sexuelle Orientierung) ☒ nein
Aufbewahrungsdauer der Daten in Monaten (z.B: (Speicherdauer Cookies):	Eine Löschung erfolgt nach Zweckentfall, spätestens jedoch 90 Tage nach entsprechender Eingabe des Verantwortlichen (vgl. Ziffer 14, AWS GDPR DATA PROCESSING ADDENDUM).

Angaben zur Drittlandsverarbeitung, Risiken und Schutzmaßnahmen

Verarbeitung von Daten im Drittland (außerhalb EU/EWR, auch durch Subunternehmer eines Dienstes)?	☐ nein (keine politisch relevanten oder sonst tendenziellen Inhalte oder Leistungen). ☒ USA. ☐ Kanada. ☐ Israel. ☐ Schweiz. Sonstige Angaben: [ ].
Ist der Datenempfänger im Drittland im Rahmen nationaler Gesetze potentiell zur Herausgabe der aus der EU empfangenen personenbezogenen Daten an Behörden verpflichtet?	☐ nein. ☒ Ja, wegen 50 U.S.C. § 1881a (= FISA 702) i.V.m. section 153 of title 47 U.S.C. o. i.V.m. section 2510 of title 18 U.S.C.; section 2711 of title 18 U.S.C. (insbes. Telekommunikationsanbieter, Anbieter elektronischer Kommunikationsdiensten oder mit Zugang zu elektronischen Kommunikationsdiensten entweder bei der Übertragung oder bei der Speicherung dieser Kommunikation haben – betrifft zB SoMe-Dienste, Webanalysedienste, Tracking- und Profiling-Dienste). Eigene Angaben: [ ].

In welchem Umfang ist der Datenempfänger im Drittland im Rahmen nationaler Gesetze potentiell zur Herausgabe der personenbezogenen Daten von EU-Bürgern an Behörden verpflichtet (trifft insbes. zu auf Telekommunikationsanbieter, Anbieter elektronischer Kommunikationsdiensten oder mit Zugang zu elektronischen Kommunikationsdiensten entweder bei der Übertragung oder bei der Speicherung dieser Kommunikation haben – d.h. z.B. SoMe-Dienste, Webanalysedienste, Tracking- und Profiling-Dienste).	☒ Foreign Intelligence Surveillance Act, Abschnitt 702: Gemäß Abschnitt 702 des FISA kann die Regierung der Vereinigten Staaten "Anbieter von elektronischen Kommunikationsdiensten" dazu zwingen, Informationen über Informationen über Nicht-US-Personen, die sich außerhalb der Vereinigten Staaten befinden für die Zwecke der Informationsbeschaffung ausländischer Geheimdienste. Diese Informationsbeschaffung wird gemeinsam vom Generalstaatsanwalt der USA Generalstaatsanwalt und dem Direktor der Nationalen Nachrichtendienste genehmigt und muss außerdem vom Foreign Intelligence Surveillance Court in Washington DC genehmigt werden. Sobald die Genehmigung erteilt ist, sendet die US-Regierung den betreffenden Anbietern bestimmte "Selektoren" (wie Telefonnummern oder E-Mail-Adressen), die mit bestimmten die mit bestimmten "Zielpersonen" (z. B. Nicht-US-Personen oder juristische Personen) verbunden sind. In Anbieter müssen sich an diese Richtlinien halten und dürfen ihre Nutzer nicht ihren Nutzern mitteilen, dass sie solche Richtlinien erhalten haben. ☒ Foreign Intelligence Surveillance Act, Abschnitt 215: Abschnitt 215 FISA gestattet die nachrichtendienstliche Überwachung sowohl von US-Personen als auch von Nicht-US-Personen, und zwar sowohl innerhalb als auch außerhalb der Grenzen der USA. Die Art und der Typ der Informationen, die gesammelt werden können, unterscheiden sich jedoch von Abschnitt 702 - es handelt sich nicht um ein Gesetz, das sich auf elektronische Daten konzentriert, sondern um ein Gesetz, das auf die Vorlage von Geschäftsunterlagen ("körperliche/greifbare Dinge") gerichtet ist. Abschnitt 215 enthält strengere Sicherheitsvorkehrungen als Abschnitt 702. Jeder Antrag auf Herausgabe von Aufzeichnungen gemäß Abschnitt 215 muss an einen Richter des FISC gerichtet werden und in einer Form vorgelegt werden, in der die spezifischen Auswahlbedingungen der materiellen Dinge, deren Herausgabe angeordnet werden soll, genau festgelegt sind und in der genau beschrieben wird, was benötigt wird und wann es herausgegeben werden muss - allgemeine Anträge dürfen nicht gestellt werden, und eine massenhafte Datenerfassung ist nicht zulässig. ☒ EO 12333 und Presidential Policy Directive 28 ("PPD- 28"): Gemäß EO 12333 dürfen US-Nachrichtendienste (wie die US National Security Agency) Überwachungen außerhalb der USA durchführen. Unter ermächtigt es die US-Geheimdienste insbesondere, Informationen über ausländischen "Signals Intelligence"-Informationen, d. h. Informationen aus der Kommunikation und anderen Daten, die über Funk, Draht oder andere Funk, Draht und anderen elektromagnetischen Mitteln übermittelt werden. Dies kann zum Beispiel den Zugriff auf Unterwasserkabel, die Internetdaten auf dem Weg in die die Vereinigten Staaten transportieren. EO 12333 stützt sich nicht auf die erzwungene Unterstützung von Dienstanbietern, sondern scheint sich stattdessen auf die Ausnutzung von Schwachstellen in der Telekommunikationsinfrastruktur. Darüber hinaus beschränkt die PPD-28 die Verwendung von in großem Umfang gesammelten auf die Aufdeckung und Bekämpfung von sechs Arten von Bedrohungen: a) Spionage und andere Bedrohungen durch ausländische Mächte; b) Terrorismus; c) Bedrohungen durch Massenvernichtungswaffen d) Bedrohungen der Cybersicherheit; e) Bedrohungen für die Streitkräfte der Vereinigten Staaten oder verbündeter Staaten; und f) grenzüberschreitende kriminelle Bedrohungen, einschließlich illegaler Finanzierung und Sanktionsumgehung im Zusammenhang mit den anderen in diesem Abschnitt genannten Zwecken. Die EO 12333 ermächtigt die Regierung der Vereinigten Staaten jedoch nicht Datenempfänger zu zwingen, Nutzer-/Kundeninformationen bereitzustellen.

	☒ Relevanz der Rechtsprechung des EUGH: Für einige Bereiche des US-amerikanischen Überwachungsrechts gibt es eine erkennbare und klar begrenzte Rechtsgrundlage. (Abschnitt 702, Abschnitt 215 FISA). Eine klare Begrenzung fehlt jedoch bei den weitreichenden Befugnisse der Exekutive zum Abfangen von Informationen, die sich im Transit in die USA befinden, gemäß EO 12.333). Ferner können auch Maßnahmen nach Abschnitt 702 und Abschnitt 215 FISA lt. EuGH nicht ausreichend zielgerichtet und damit verhältnismäßig sein. Ferner enthält EO 12.333 keine richterliche Aufsicht. Der EuGH erachtete die Executive Order 12.333 als relevant für die Frage der Datenübermittlung in die EU, da davon ausgegangen wird, dass sie zum Abhören von Kommunikation auf dem Weg in die Vereinigten Staaten (z. B. über Internet-Seekabel) herangezogen wird. PPD-28 Presidential Policy Directive 28 ("PPD-28") gilt für die Überwachung im Rahmen des EO 12.333 und versucht, ein gewisses Maß an Verhältnismäßigkeit einzuführen (d. h. eine Anforderung, dass die Überwachungsmaßnahmen so angemessen wie möglich sein müssen), die sowohl Nicht-US-Personen als auch US-Personen zugutekommt. Die PPD-28 ist zwar kein verbindliches Gesetz, aber es wird argumentiert, dass es als Anweisung des Präsidenten keinen Grund gibt, anzunehmen, dass sie in der Praxis von der Exekutive nicht befolgt wird. Lt. EuGH ist diese Sachlage nicht mit den EWR-Standards vereinbar. ☒ CLOUD Act: Im März 2018 hat der US-Kongress den Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") ratifiziert. Das Gesetz regelt die Herausgabe von Daten an Behörden, auch wenn diese Daten nicht in den USA, sondern beispielsweise auf Servern in der Europäischen Union gespeichert sind. Bei der Verfolgung von organisierter Kriminalität oder Terrorismus haben Behörden in den USA (aber auch in Europa) ein berechtigtes Interesse, schnell an Daten zu kommen. Bei den Diskussionen um den CLOUD Act und alle damit zusammenhängenden Fragen geht es unserer Meinung nach also darum, einen Ausgleich zwischen diesen auf beiden Seiten legitimen Interessen zu finden. Ein wichtiger Punkt im Rahmen des U.S. CLOUD Act ist die Möglichkeit für betroffene Unternehmen, sich gegen eine behördliche Anfrage zu wehren ("may file a motion to modify or quash the legal process"). Diese Möglichkeit besteht zwar prinzipiell, aber nur, wenn bestimmte Bedingungen erfüllt sind. Eine dieser Bedingungen ist, dass das Unternehmen gegen das Recht einer sogenannten "qualifizierten ausländischen Regierung" verstößt. Dabei handelt es sich um Länder, die ein spezielles Exekutivabkommen mit den Vereinigten Staaten im Rahmen des CLOUD-Gesetzes geschlossen haben, das gemäß Abschnitt 25239 in Kraft getreten ist. Die EU verhandelt noch mit den USA über dieses Thema. Hierbei ist zu beachten, dass der CLOUD Act im Rahmen des Schrems II Abkommen keine Relevanz hatte. Die EuGH-Rechtsprechung zu Schrems II betrifft nur die Konstellation, in denen die personenbezogenen Daten zu anderen Zwecken in die USA übermittelt werden und dort dann einer Herausgabeanordnung nach FISA 702 bzw EO 12333 werden.

Im welchen Maße unterliegen die Überwachungsmaßnahmen im Drittland einer behördlichen, gerichtlichen oder sonstigen übergeordneten Aufsicht?	Sowohl auf Bundes- als auch auf Staatsebene gibt es dort, wo es Datenschutzgesetze gibt, eine Überwachung und Regulierung des Datenschutzes. So setzt die Federal Trade Commission (FTC) die Einhaltung des FTC-Gesetzes durch, das Office of Civil Rights (Amt für Bürgerrechte) die Datenschutz- und Sicherheitsvorschriften des HIPAA, die FTC die GLBA Privacy Rule und die Federal Communications Commission die TCPA. Die Generalstaatsanwälte der Bundesstaaten spielen eine Schlüsselrolle bei der Durchsetzung der staatlichen Sicherheits- und Datenschutzgesetze. In den begrenzten Bereichen, in denen die USA den Datenschutz ausweiten, gibt es Anzeichen für eine aktive Durchsetzung und oft erhebliche Geldstrafen. Im Zusammenhang mit der Überwachung wird die richterliche Aufsicht (durch das FISC) auf Abschnitt 702 angewandt. Jedoch betrifft diese richterliche Aufsicht im Rahmen von Abschnitt 702 Maßnahmen auf abstrakter Ebene (als ein Gesamtüberwachungsprogramm) und nicht Entscheidungen, die einzelne Personen betreffen und auch nicht jede nachfolgende Suche/Nutzung von Daten, die die Regierung als Reaktion auf eine Anfrage erhält. . Im Fall der EO 12.333 schreibt PPD-28 vor, dass erhebliche Probleme bei der Einhaltung der Vorschriften, die Nicht-US-Bürger betreffen, dem Director of National Intelligence (DNI) gemeldet werden müssen. Lt. EuGH gibt es jedoch keine gerichtliche Aufsicht über die weitreichenden Befugnisse der Exekutive zum Abfangen von Informationen, die sich im Transit in die USA befinden, gemäß EO 12.333.

Welche Datenschutzbestimmungen existieren in dem Drittland?	In den USA existiert es kein Bundesdatenschutzgesetz, das der DSGVO entspricht. Das US-Datenschutzsystem ist auf Bundesebene nach Sektoren aufgesplittert. Einzelne Bundesstaaten können ihre Gesetze unterschiedlich gestalten; dementsprechend hat die Regulierung nicht den umfassenden Charakter der DSGVO, zumindest nicht direkt. Zu den sektoralen Vorschriften gehören u. a. FISA für Beschränkungen der Überwachung ausländischer Geheimdienste, HIPAA mit Datenschutz- und Sicherheitsanforderungen für bestimmte Gesundheitsdaten oder GLBA mit Datenschutz- und Sicherheitsanforderungen für Finanzdienstleistungen. Abschnitt 5 des Federal Trade Commission (FTC)-Gesetzes verbietet unlautere und betrügerische Handelspraktiken, die ebenfalls gegenüber Unternehmen zur Anwendung kommen können. Auch einzelne Bundesstaaten sind dabei, eigene Datenschutzgesetze zu erlassen, wie z. B. CCPA, das kalifornische Datenschutzgesetz. Unter dem Gesichtspunkt der Sicherheit verpflichten Bundes- und/oder Landesgesetze die meisten US-Unternehmen dazu, angemessene technische, physische und organisatorische Maßnahmen zum Schutz sensibler persönlicher Daten zu ergreifen (z. B. Gesundheits- oder Finanzdaten, Informationen über die Nutzung von Telekommunikationsdiensten, biometrische Daten, Daten, die für Identitätsdiebstahl ausgenutzt werden können, oder andere Informationen, die eine Benachrichtigung bei Sicherheitsverletzungen erfordern). Darüber hinaus verlangen viele Staaten, dass angemessene Sicherheitsmaßnahmen für personenbezogene Daten getroffen werden. Die Anwendung dieser Gesetze hängt in der Regel davon ab, wo die betroffene Person ihren Wohnsitz hat, und bis zu einem gewissen Grad auch davon, wo das Unternehmen ansässig ist. Insbesondere Kalifornien verlangt von jedem Unternehmen, das eine Website betreibt, eine Online-Datenschutzrichtlinie, und die Unternehmen beschränken ihre Datenschutz-richtlinien in der Regel nicht nur auf Einwohner Kaliforniens.
Bestehen bilaterale Abkommen, die personenbezogene Daten von Betroffenen vor Überwachungsmaßnahmen schützen?	Im März 2022 einigten sich die EU-Kommission und der US-Präsident auf den Nachfolger des Privacy Shields, den sogenannten "Trans-Atlantic Data Privacy Framework". Die genauen Spezifikationen und insbesondere Abhilfemaßnahmen für die vom EuGH beanstandeten Risiken sowie Möglichkeiten der Durchsetzung sollen Ende 2022 bekannt gegeben und schnellstmöglich umgesetzt werden. D.h. zum jetzigen Zeitpunkt können noch keine Einschätzungen vorgenommen werden, obwohl auch hier in Zukunft mit einer Entscheidung des EU-Gerichtshofs zu rechnen ist.
Besondere Risiken, die sich ergeben, falls die Nutzung der Leistungen des Verantwortlichen durch US-Sicherheitsbehörden einen Nachteil darstellen könnte.	☒ Nein. ☐ Einreiseverbote. ☐ Beeinträchtigung wirtschaftlicher Interessen. ☐ Relevante Beeinträchtigung der Privatsphäre. ☐ Beeinträchtigung der Glaubensausübung. ☐ Beeinträchtigung der politischen Freiheit. ☒ Sonstige Angaben: [Die Wahrscheinlichkeit des direkten Zugriffs auf die Daten der Betroffenen bei US-Empfängern ist geringer Natur.].
Alternative Verfahren/ Dienste aus der EU und warum sie nicht eingesetzt werden:	☒ Keine EU-Dienste mit vergleichbaren Funktionen vorhanden. ☒ Es wird eine höhere Performance zu anvisierten Zwecken erwartet. ☒ Es wird eine effektivere Kosten-Nutzen-Relation erwartet. ☒ Erfahrung der Mitarbeiter im Umgang mit dem Verfahren/ Einfachere Einarbeitung. ☐ Sonstige Angaben: [ ].

Gewährleistung des Datenschutzniveaus falls Übermittlung in ein Drittland:	☐ Angemessenheitsbeschluss (insbes.: Israel (eingeschränkt), Japan, Kanada (eingeschränkt), Schweiz, vollständige Liste). ☒ EU-Standardvertragsklauseln. ☐ Binding Corparate Rules. ☐ Einwilligung der Nutzer (z.B. im Rahmen der CMP (wenn dort ausdrücklich auf Einwilligung gem. Art. 49 Abs.1 a) DSGVO hingewiesen wird). ☐ sonstige Garantien: [ ].
Standardvertragsklauseln, BCR, wie oben angegeben):	URL: Standardvertragsklauseln Modul 2 (Controller to Processor): https://d1.awsstatic.com/Controller_to_Processor_SCCs.pdf Standardvertragsklauseln Modul 3 (Processor to Processor): https://d1.awsstatic.com/Processor_to_Processor_SCCs.pdf ☒ als PDF-Datei gesichert/beiliegend.
Technische und Organisatorische Maßnahmen, die ergriffen wurden, um ein angemessenes Schutzniveau zu gewährleisten:	☒ Bereitstellung von Transparenzberichten Sicherheitsberichte: https://aws.amazon.com/de/security/security-bulletins/?card-body.sort-by=item.additionalFields.bulletinId&card-body.sort-order=desc&awsf.bulletins-flag=*all&awsf.bulletins-year=*all Amazon Information Request Report (halbjährliche Veröffentlichung): http://d0.awsstatic.com/certifications/Information_Request_Report.pdf ☒ Maßnahmen zur Datensicherheit und zum Schutz der Privatsphäre auf der Grundlage von EU-Zertifizierungen, Verhaltenskodizes oder internationalen Standards (z.B. ISO-Normen): ISO 27001 (Zertifikat beiliegend), ISO 27017 (Zertifikat beiliegend), ISO 27018 (Zertifikat beiliegend), C5, SOC 1, SOC 2, SOC 3, PCI DSS; ☒ „Government data access policy“ o.ä. Richtlinie, die eine angemessene Reaktion gewährleisten soll (Festlegung interner Verfahren mit klarer Zuweisung der Zuständigkeiten für die Datenübermittlung, der Meldewege und der Standardverfahren für formelle und informelle Anträge, insbesondere Verfahren zur Kontrolle von Anträgen von Behörden auf Zugang zu Daten). ☒ Schulung von Mitarbeitern. ☒ Zugangskontrollen und Vertraulichkeitsrichtlinien, die regelmäßig kontrolliert und durch disziplinarische Maßnahmen durchgesetzt werden. ☒ 2-Faktor-Authentifizierung ("2FA"): ☐ Nutzung von Pseudonymen, die von den Behörden des Drittlandes nicht zugeordnet werden könnten (z.B. Pseudonymisierung IP-Adresse). ☒ Anonymisierung, d.h. Verlust des Personenbezug z. B. durch Aggregierung und Löschung Einzeldaten. ☒ Verschlüsselung im Transfer entsprechend dem Stand der Technik. ☒ „Verschlüsselung at rest“, beim Speichern auf Server entsprechend dem Stand der Technik. ☒ Serverstandorte beschränkt auf EU/EWR.

Stehen den betroffenen Personen in dem o.g. Drittland durchsetzbare Rechte (z. B. Auskunft, Löschung) zur Verfügung und besteht im Drittland die Möglichkeit für Betroffene eine gerichtliche Überprüfung für behördliche Zugriffe vorzunehmen und sonstige Rechtsbehelfsmöglichkeiten zu?	☒ Einige Datenschutzgesetze (z. B. Marketing und elektronische Kommunikation, Gesetze über die Aufzeichnung von Telefongesprächen und den Datenschutz in der Kabelkommunikation, das CCPA) als auch Rechte auf Schutz der Privatsphäre können zumindest zum Teil privat, entweder durch Einzelklagen oder durch Sammelklagen auf Unterlassung und Schadenersatz durchgesetzt werden. Der EuGH beanstandete diese Rechte durch verfassungsrechtliche Fragen, z. B. der Klagebefugnis sowie durch fehlenden erkennbaren Schaden in vielen Fällen erschwert. Ferner kann die Fehlende Kenntnis der Überwachungsmaßnahmen die Durchsetzung der Rechte einschränken. Das US-amerikanische System sieht im Allgemeinen keine Rechte für Einzelpersonen vor, Rechtsmittel einzulegen, um Zugang zu den sie betreffenden personenbezogenen Daten zu erhalten oder die Berichtigung oder Löschung dieser Daten zu erwirken. Dementsprechend gibt es in den USA - abgesehen von bestimmten Sektoren oder einzelstaatlichen Gesetzen (wie dem CCPA in Kalifornien) - keine mit der DSGVO vergleichbare Datenschutzgesetze, die den Betroffenen grundlegende Rechte auf Auskunft, Löschung oder Änderung ihrer Daten und auf gerichtliche Durchsetzung dieser Rechte einräumen. Hier sieht der EuGH eine eine Diskrepanz zwischen dem europäischen Verständnis von wirksamen Rechten und Rechtsbehelfen bei Datenschutzverletzungen. Denn das umfasst nicht nur ein Recht auf Entschädigung für Schäden, sondern auch wirksame Rechte auf Zugang, Berichtigung oder Löschung von Daten. Ferner kann der Schutz des Rechts auf Privatsphäre im vierten Verfassungszusatzes nur von US-Bürgern in Anspruch genommen werden. ☒ ja, im Rahmen der Klausel 14 des Beschlusses (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer verpflichtet sich der Anbieter zur Gewährleistung der Rechte der Betroffenen. Soweit die EO 12333 einschlägig ist, ermächtigt diese Regelung die Regierung der Vereinigten Staaten nicht Datenempfänger zu zwingen, Nutzer-/Kundeninformationen bereitzustellen.
Informationen angegeben durch/ am:	Name: Björn Barthelmes, Andreas Bersch Datum: 12.09.2022-14.09.2022

Prüfung des Datenschutzniveaus, Restrisiken und Hinweise

Abwägung und Ergebnis:	**Die Abwägung hat ergeben, dass die möglichen Risiken der Nutzer als gering einzustufen sind und/oder durch die genannten vertraglichen und/oder den technischen sowie organisatorischen Maßnahme auf ein Maß gesenkt werden, dass den Anforderungen der Art. 44 ff. DSGVO an eine rechtmäßige Verarbeitung im Drittland knüpft.** Es besteht insbesondere kein Grund zur Annahme, dass die für die Verarbeitung personenbezogener Daten durch den Anbieter geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Datenempfänger an der Erfüllung seiner Pflichten gemäß diesen Klauseln hindern. Dies basiert auf dem Verständnis, dass Rechtsvorschriften und Gepflogenheiten, die den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, um eines der in Artikel 23 Absatz 1 der DSGVO aufgeführten Ziele sicherzustellen. Der Datenempfänger erklärte sich vertraglich damit einverstanden, während der Laufzeit des Vertrags den Verantwortlichen unverzüglich zu benachrichtigen, wenn er Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten, die nicht mit den o.g. Anforderungen im Einklang stehen; hierunter fällt auch eine Änderung der Rechtsvorschriften des Drittlandes oder eine Maßnahme (z. B. ein Offenlegungsersuchen). Bei der Prüfung wurden insbesondere die folgenden Aspekte berücksichtigt: ▪ die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten, ▪ die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien, ▪ alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden. Insofern der Anbieter als verantwortlicher Dritter handelt bzw. eine etwaige Mitverantwortung mit der Übermittlung der Daten in die EU-Abhängigkeit endet, ist zum Zeitpunkt der Datenübermittlung in die USA nur der Anbieter allein verantwortlich gemäß Art. 44 ff. DSGVO. Nach den Datenschutzbestimmungen des Anbieters erfolgt diese Übermittlung auf der Grundlage von Standardvertragsklauseln. Insofern der Anbieter als Auftragsverarbeiter handelt und eine Beschränkung der regelmäßigen Verarbeitungsprozesse auf EU-Servern zusichert, sind Datenübermittlungen in die USA auf wenige Ausnahmefälle für die eine Konsultations- bzw. Mitteilungsregelung besteht beschränkt. Dementsprechend sprechen die vorstehenden Prüfungsergebnisse erst recht für die Zulässigkeit der Verarbeitung.

Bestehende Unsicherheiten und/oder Risiken sowie ergriffene Maßnahmen:	▪ Generelle rechtliche Unklarheit im Hinblick auf Drittlandtransfers als Folge des Wegfalls des „Privacy-Shield“ sowie des EUGH-Urteils (Schrems II). Unklarheit besteht auch hinsichtlich der Rechtsauffassung des Anbieters bezüglich der fehlenden Verantwortlichkeit im Hinblick auf dessen Datenübermittlungen zwischen seiner EU-Dependance und den USA. ▪ Durchführung einer Rechtmäßigkeits- und Risikoprüfung. ▪ Fortlaufende und regelmäßige Evaluierung der Sach- und Rechtslage. ▪ Fachgerechte interne/ und externe Beratung, bzw. Einholung der erforderlichen Expertise. ▪ Abwägung der Risiken durch den Verantwortlichen unter handelsrechtlichen Gesichtspunkten einer ordnungsgemäßen Unternehmensführung und innerhalb eines der Rechtslage entsprechenden Entscheidungsspielraums.
Empfohlene Maßnahmen:	Es wird empfohlen, die verfügbaren Einstellungsmöglichkeiten auszuschöpfen, um den höchstmöglichen Datenschutz unter Berücksichtigung der Anforderungen zu gewährleisten. Dazu gehören insbesondere: ▪ Beschränkung der Speicherdauer der Daten (z.B. Einstellung ab wann Daten anonymisiert/gelöscht werden). ▪ Vorab-Hinzuziehen des Datenschutzbeauftragten vor einer möglichen zukünftigen erweiterten Nutzung bzw. einem erweiterten Einsatz der AWS Services (insbes. im Falle der Hinzunahme weiterer Services, Erweiterung auf Workflow-Ebene). ▪ Regelmäßige Kontrolle der Datenhaltung durch den Fachbereich (u.a. Löschung Alt-Daten bzw. nicht mehr benötigter Daten nach Zweckentfall oder -erfüllung). ▪ Einhaltung des Data Privacy by default-Prinzips durch den Fachbereich: Insbesondere Verzicht auf Verarbeitung von Daten, die für den jeweiligen Zweck nicht erforderlich sind. ▪ Dokumentation der Verarbeitungen, inkl. der betr. Datenarten und Verarbeitungszwecke durch den Fachbereich sowie Bereitstellung der Informationen für den betrieblichen Datenschutzbeauftragten.
Weitere Anmerkungen:	
Prüfung durchgeführt durch/ am:	Name: Björn Barthelmes Datum: 12.09.2022-14.09.2022