AUFTRAGSVERARBEITUNGSVERTRAG

zur **Teilnehmer-Vereinbarung**

(nachfolgend: „**Vereinbarung**“)

zwischen dem

„**Teilnehmer**“ aus der Vereinbarung

(nachfolgend auch „**Auftraggeber**“ genannt)

und

„**Trustlog**“ aus der Vereinbarung

(nachfolgend auch „**Auftragnehmer**“ genannt)

(nachfolgend beide einzeln auch „**Partei**“ und zusammen „**Parteien**“ genannt)

PRÄAMBEL

Die Parteien haben die oben genannte Vereinbarung abgeschlossen, nach welcher der Auftragnehmer Leistungen für den Auftraggeber erbringt und nach welcher dieser Auftragsverarbeitungsvertrag mit dem Inkrafttreten der Vereinbarung gleichsam in Kraft tritt. Dieser AVV schafft die gemäß Artikel 28 (3) DS-GVO nötige vertragliche Grundlage für die Verarbeitung personenbezogener Daten durch den Auftragnehmer bei der Erbringung der Leistungen des Auftragnehmers.

Dies vorausgeschickt, vereinbaren die Parteien Folgendes:

1 BEGRIFFSBESTIMMUNGEN

1.1 Begriffsbestimmungen der DS-GVO

Für die Zwecke dieses Auftragsverarbeitungsvertrags finden die Begriffsbestimmungen des Artikel 4 DS-GVO und der Vereinbarung Anwendung, sofern nachfolgend in Abschnitt 1.2 nichts anderes bestimmt ist.

1.2 Besondere Begriffsbestimmungen dieses Auftragsverarbeitungsvertrags

1.2.1 „**Auftragsverarbeitungsvertrag**“ oder “**AVV**” ist dieser Vertrag einschließlich seiner Anhänge.

1.2.2 „**Banktage**“ sind Tage, an denen Banken am Sitz des Auftragnehmers geöffnet sind.

1.2.3 „**DS-GVO**” ist die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016.

1.2.4 „**Dritte**” (oder einzeln „**Dritter**“) sind alle natürlichen oder juristischen Personen, Behörden, Einrichtungen, betroffene Personen oder andere Stellen, außer den Parteien und natürlichen Personen, die unter der unmittelbaren Verantwortung einer der Parteien stehen und befugt sind, personenbezogene Daten zu verarbeiten.

1.2.5 “**Drittland**” ist jedes Land außerhalb des EWR.

1.2.6 „**EU**” oder „**Union**” ist die Europäische Union.

1.2.7 „**EWR**” ist der Europäische Wirtschaftsraum.

1.2.8 „**Mitgliedstaat**” ist ein Mitgliedstaat der EU und/oder Vertragsstaat des EWR.

1.2.9 „**Sichere Drittländer**” sind alle Drittländer, für die ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Artikel 45 (3) DS-GVO gilt.

1.2.10 „**Standardvertragsklauseln**” oder „SVK” sind die Standardvertragsklauseln in ihrer jeweils aktuellen Fassung der Europäischen Kommission.

1.2.11 „**Unterauftragsverarbeiter**” ist jeder weitere Auftragsverarbeiter, den ein Auftragsverarbeiter gemäß Artikel 28 (2) und (4) DS-GVO in Anspruch nimmt. Klarstellend halten die Parteien fest, dass Dienstleister, die der Auftragsverarbeiter mit reinen Nebenleistungen betraut und die nicht als „weitere Auftragsverarbeiter“ im Sinne des Artikel 28 (2) und (4) DS-GVO tätig werden, keine Unterauftragsverarbeiter sind. Dazu können z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen und Reinigungsleistungen zählen.

2 ANWENDUNGSBEREICH, PARTEIEN UND IHRE JEWEILIGEN ROLLEN

2.1 Anwendungsbereich

Dieser AVV findet Anwendung auf die Verarbeitung personenbezogener Daten durch den Auftragnehmer bei der Erbringung der Services.

2.2 Parteien und ihre jeweiligen Rollen

2.2.1 Im Rahmen dieses AVVs ist der Auftraggeber der Verantwortliche und der Auftragnehmer der Auftragsverarbeiter. Das heißt die Pflichten und Rechte des Verantwortlichen (insbesondere aus Abschnitt 4 dieses AVVs) gelten für den Auftraggeber und die Pflichten des Auftragsverarbeiters (insbesondere aus Abschnitt 5 dieses AVVs) gelten für den Auftragnehmer.

2.2.2 Soweit der Auftraggeber für personenbezogene Daten, die Gegenstand dieses AVVs sind, selbst lediglich als Auftragsverarbeiter für einen anderen Verantwortlichen handelt, ist der Auftragnehmer ein Unterauftragsverarbeiter. Hier gilt:

a) Die Pflichten des Auftragsverarbeiters aus diesem AVV gelten für den Auftragnehmer als Unterauftragsverarbeiter. Der Auftraggeber handelt im Namen des jeweiligen Verantwortlichen und gemäß dessen Weisungen als einziger Ansprechpartner für jedwede Kommunikation zwischen dem jeweiligen Verantwortlichen und dem Auftragnehmer bezüglich der Ausübung der Rechte des Verantwortlichen und der Durchsetzung der Datenschutzpflichten des (weiteren) Auftragsverarbeiters und leitet jede Mitteilung, die vom jeweiligen Verantwortlichen an den Auftragnehmer und umgekehrt gerichtet ist, unverzüglich an den Auftragnehmer bzw. an den jeweiligen Verantwortlichen weiter.

b) Der Auftragnehmer informiert den Auftraggeber unverzüglich über jegliche Mitteilungen (einschließlich jeglicher Weisungen) und/oder Anfragen (einschließlich Informationsanfragen oder Anfragen zur Durchführung von Überprüfungen – einschließlich Inspektionen), die er unmittelbar vom Verantwortlichen empfängt. Der Auftraggeber koordiniert solche Mitteilungen und/oder Anfragen als einziger Ansprechpartner zwischen dem jeweiligen Verantwortlichen und dem Auftragnehmer und unterstützt den Auftragnehmer beim Umgang mit solchen Mitteilungen und/oder Anfragen.

c) Der Auftraggeber legt auf Verlangen des Auftragnehmers diesem eine Liste der jeweiligen Verantwortlichen vor und garantiert dem Aufragnehmer, dass die Beauftragung des Auftragnehmers als Unterauftragsverarbeiter sowie die Ausübung der Rechte des Verantwortlichen durch den Auftraggeber und die Durchsetzung der Datenschutzpflichten des Auftragsverarbeiters (einschließlich etwaiger Weisungen) im Namen des jeweiligen Verantwortlichen stets ordnungsgemäß und wirksam vom entsprechenden Verantwortlichen autorisiert ist und bleiben wird.

3 DETAILS DER VERARBEITUNG

Ort, Gegenstand, Dauer, Art und Zweck der Verarbeitung sowie Art der personenbezogenen Daten und Kategorien betroffener Personen sind in der Vereinbarung sowie in einem groben Überblick in Anhang 1 dieses AVVs festgelegt.

4 PFLICHTEN UND RECHTE DES VERANTWORTLICHEN

4.1 Verantwortlichkeiten des Verantwortlichen

Der Verantwortliche ist für die Einhaltung der nach der DS-GVO auf einen Verantwortlichen anwendbaren Verpflichtungen verantwortlich.

4.2 Weisungsrecht

4.2.1 Der Verantwortliche hat das Recht, Weisungen an den Auftragsverarbeiter bezüglich der Verarbeitung personenbezogener Daten unter diesem AVV zu erteilen. Die Regelungen dieses AVVs, insbesondere die Bestimmung der Details der Verarbeitung gemäß Abschnitt 3, dienen als allgemeine Weisungen, personenbezogene Daten so zu verarbeiten, wie es für die Erbringung der Services nach Treu und Glauben erforderlich ist und mit diesem AVV und der Vereinbarung vereinbar ist. Der Verantwortliche ist befugt, Einzelweisungen mindestens mit den aus der Vereinbarung genannten E-Mail-Adressen in Textform zu erteilen. In dringenden Fällen ist der Verantwortliche befugt, mündliche Einzelweisungen zu erteilen. Der Verantwortliche muss mündliche Weisungen unverzüglich mindestens mit den aus der Vereinbarung genannten E-Mail-Adressen in Textform bestätigen. Durch die Verletzung der Obliegenheit des Verantwortlichen, mündliche Weisungen unverzüglich mindestens in Textform zu bestätigen, wird die Wirksamkeit einer solchen Weisung nicht berührt.

4.2.2 Die individuelle Nutzung von Services der Plattform stellen Einzelweisungen dar, personenbezogene Daten so zu verarbeiten, wie es für die Erbringung der angeforderten Services nach Treu und Glauben erforderlich ist und mit diesem AVV und der Vereinbarung vereinbar ist.

4.2.3 Personen, die gemäß der Vereinbarung autorisiert sind, im Namen des Auftraggebers Einzelweisungen nach Abschnitt 4.2.1 dieses AVV an den Auftragnehmer zu erteilen und Weisungen vom Auftraggeber im Namen des Auftragnehmers zu empfangen, werden in der Vereinbarung durch eine autorisierte E-Mail-Adresse benannt.

Die Parteien benachrichtigen einander unverzüglich mindestens in Textform über etwaige Änderungen der autorisierten E-Mail-Adressen, die in der Vereinbarung

genannt sind. Bis zum Zugang einer solchen Benachrichtigung bei der anderen Partei gelten die autorisierten E-Mail-Adressen, die in der Vereinbarung genannt sind, weiterhin als autorisiert, Weisungen zu erteilen und zu empfangen.

4.2.4 Der Verantwortliche dokumentiert die an den Auftragsverarbeiter erteilten Einzelweisungen.

4.3 Informationsrecht, und Überprüfungsrecht, einschließlich Inspektionsrecht

4.3.1 Der Verantwortliche hat das Recht vom Auftragsverarbeiter alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 DS-GVO niedergelegten Pflichten zu verlangen und Überprüfungen – einschließlich Inspektionen – beim Auftragsverarbeiter entweder selbst oder durch einen von ihm beauftragten Prüfer durchzuführen. Der Auftragsverarbeiter stellt dem Verantwortlichen diese Informationen zur Verfügung und ermöglicht und trägt zu solchen Überprüfungen bei.

4.3.2 Zum Nachweis der Einhaltung seiner Pflichten kann der Auftragsverarbeiter aktuelle Bescheinigungen, Berichte oder Auszüge aus Berichten von unabhängigen Stellen (z.B. Wirtschaftsprüfer, interne Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzprüfer, Qualitätsprüfer) oder eine entsprechende Zertifizierung durch eine IT-Sicherheits- oder Datenschutzüberprüfung (z.B. gemäß dem BSI Grundschutz) vorlegen.

4.3.3 Vor der Durchführung von Überprüfungen – einschließlich Inspektionen – prüft der Verantwortliche die vom Auftragsverarbeiter bereitgestellten Informationen dahingehend, ob diese zum Nachweis der Einhaltung der in Artikel 28 DS-GVO niedergelegten Pflichten des Auftragsverarbeiters genügen. Der Verantwortliche führt Überprüfungen – einschließlich Inspektionen – nur durch, wenn der Verantwortliche die nachvollziehbare Auffassung vertritt, dass die vom Auftragsverarbeiter bereitgestellten Informationen nicht ausreichend sind oder dass der Auftragsverarbeiter seine Pflichten aus Artikel 28 DS-GVO oder dieses AVVs verletzt.

4.3.4 Der Verantwortliche informiert den Auftragsverarbeiter rechtzeitig, mindestens zwei (2) Wochen im Voraus, über die Durchführung einer Überprüfung, einschließlich einer Inspektion und führt Inspektionen während der normalen Geschäftszeiten des Auftragnehmers durch. Das Betreten der Räumlichkeiten des Auftragsverarbeiters darf nur in ständiger Anwesenheit eines Vertreters des Auftragsverarbeiters erfolgen. Dieser Vertreter ist befugt, Entscheidungen über den Verlauf der Inspektion zu treffen, soweit dies erforderlich ist, um Störungen des Geschäftsbetriebs des Auftragsverarbeiters zu vermeiden und dessen Geheimhaltungspflichten gegenüber Dritten zu wahren.

4.3.5 Soweit in diesem Abschnitt 4.3 geregelte Informations- und Überprüfungsrechte gemäß der nachvollziehbaren Einschätzung des Auftragsverarbeiters Informationen/Daten/Datenbanken/Datenträger von Dritten betreffen, die nicht der datenschutzrechtlichen Verantwortlichkeit des Verantwortlichen unterfallen und deren Offenlegung an den Verantwortlichen rechtlich unzulässig wäre, oder der Ausübung der Informations- und Überprüfungsrechte Vertraulichkeitsinteressen entgegenstehen, kann der Verantwortliche seine Informations- und Überprüfungsrechte nicht selbst wahrnehmen. Insoweit steht es dem Verantwortlichen frei, zur Wahrnehmung seiner Informations- und Überprüfungsrechte einen berufsrechtlich zur Verschwiegenheit verpflichteten Dritten (zum Beispiel Wirtschaftsprüfer) einzusetzen, der die Einhaltung datenschutzrechtlicher Vorgaben und die Wahrung etwaiger Vertraulichkeitsinteressen bei Ausübung der Informations- und Überprüfungsrechte sicherstellt.

4.3.6 Der Verantwortliche darf regelmäßige Überprüfungen – einschließlich Inspektionen – höchstens einmal pro Kalenderjahr durchführen. Der Verantwortliche darf zusätzliche Überprüfungen – einschließlich Inspektionen – nur aus einem von ihm nachzuweisenden wichtigen Grund durchführen. Der Verantwortliche hat die Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters, die dem Verantwortlichen während einer Überprüfung – einschließlich Inspektionen – bekannt werden, streng vertraulich zu behandeln. Der Verantwortliche erstellt keine Aufzeichnungen über diese Informationen, es sei denn, dies ist für die Ausübung seines Prüfungsrechts unbedingt erforderlich.

5 PFLICHTEN DES AUFTRAGSVERARBEITERS

5.1 Verarbeitung auf dokumentierte Weisung des Verantwortlichen

5.1.1 Der Auftragsverarbeiter verpflichtet sich zur Einhaltung der DS-GVO und verarbeitet die personenbezogenen Daten, die Gegenstand dieses AVVs sind, nur auf dokumentierte Weisung des Verantwortlichen auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation - sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.1.2 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DS-GVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Der Auftragsverarbeiter ist befugt, die Ausführung der jeweiligen Weisung auszusetzen, bis sie vom Verantwortlichen bestätigt oder geändert wurde.

5.2 Vertraulichkeit der Erfüllungs- und Verrichtungsgehilfen

Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten, die Gegenstand dieses AVVs sind, befugten Personen zur

Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

5.3 Sicherheit der Verarbeitung

5.3.1 Der Auftragsverarbeiter ergreift alle gemäß Artikel 32 DS-GVO erforderlichen Maßnahmen, welche in Anhang 2 dieses AVVs festgelegt sind. Diese technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragsverarbeiter ist daher befugt, zusätzliche oder alternative Maßnahmen zu den in Anhang 2 dieses AVVs aufgeführten Maßnahmen zu ergreifen, solange das Sicherheitsniveau der bis dahin festgelegten Maßnahmen nicht unterschritten wird. Der Auftragsverarbeiter dokumentiert alle Änderungen der Maßnahmen und legt sie dem Verantwortlichen auf Anfrage vor.

5.3.2 Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten, die Gegenstand dieses AVVs sind, bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

5.4 Beauftragung weiterer Auftragsverarbeiter (Unterauftragsverarbeiter)

5.4.1 Der Auftragsverarbeiter hält die folgenden in Artikel 28 (2) und (4) DS-GVO genannten Bedingungen für die Beauftragung eines weiteren Auftragsverarbeiters ein:

a) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartigen Änderungen Einspruch zu erheben.

b) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags dieselben Datenschutzpflichten auferlegt, wie sie in diesem AVV festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt.

c) Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

5.4.2 Der Auftragnehmer handelt als einziger Ansprechpartner für jedwede Kommunikation zwischen dem Auftraggeber und jedem Unterauftragsverarbeiter bezüglich der Ausübung der Rechte des Verantwortlichen und der Durchsetzung der Verpflichtungen des Auftragsverarbeiters im Namen des jeweiligen Verantwortlichen und gemäß den Weisungen des jeweiligen Verantwortlichen. Der Auftragnehmer verpflichtet sich als einziger Ansprechpartner, jede Mitteilung, die vom Auftraggeber an einen Unterauftragsverarbeiter gerichtet ist, unverzüglich an den jeweiligen weiteren Unterauftragsverarbeiter weiterzuleiten. Der Auftragnehmer verpflichtet sich als einziger Ansprechpartner, jede Mitteilung, die von einem Unterauftragsverarbeiter an den Auftraggeber gerichtet ist, unverzüglich an den Auftraggeber weiterzuleiten.

5.4.3 Der Auftraggeber erteilt hiermit die gesonderte Genehmigung, die Unterauftragsverarbeiter, die in Anhang 3 festgelegt sind, unter den in Abschnitt 5.4.1 genannten Bedingungen zu beauftragen und erteilt weiter hiermit die allgemeine Genehmigung, Unterauftragsverarbeiter unter den in Abschnitt 5.4.1 genannten Bedingungen zu beauftragen.

5.4.4 Der Verantwortliche kann gegen eine beabsichtigte Änderung hinsichtlich der Hinzuziehung oder der Ersetzung eines Unterauftragsverarbeiters Einspruch erheben, indem er dem Auftragsverarbeiter unverzüglich, spätestens jedoch innerhalb von zehn (10) Banktagen nach Erhalt der Änderungsinformationen, in Textform benachrichtigt, dass er von seinem Einspruchsrecht Gebrauch macht. Bei einem solchen Einspruch wird der Auftragnehmer angemessene Anstrengungen unternehmen, um dem Verantwortlichen eine Anpassung der jeweils betroffenen Verarbeitungen zur Verfügung zu stellen oder eine wirtschaftlich zumutbare Anpassung der Nutzung der jeweils betroffenen Leistung vorzuschlagen, um eine Verarbeitung personenbezogener Daten durch den beanstandeten Unterauftragsverarbeiter zu vermeiden. Falls der Auftragnehmer eine derartige Anpassung nicht innerhalb eines angemessenen Zeitraums von maximal dreißig (30) Banktagen vornehmen kann, ist der Auftraggeber berechtigt, die betroffenen Leistungen zu kündigen, welche der Auftragnehmer nicht ohne Einsatz des beanstandeten Unterauftragsverarbeiters erbringen kann. Sollte die Nutzung der Plattform entsprechend der Vereinbarung ohne die Beauftragung des Unterauftragsverarbeiters, gegen den das Einspruchsrecht geltend gemacht wurde, nicht möglich sein, besteht ein beiderseitiges Sonderkündigungsrecht. Die Beweislast der Unmöglichkeit der Nutzung liegt beim Auftragnehmer. Dem Auftraggeber werden für die Zeit nach Wirksamwerden der Kündigung sämtliche für die gekündigten Leistungen im Voraus gezahlten Gebühren erstattet und wegen einer solchen Kündigung wird der Auftragnehmer keine zusätzlichen Gebühren verlangen.

5.5 Unterstützungspflichten

5.5.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der betroffenen Personen nachzukommen. Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter den Verantwortlichen außerdem bei der Einhaltung der in den Artikel 32 bis 36 DS-GVO genannten Pflichten bezüglich personenbezogener Daten, die Gegenstand dieses AVVs sind.

5.5.2 Der Auftragsverarbeiter informiert den Verantwortlichen, nachdem er Kenntnis von einem Antrag einer betroffenen Person auf Wahrnehmung ihrer Rechte bezüglich personenbezogener Daten erhalten hat, die Gegenstand dieses AVVs sind, soweit der jeweilige Antrag dem Verantwortlichen konkret zuordenbar ist.

5.6 Löschung oder Rückgabe nach dem Ende der Vereinbarung

Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen entweder alle personenbezogenen Daten, die Gegenstand dieses AVVs sind, oder gibt diese an den Verantwortlichen zurück und löscht die vorhandenen Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Der Auftragsverarbeiter bewahrt seine Unterlagen zum Nachweis der Einhaltung der Pflichten aus Artikel 28 DS-GVO und diesem AVV gemäß den entsprechenden Aufbewahrungsfristen auch nach Abschluss der Erbringung der Verarbeitungsleistungen auf.

6 BEI NUTZUNG VON ANBIETERN AUS DRITTLÄNDERN

6.1 Etwaige Anbieter aus Drittländern

6.1.1 Der Auftragnehmer und etwaige vom Auftragnehmer beauftragte Unterauftragsverarbeiter dürfen personenbezogenen Daten, die Gegenstand dieses AVVs sind, im Rahmen der Erbringung der Services in Drittländern verarbeiten, sofern es sich dabei um Sichere Drittländer handelt oder die in Kapitel V der DS-GVO festgelegten Anforderungen auf andere Weise erfüllt sind.

6.1.2 Unbeschadet der Bedingungen für die Beauftragung eines Unterauftragsverarbeiters (Abschnitt 5.4 dieses AVV), erteilt der Auftraggeber dem Auftragnehmer hiermit die Genehmigung, personenbezogene Daten, die Gegenstand dieses AVVs sind, auf der Grundlage von Standardvertragsklauseln an Unterauftragsverarbeiter in einem Drittland zu übermitteln, die dann solche personenbezogenen Daten auf Grundlage der Standardvertragsklauseln verarbeiten dürfen.

6.2 Übermittlungen an vom Verantwortlichen individuell bestimmte Empfänger

6.2.1 Ein wesentlicher Bestandteil der Services, die Gegenstand dieses AVV sind, ist der Austausch von Informationen zwischen dem Verantwortlichen als Teilnehmer und anderen an einem Aval Beteiligten, insbesondere dem jeweiligen Avalgeber. In diesem Zusammenhang übermittelt der Auftragnehmer Daten, die Gegenstand dieses AVV sind, entsprechend den konkreten Weisungen des Verantwortlichen gemäß Abschnitt 5.1.1 dieses AVV an den jeweiligen Empfänger, insbesondere den Avalgeber. Abhängig von der konkreten Weisung des Verantwortlichen kann es sich hierbei beispielsweise um Avalgeber oder sonstigen Empfänger in Drittländern handeln.

6.2.2 Der Auftragnehmer wird konkrete Weisungen zur Übermittlung ungeachtet und ohne Prüfung des Verarbeitungsorts des jeweiligen Avalgeber oder eines sonstigen Empfängers gemäß den Regelungen dieses AVV befolgen. Der Auftraggeber gewährleistet, dass die jeweilige Übermittlung sowohl aus Sicht des Verantwortlichen als auch aus Sicht des Auftragsverarbeiters die in Kapitel V der DS-GVO festgelegten Anforderungen erfüllt.

7 AUFWÄNDE DES AUFTRAGGEBERS

7.1.1 Die eigenständige Ausübung der auf der Plattform vorgesehenen Funktionen durch den Auftraggeber und die Ausübung seiner Rechte gemäß der DS-GVO löst für den Auftraggeber keine Kosten aus.

7.1.2 Im Falle eines Missbrauchs seiner Rechte (z.B. wiederholter Wunsch nach Inspektionen innerhalb einer kurzen Zeit, obgleich kein Verstoß seitens des Auftragnehmers vorliegt) erstattet der Auftraggeber etwaige Aufwände des Auftragsnehmers unter diesem AVV; für Tätigkeiten gilt ein Stundensatz von 90 Euro (netto). Der Auftragnehmer kann auf die Geltendmachung verzichten, insb. wenn sich die Aufwände in einem angemessenen Umfang bewegen.

8 HAFTUNG

Für die Haftung des Auftragnehmers bezüglich Ansprüche aus diesem AVV gilt Art. 82 DS-GVO nach Maßgabe der Bestimmung der Vereinbarung zur Haftung entsprechend.

9 FREISTELLUNG

9.1 Wenn Dritte Ansprüche (einschließlich Schadensersatz und/oder Geldbußen) gegen den Auftragnehmer in solchen Fällen geltend machen, in denen der Auftraggeber gegen die DS-GVO verstößt und/oder in denen der Auftraggeber gegen anderes geltendes Datenschutzrecht und/oder die Rechte des Betroffenen verstößt („Ansprüche"), kann der Auftragnehmer vom Auftraggeber verlangen, die

Verantwortung für die Abwehr der Ansprüche zu übernehmen und den Auftragnehmer von den Ansprüchen in dem Umfang freizustellen, wie sie durch ein rechtsverbindliches Urteil festgestellt wurden oder vom Auftraggeber mit Zustimmung des Auftragnehmers verglichen oder anerkannt wurden. Der Auftraggeber trägt die Kosten, die im Zusammenhang mit der Abwehr oder Beilegung der Ansprüche angefallen sind, und erstattet dem Auftragnehmer etwaige Kosten, die ihm entstanden sind. Sonstige gesetzliche und vertragliche Ansprüche des Auftragnehmers im Zusammenhang mit den Ansprüchen, insbesondere auf Ersatz weiterer Schäden des Auftragnehmers, bleiben unberührt.

9.2 Wenn der Auftragnehmer den Auftraggeber auffordert, Maßnahmen gemäß diesem Abschnitt 9 zu ergreifen, überlässt der Auftragnehmer dem Auftraggeber die alleinige interne Kontrolle über die Abwehr der Ansprüche und unterstützt den Auftraggeber auf dessen Kosten angemessen bei der Abwehr dieser Ansprüche.

9.3 Der Auftraggeber ist nicht zur Freistellung gemäß diesem Abschnitt 9 verpflichtet, wenn sich die Ansprüche aus einem Verstoß des Auftragnehmers gegen diesen AVV ergeben.

10 INKRAFTTRETEN, LAUFZEIT, ANWENDBARES RECHT UND GERICHTSSTAND

10.1 Dieser AVV tritt gleichzeitig mit dem Inkrafttreten der Vereinbarung (Hauptvertrag) automatisch in Kraft.

10.2 Die Laufzeit dieses AVVs richtet sich nach der Laufzeit der Vereinbarung.

10.3 Das anwendbare Recht und der Gerichtsstand richten sich nach den Regelungen hierzu in der Vereinbarung.

11 SCHLUSSBESTIMMUNGEN

11.1 Benachrichtigung über Defizite dieses Auftragsverarbeitungsvertrags

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er der Ansicht ist, dass dieser AVV nicht den Anforderungen der einschlägigen Bestimmungen der DS-GVO und/oder etwaiger Richtlinien, Empfehlungen oder sonstiger Positionen der Aufsichtsbehörden, insbesondere des Europäischen Datenschutzausschusses (EDSA), an einen Auftragsverarbeitungsvertrag entspricht. In diesem Fall bemühen sich der Auftraggeber und der Auftragnehmer, diesen AVV an die gesetzlichen und/oder behördlichen Anforderungen anzupassen.

11.2 Änderungen und Ergänzungen dieses Auftragsverarbeitungsvertrags

Der Auftragnehmer ist berechtigt Änderungen und Ergänzungen an diesem AVV vornehmen, wenn dies aus rechtlichen und technischen Gründen oder bei Veränderung der Gesetzeslage, höchstrichterlicher Rechtsprechung oder der Marktgegebenheiten erforderlich wird und sofern die Änderungen für den Auftraggeber nicht unzumutbar sind. In diesen Fällen wird der Auftragnehmer den Auftraggeber mindestens acht (8) Wochen vor Inkrafttreten der Änderungen davon in geeigneter Weise in Kenntnis setzen. Ist der Auftraggeber mit der Änderung nicht einverstanden, ist er berechtigt, innerhalb von vier (4) Wochen nach Kenntnis der Änderungen diesen AVV zum Wirksamwerden der Änderungen zu kündigen. Setzt der Auftraggeber die Inanspruchnahme der Services fort, so gilt die Änderungen mit Ablauf der Kündigungsfrist als wirksam vereinbart. Auf diese Folgen wird der Auftragnehmer in der Mitteilung hinweisen.

11.3 Salvatorische Klausel

Sollte eine Regelung dieses AVVs ganz oder teilweise unwirksam oder nicht durchsetzbar sein oder werden, berührt dies nicht die Gültigkeit der übrigen Regelungen. Die Parteien verpflichten sich, die unwirksame oder nicht durchsetzbare Regelung gemeinsam durch eine wirksame Regelung zu ersetzen, die der unwirksamen oder nicht durchsetzbaren Regelung entspricht, soweit dies möglich ist. Gleiches gilt für jegliche Regelungslücken dieses AVVs.

11.4 Rangfolge

Bei Widersprüchen zwischen diesem AVV und anderen zwischen den Parteien geschlossenen Verträgen, insbesondere der Vereinbarung, haben die Regelungen dieses AVVs Vorrang, soweit es sich dabei um die in Artikel 28 DS-GVO geregelten Anforderungen handelt.

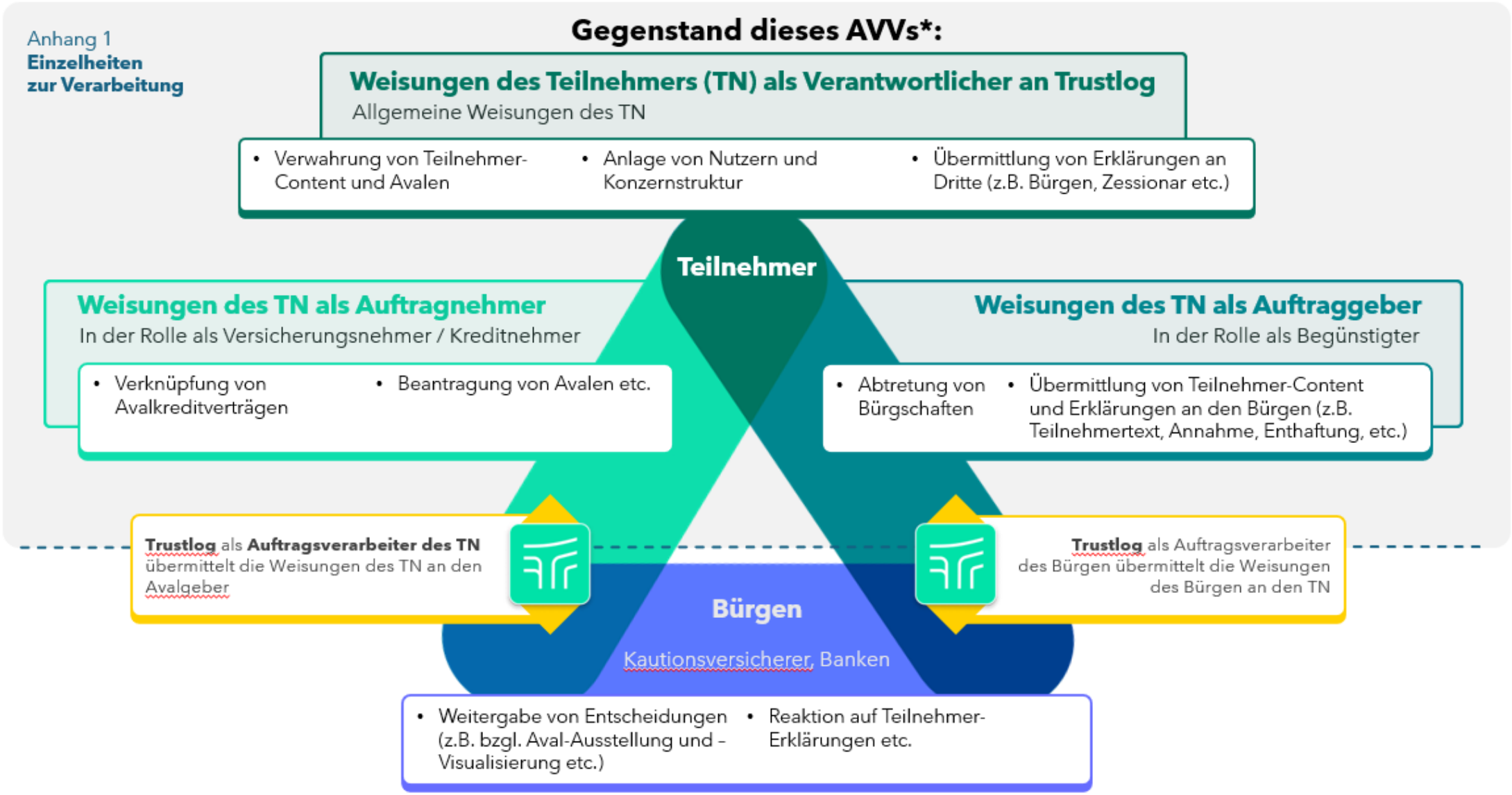
ANHÄNGE

Anhang 1: Grober Überblick zu den Einzelheiten zur Verarbeitung

Anhang 2: Technische und Organisatorische Maßnahmen (TOMs)

Anhang 3: Unterauftragsverarbeiter

Anhang 1
Grober Überblick zu den Einzelheiten zur Verarbeitung



* Schematische Darstellung. Der Gegenstand in Detail ergibt sich aus der Nutzung der Funktionen, die in der Vereinbarung beschrieben sind.

1. Gegenstand der Verarbeitung

Der Gegenstand der Verarbeitung ist die Erbringung der Services.

Abgrenzung der Tätigkeit des Auftragnehmers (als Auftragsverarbeiter) für den Auftraggeber (als Verantwortlichen) von Tätigkeiten des Auftragnehmers (als Auftragsverarbeiter) für andere an einem Aval beteiligten Stellen, insbesondere den jeweiligen Avalgeber (als Verantwortlichen):

Ein wesentlicher Bestandteil der Services, die Gegenstand dieses AVV sind, ist der Austausch von Informationen zwischen dem Auftraggeber (als „Teilnehmer") und dem jeweiligen Avalgeber über die Plattform. In diesem Zusammenhang übermittelt der Auftragnehmer Daten, die Gegenstand dieses AVV sind, entsprechend den konkreten Weisungen des Auftraggebers gemäß Abschnitt 5.1.1 dieses AVV insbesondere an den jeweiligen Avalgeber.

Beim Betrieb der Plattform handelt der Auftragnehmer getrennt für den Auftraggeber (als „Teilnehmer"; diese Tätigkeit ist Gegenstand dieses AVV) und, unabhängig von diesem AVV, ggf. auch im Auftrag von anderen an einem Aval beteiligten Stellen, insbesondere Avalgeber mit personenbezogenen Daten. Dieser AVV und damit auch die Weisungsbefugnis des Auftraggebers erstreckt sich ausschließlich auf diejenigen personenbezogenen Daten, die der Auftragnehmer für den Auftraggeber (als „Teilnehmer") verarbeitet. Weist der Auftraggeber den Auftragnehmer an, bestimmte Informationen an einen Avalgeber zu übermitteln, so erfolgt die Übermittlung im Rahmen dieses AVV. Die weitere Verarbeitung der an den Avalgeber übermittelten Daten fällt nicht mehr unter diesen AVV. Vielmehr verarbeitet der Auftragnehmer diese übermittelten Daten im Auftrag und in der Verantwortlichkeit des jeweiligen Avalgebers. Insbesondere die zwischen dem Auftraggeber und einem Avalgeber abgestimmten Avaltexte sowie abgeschlossene Avale bzw. Übermittlung eines Avalantrags an einen Avalgeber verarbeitet der Auftragnehmer im Auftrag des Auftraggebers (als „Teilnehmer") unter diesem AVV.

Das vorangehende Schaubild veranschaulicht die Beziehungen zwischen dem Auftraggeber und dem Auftragnehmer sowie zwischen dem Auftragnehmer und dem jeweiligen Avalgeber. Die in dieser Ziffer 1 (Gegenstand der Verarbeitung) enthaltenen Beschreibungen dienen lediglich der exemplarischen, stark vereinfachten Veranschaulichung der jeweiligen Beziehungen. Die Einzelheiten der vom Auftragnehmer geschuldeten Leistungen und der Funktionalitäten der Plattform ergeben sich ausschließlich aus den jeweiligen Regelungen der Vereinbarung.

2. Dauer der Verarbeitung

Die Dauer der Verarbeitung ist durch die Dauer der Erbringung der Services bestimmt.

3. Zweck der Verarbeitung

Die Verarbeitung dient dem Zweck der Erbringung der Services, namentlich die Verwaltung bestimmter Datensätze zu Avalen in einer webbasierten Anwendung.

Soweit der Auftragsverarbeiter personenbezogene Daten verarbeitet, um den Verantwortlichen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der betroffenen Person nachzukommen (Abschnitt 5.5 dieses AVV), dient die Verarbeitung außerdem dem Zweck der Erfüllung der rechtlichen Verpflichtungen des Verantwortlichen aus Kapitel III DS-GVO.

Soweit der Auftragsverarbeiter personenbezogene Daten verarbeitet, um den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten zu unterstützen (Abschnitt 5.5 dieses AVV), dient die Verarbeitung außerdem dem Zweck der Erfüllung der rechtlichen Verpflichtungen des Verantwortlichen aus Artikeln 32 bis 36 DS-GVO.

4. Art der Verarbeitung

Alle für die Erbringung der Services erforderlichen Arten der Verarbeitung personenbezogener Daten, insbesondere:

☒	Erheben, Erfassen: Erfassen von vom Auftraggeber übermittelter Daten insb. zu • Gesellschaften und Nutzern auf der Plattform, • Avalgeber, Avale (z.B. Enthaftung, Freigabe, Ablehnung) und Avaltexte • Erfassen von vom Avalgeber dem Teilnehmer übermittelten Daten zu Avalen und zu Avaltexten (z.B. Freigabe / Ablehnung) • Erhebung von Daten zur Übertragung von Avalen von Avalgebern
☒	Organisation, Ordnen: Organisation und Ordnen von Daten zur Verwaltung von vom Auftraggeber hinterlegter Avale und Avaltexte (Avaltemplates): • Organisation und Ordnen zur Erzeugung einer Ansicht des Avals anhand des Datensatzes der Avalgeber, die der Auftraggeber in der Plattform, auch als PDF, einsehen kann • Organisation und Ordnen von Gesellschaften
☒	Speicherung: Speicherung von vom Auftraggeber • hinterlegten Avalen, • übermittelter Daten zu Avalen • übermittelter und hinterlegter Avaltexte (Avaltemplates). • Speicherung von Avalgeber übermittelter Daten zu Avaltexten (Avaltemplates) • Speicherung erzeugter Ansichten des Avals (auch als PDF) • Speicherung von Nutzerdaten • Speicherung von Unternehmensdaten
☒	Anpassung, Veränderung: Anpassung und Veränderung von Daten zur Verwaltung von vom Auftraggeber hinterlegter Avale und Avaltexte (Avaltemplates).

	• Gegebenenfalls Berichtigung auf Einzelweisung des Verantwortlichen, um den Verantwortlichen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der betroffenen Person nachzukommen (Abschnitt 5.5 dieses AVV).
☒	Auslesen, Abfragen: Auslesen von Daten zur Verwaltung von vom Auftraggeber hinterlegten Avalen und Avaltexte (Avaltemplates). • Auslesen von Daten zur Erzeugung einer Ansicht des Avals anhand des Datensatzes der Avalgeber, die der Auftraggeber in der Plattform, auch als PDF, einsehen kann. • Gegebenenfalls Auslesen auf Einzelweisung des Verantwortlichen, um den Verantwortlichen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der betroffenen Person nachzukommen (Abschnitt 5.5 dieses AVV).
☐	Verwendung: -
☒	Offenlegung (durch Übermittlung, Verbreitung oder andere Form der Bereitstellung): • Freigabe von vom Auftraggeber hinterlegter Avaltexte (Avaltemplates) für Avalgeber zur Prüfung der Avaltexte. • Übermittlung von freigegebenen Avaltexten (Avaltemplates) an Avalgeber/Versicherungsnehmer. • Übermittlung von erzeugten Ansichten des Avals an Avalgeber als PDF-Dokument. • Gegebenenfalls Bereitstellung auf Einzelweisung des Verantwortlichen, um den Verantwortlichen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der betroffenen Person nachzukommen (Abschnitt 5.5 dieses AVV).
☐	Abgleich: -
☒	Verknüpfung: Verknüpfung von vom Auftraggeber verwalteter Daten zu Avalen und Avaltexten mit von Avalgeber zur Verfügung gestellten Daten zu Avalen und Avaltexten.
☒	Einschränkung: Gegebenenfalls Einschränkung der Verarbeitung auf Einzelweisung des Verantwortlichen, um den Verantwortlichen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der betroffenen Person nachzukommen (Abschnitt 5.5 dieses AVV).
☒	Löschen, Vernichtung: Löschen von Daten zur Verwaltung von vom Auftraggeber hinterlegten Avalen und Avaltexte (Avaltemplates). • Gegebenenfalls Löschung auf Einzelweisung des Verantwortlichen, um den Verantwortlichen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der betroffenen Person nachzukommen (Abschnitt 5.5 dieses AVV). • Löschung nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Verantwortlichen (Abschnitt 5.6 dieses AVV).

5. Art der Personenbezogenen Daten

Alle für die Erbringung der Services erforderlichen Arten personenbezogener Daten, insbesondere:

Von Beschäftigten des Verantwortlichen (als "Teilnehmer") als Nutzer der Plattform:

- Namen, Geschäftliche Kontaktdaten (Adresse, Telefonnummer, Telefaxnummer, E-Mail-Adresse)
- Zugangsdaten (Benutzername, (verschlüsseltes) Passwort)
- Nutzungsdaten (insbesondere IP-Adressen, Zugriffszeiten, Tätigkeiten und sonstige Daten zur Kommunikation sowie zur Abwicklung und Kontrolle von Transaktionen sowie der technischen Systeme

Von Seiten des Verantwortlichen (als "Teilnehmer") im Zusammenhang mit der Nutzung der Plattform, insbesondere in Avalen:

- Namen und Kontaktdaten (Adresse) von bei Abschluss, Durchführung und Beendigung der Avale und bei der Abstimmung von Avaltexten einbezogenen Personen, zum Beispiel Mitarbeitende des Verantwortlichen (als "Teilnehmer") oder Treuhänder

Von Schuldnern für Avale für den Verantwortlichen ("als Teilnehmer"):

- Namen und Kontaktdaten (Adresse) von bei Abschluss, Durchführung und Beendigung von Avalen einbezogenen Personen, zum Beispiel der Schuldner selbst, Mitarbeitende des Schuldners oder Treuhänder
- Vertragsdaten (insbesondere Ordnungsnummern der am Grundgeschäft beteiligten Parteien)
- Avaldaten (insbesondere Vertragsdaten das Hauptschuldverhältnis betreffend (Auftragsnummer, Auftragsdatum, Art der Arbeit, Ort der Arbeit, Schadendaten, Abrechnungs- und/oder Leistungsdaten oder sonstigen Geschäftsdaten)

Von Avalgebern:

- Namen und Kontaktdaten von bei Abschluss, Durchführung und Beendigung von Avalen und bei der Abstimmung von Avaltexten einbezogenen Personen, zum Beispiel Mitarbeitende des Avalgebers oder Treuhänder

Eine Verarbeitung besonderer Kategorien personenbezogener Daten (Artikel 9 Absatz 1 DS-GVO) findet nicht statt und der Auftraggeber sichert zu, solche Daten nicht in die Plattform hochzuladen oder dem Auftragnehmer anderweitig im Rahmen dieses AVV zu übermitteln.

6. Kategorien der betroffenen Personen

☒	Beschäftigte des Verantwortlichen
☐	Bewerber des Verantwortlichen
☒	Kunden des Verantwortlichen und deren Beschäftigte
☐	Zukünftige Kunden des Verantwortlichen und deren Beschäftigte

☒	Lieferanten des Verantwortlichen und deren Beschäftigte	
☐	Besucher des Verantwortlichen	
☐	Nutzer der Webseite/Apps des Verantwortlichen	
☒	Andere:	Die bei Abschluss, Durchführung und Beendigung der Vereinbarung und/oder des Avals einbezogenen Personen (insbesondere Zeichnungsberechtigte von Avalgebern oder Treuhänder)

7. Ort der Verarbeitung

☒	EU / EWR	
☒	Drittland:	Die Speicherung der Daten erfolgt ausschließlich in der EU (Rechenzentrum in Frankfurt). Im sehr seltenen Einzelfall sind gesetzlich erlaubte Behördenanfrage nicht ausgeschlossen, die grundsätzlich abgewehrt werden, soweit dies gesetzlich möglich ist.

Anhang 2
Technische und organisatorische Maßnahmen des Auftragsverarbeiters

1. Verschlüsselung personenbezogener Daten (Artikel 32 (1) (a) DS-GVO)

Technische Maßnahmen

- Einsatz starker Verschlüsselung (AES-256) für Datenbanken im Ruhezustand. Verwaltung der Verschlüsselungskeys über ein internes, gehärtetes Key-Management-System. AWS Key Management Service wird ab Ende 2026 nicht mehr verwendet.
- Verschlüsselung bei Web-Übertragungen (Einsatz von TLS v1.2 als Mindeststandard; TLS v1.3 wird bevorzugt eingesetzt)
- Komplexe Schlüssel/Passwörter zur Erschwerung von sog. Brute-Force-Attacken
- Zugriff auf personenbezogene Daten nur über authentifizierte Kanäle
- Konsequente Trennung der Zugriffe: Technische Trennung der Nutzerzugriffe basierend auf den Domänen und Unternehmen
- E-Mails werden aktuell standardmäßig von einer Seppmail Appliance signiert und verschlüsselt. Das Verschlüsselungsverfahren nennt sich GINA und ist von Seppmail patentiert. (https://seppmail.de/technologie/gina-verschluesselung/)
- Festplattenverschlüsselungen auf Notebooks und Backup-Datenträgern für Clientsysteme
- Verzicht auf die Nutzung von externen Datenträgern
- Zugriff auf das interne Netzwerk nur über (verschlüsselte VPN-Verbindungen/ Nutzer- und Kennworteingabe) möglich
- Zentrale softwaregestützte Kennwortverwaltung mit Zugriffshistorie
- Einsatz passwortgeschützter Tools zur Pflege von personenbezogenen Daten
- Schutz vor Schadcodesoftware:
  - Zum Schutz vor Angriffen beim Hochladen von Daten ist in Trustlog ein Virenscanner und eine Poison-Detection eingebunden
  - Virenscanner auf jedem Rechner durch IT-Dienstleister sichergestellt
- Kontrolltools zur Überwachung, die von dem IT-Dienstleister ausgewertet werden
- Berechtigungskonzept: In der Trustlog Anwendung ist es möglich ein feingranulares Rechtekonzept vorzusehen, welches sicherstellt, dass Personen, die nur mit bestimmten Zwecken der Verarbeitung betraut sind, auch nur die Daten verarbeiten können, die für diese Zwecke notwendig sind. Daten, zu denen Personen keine Rechte vorliegen, werden diesen auch nicht angezeigt.
- Anmeldeverfahren: Die Trustlog-Plattform nutzt ein Standard-Anmeldeverfahren basierend auf Open-ID Connect.
  - Die Anmeldung erfolgt entweder per Nutzername / Passwort oder per Single Sign On, wenn dies mit Trustlog vereinbart ist.

- Der Zugriff des Nutzers über einen Browser ist per HTTPS abgesichert.
- Kunden, die sich mittels technischer Schnittstelle (API) verbinden, werden entsprechend standardisierter Verfahren authentifiziert und autorisiert.

2. Fähigkeit, die Vertraulichkeit von Verarbeitungssystemen und -diensten auf Dauer sicherzustellen (Artikel 32 (1) (b) DS-GVO)

Zutrittskontrolle

Technische Maßnahmen

- Absicherung der Räume durch Türen und Türschlösser, Zutrittskontrollsystem für den Zutritt zu den Räumen (Magnetkarten für die Eingangstüren) und Türen ohne Klinken an der Außenseite der Eingangstüren
- Abschließen der Büroräume nach Arbeitstag sowie Sicherung durch Alarmanlage
- Videoüberwachung und Videoaufzeichnung des Eingangsbereichs
- Regelmäßige Kontrollgänge des Sicherheitspersonals

Organisatorische Maßnahmen

- Bestehende transparente Infrastruktur: Die eingesetzten Systeme sind für die verschiedenen Zwecke der Datenverwaltung bewusst gewählt und auf deren Sicherheit bewertet:
  - Existenz von Schaubildern der Zusammenhänge der Datenverwaltung
  - Kennzeichnung der Domänen und der Wirkungsbereich der Daten
- Schlüsselprotokollierung
- Sorgfalt bei der Auswahl von Dienstleistern, die vor Ort tätig werden
- Zutritt nur für autorisierte Mitarbeitende
- Durchgehende Begleitung von Besuchern durch Mitarbeitende
- Safe-Aufbewahrung oder Mitnahme von Endgeräten durch Mitarbeitende
- Regelmäßige Schulungen und Sensibilisierungen von Mitarbeitenden
- Erstellung und Umsetzung geeigneter, unternehmensweiter Benutzerrichtlinien für den Umgang mit Technologien mit Gefährdungspotential
- Fortlaufende Unterrichtung der Geschäftsführung und Mitarbeitenden über neue Bedrohungsszenarien aufgrund technischer Weiterentwicklungen
- Schaffung der Rolle / Zuordnung der Aufgaben eines Datenschutzbeauftragten

Zugangskontrolle

Technische Maßnahmen

- Zentrale Firewall (Sophos)
- Zentrale Geräteverschlüsselung (Sophos)
- Jeder Mitarbeitende hat ein eigenes Benutzerkonto
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter)
- Automatisierte Standardroutinen zur Aktualisierung von Schutzsoftware
- Die unternehmensweiten Mitarbeiterpasswörter werden zentral von einer Software verwaltet und die einzuhaltenden Regeln vorgegeben:
  - Authentifizierung zwischen Windows-PC und der Azure AD Cloud erfolgt über verschlüsseltes Kerberos
  - Hinweise der Software zur Sicherheit des gewählten Passworts
  - Die Passwörter sollen aus einer Kombination aus Klein- und Großbuchstaben, Zahlen und gebräuchliche Sonderzeichen in einer Mindestlänge von 8 Zeichen bestehen (PBKDF2).
  - Nach 6 Monaten werden die Passwörter invalidiert, sodass zwingend ein neues Passwort generiert werden muss.
  - Nach 10 erfolglosen Anmeldeversuchen wird der Account für 60 Sekunden gesperrt. Die Sperrdauer multipliziert sich dann nach jedem weiteren Versuch.
  - Kennwörter laufen nach aktueller Richtlinie nicht ab (Microsoft-Empfehlung).
- Zweifaktor-Authentifizierung
- Festplattenverschlüsselungen auf Notebooks und Backup-Datenträgern
- Automatisches Sperren der Bildschirme mit Passwortschutz nach 3 Minuten.
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern
- Getrennte Netzwerke (Gäste-WLAN und Internes Netzwerk)
- VPN- / SSH-Tunnel für Fernzugriffe

Organisatorische Maßnahmen

- Richtlinie zur sicheren Wahl und dem ordnungsgemäßen Umgang mit Passwörtern
- Dokumentierter Ablauf für das Anlegen und Sperren von neuen/scheidenden Mitarbeitenden
- Richtlinie zur Einhaltung von Datenschutz/Datensicherheit
- Richtlinie zur Datenlöschung
- Vertraulichkeitsvereinbarungen

Zugriffskontrolle

Technische Maßnahmen

- Netzlaufwerke mit Zugriff nur für berechtigte Benutzer(gruppen)
- Konzept der Laufwerksnutzung
- Aktenvernichter mindestens P4-Standard
- Physische Löschung von Datenträgern

- Löschen von Datenträgern durch Überschreiben
- Monitoring und Protokollierung von Zugriffen
- Klare Einschränkung von Themenbereichen

Organisatorische Maßnahmen
- Trennung von Berechtigungsbewilligung (organisatorisch) durch Geschäftsführer und Berechtigungsvergabe (technisch) durch IT-Abteilung
- Berechtigungskonzepte
- Verwaltung von Benutzerrechten durch Administratoren
- Minimierung der Anzahl von Administratoren

Trennungskontrolle

Technische Maßnahmen
- Trennung von Produktiv- und Testumgebungen
- Physikalische Trennung (System/Netzwerke/Datenbanken/Datenträger)
- Logische Trennung (System/Netzwerke/Datenbanken/Datenträger)
- Kunden-WLAN beschränkt auf Internetzugriff, kein Zugang zu internen Systemen

Organisatorische Maßnahmen
- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten
- Datensätze mit Zugehörigkeits- und Verwendungsinformation

3. Fähigkeit, die Integrität von Verarbeitungssystemen und -diensten auf Dauer sicherzustellen (Artikel 32 (1) (b) DS-GVO)

Weitergabekontrolle

Technische Maßnahmen
- E-Mail-Verschlüsselung bei Bedarf (via S/MIME und OpenPGP)
- Registrierung der Nutzer und Uhrzeit der jeweiligen Eingabe, Änderung oder Löschung in der Plattform und Monitoring und Protokollierung der Zugriffe
- Datentransport und -bereitstellung über verschlüsselte Verbindungen
- VPN-/SSH-Tunnel für Fernzugriffe
- Zugriff auf personenbezogenen Daten nur über authentifizierte Kanäle
- Verzicht auf externe Datenträger

Organisatorische Maßnahmen

Verfahrensprozess zur Prüfung der Notwendigkeit einer Anonymisierung/Pseudonymisierung personenbezogener Daten vor Weitergabe oder nach Ablauf der gesetzlichen Frist

Eingabekontrolle

Technische Maßnahmen
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Regelmäßige manuelle Kontrolle der Protokolle
- Monitoring und Protokollierung von Zugriffen

Organisatorische Maßnahmen
- Übersicht, in welche Systeme welche Daten eingegeben, geändert oder gelöscht werden können sowie deren Nachvollziehbarkeit durch eindeutige Benutzernamen
- Berechtigungskonzept zur Eingabe, Änderung und Löschung von Daten
- Klare Zuständigkeiten für Löschungen

4. Fähigkeit, die Verfügbarkeit und Belastbarkeit von Verarbeitungssystemen und -diensten auf Dauer sicherzustellen (Artikel 32 (1) (b) DS-GVO)

Verfügbarkeit und Belastbarkeit

Technische Maßnahmen
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter)
- Automatisierte Standardroutinen für Aktualisierung von Schutzsoftware
- Monitoring und Wartung der Server & Infrastruktur
- Technische Überwachung der Plattform mittels Logging- und SIEM-Events
- Client-Überwachung (Monitoring) & Aktualisierung (Patch-Management) der IT-Arbeitsplätze
- Microsoft Office 365 Advanced Threat Protection Plan 2 (CSP)
- BCM und Notfallkonzept
- Regelmäßige Updates werden eingespielt
- Managed Backup der Server zur Wiederherstellung von Daten
- Managed Backup der IT-Arbeitsplätze zur Wiederherstellung von Daten
- Feuer- und Rauchmeldeanlagen
- Feuerlöscher Serverraum
- Temperaturüberwachung Serverraum
- Klimatisierung Serverraum
- Unterbrechungsfreie Stromversorgung Serverraum
- Festplattenspiegelung auf verschiedenen Server
- Alarmanlage bei unberechtigtem Zutritt

Organisatorische Maßnahmen
- Backup & Restore-Konzept

- Backups auf getrennten Servern und Rechenzentren
- Regelmäßige Kontrolle der Backups
- Regelmäßige Wiederherstellungstests zu Daten und Systemen
- Aufbewahrung der Backups in einem anderen Brandabschnitt
- Keine sanitären Anschlüsse und Leitungen oberhalb der Serverräume
- Toolgestütztes Monitoring der Backup-Verwaltung
- Getrennte Partitionen für Betriebssysteme und Daten

5. Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Artikel 32 (1) (c) DS-GVO)

- Managed Backup der Server
- Managed Backup der IT-Arbeitsplätze

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Artikel 32 (1) (d) DS-GVO)

Technische Maßnahmen

- System- und Sicherheitstests, wie z. B. Code-Scan und Penetrationstests
- Die Vereinbarung enthält detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers sowie ein Verbot der Nutzung durch den Auftragnehmer außerhalb des schriftlich formulierten Auftrags oder der Einzelweisungen gemäß dieses AVV.
- Die Vereinbarung enthält detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
- Datenbeständigkeit und -zuverlässigkeit: Für die Trustlog-Plattform wird eine serverseitige Verschlüsselung der S3-Buckets mit Kundenmasterschlüssel (CMKs) verwendet. Amazon S3 verschlüsselt somit ein Objekt, bevor es gespeichert wird, und entschlüsselt es, sobald ein Objekt heruntergeladen wird. Die CMKs werden dabei im AWS Key Management Service (AWS KMS) verwaltet und alle drei Jahre automatisch rotiert. Für den Zugriff auf den AWS KMS wird vom Betriebsteam eine "Organization Account Access Role" verwendet. Nur diese Rolle ist berechtigt auf die KMS-Schlüssel zuzugreifen und aktuell haben ausschließlich die Mitarbeitenden des Betriebsteams das Recht diese Rolle zu übernehmen.
- Absicherung der Webanwendung: Der Zugriff auf die Webanwendung läuft über das Content Delivery Network "Amazon CloudFront", welches so konfiguriert ist, dass HTTP-Anfragen automatisch an HTTPS geleitet werden, wodurch nur verschlüsselte Verbindungen zwischen einem Client und dem Frontend zugelassen werden. Amazon CloudFront verwendet SSLv3- oder TLSv1-Protokolle und eine Auswahl von Cipher Suites, die allesamt das ECDHE-Schlüsselvereinbarungsprotokoll (Elliptic Curve Diffie-Hellman Ephemeral) enthalten. Dieses ermöglicht SSL/TLS-Clients die Bereitstellung von "Perfect Forward Secrecy," welches Sitzungsschlüssel verwendet, die flüchtig sind und nirgendwo gespeichert werden. Auf diese Weise wird die Entschlüsselung von erfassten Daten durch unbefugte Dritte verhindert, selbst wenn der geheime Sitzungsschlüssel selbst kompromittiert wird. Für die Plattform von Trustlog soll zukünftig die Verwendung von mindestens TLS in der Version 1.2 erzwungen werden, wobei TLSv1.3 optional sein soll.
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeitende nach Bedarf/Berechtigung
- Jährliche Überprüfung der Wirksamkeit von technischen Maßnahmen
- Zweckbezogene Minimierung der Erhebung von personenbezogenen Daten
- Ermöglichung aller Rechte für Betroffene nach Maßgabe der DS-GVO
- Einsatz von Firewalls und regelmäßigen Aktualisierungen
- Einsatz von Spamfiltern und regelmäßigen Aktualisierungen
- Einsatz von Virenscannern und regelmäßige Aktualisierungen
- Intrusion Detection Systeme (IDS)
- Intrusion Prevention Systeme (IPS)

Organisatorische Maßnahmen

- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen
- Festgelegte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Einbindung von DSB und ISB in Sicherheitsvorfällen und Datenpannen
- Dokumentation von Sicherheitsvorfällen und Datenpannen
- Informationspflichten der DS-GVO werden erfüllt
- Datenschutzbeauftragter ist bestellt: datenschutz@trustlog.de
- Interner Informationssicherheitsbeauftragter ist bestellt: itsec@trustlog.de
- Datenschutzfolgeabschätzung wird bei Bedarf durchgeführt
- Mitarbeiterschulungen und -verpflichtung auf Datengeheimnis und Vertraulichkeit
- Jährliche Sensibilisierung der Mitarbeitenden
- Prozess zur Bearbeitung von Auskunftsanfragen betroffener Personen
- Sorgfältige Auswahl der Unterauftragsverarbeiter samt Vorabprüfung der Verträge und TOMs vor Beauftragung
- Weisungen werden durch Auftraggeber per E-Mail dokumentiert

Anhang 3
Unterauftragsverarbeiter

Name und Adresse des Unterauftragsverarbeiters	**Umfang, Art und Zweck der Unterauftragsverarbeitung**	**Ort der Unterauftragsverarbeitung**
adesso SE (Adessoplatz 1, 44269 Dortmund), adesso as a service GmbH (3as) (Adessoplatz 1, 44269 Dortmund) Amazon Web Services Germany GmbH (AWS-Germany) (Krausenstr. 38, 10117 Berlin)	Betrieb der Plattform und der entsprechenden Datenbanken.	Siehe Anhang 1 Ziffer 7
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Bereitstellung von Rechenzentrumskapazitäten (dedizierte Server) und Cloud-Services.	Deutschland und EU (Rechenzentren in Falkenstein, Nürnberg, Helsinki)
intercolo GmbH, Carl-Goerdler-Straße 114, 60320 Frankfurt am Main	Unterauftragsverarbeiter zur Dokumentspeicherung.	Deutschland (Rechenzentrum Frankfurt am Main)