Auftragsverarbeitung gemäß Art. 28 DSGVO

Zwischen dem reteach Kunden (Verantwortlicher und Auftraggeber nach diesem Vertrag und der Susell GmbH (Joachimstrasse 7, 10119 Berlin) als Anbieter der reteach Produkte und Auftragnehmer nach diesem Vertrag wird folgender Vertrag geschlossen.

Vorbemerkung

Zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht ein Vertrag über die Nutzung des reteach Produktes des Auftragsverarbeiters durch den Verantwortlichen. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Umsetzung eigener Geschäftszwecke im Zusammenhang mit diesem Vertrag. Eine Übertragung von Funktionen ist ausdrücklich nicht beabsichtigt.

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 - Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff »Datenverarbeitung« oder »Verarbeitung« (von Daten) benutzt wird, wird die Definition der »Verarbeitung« i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen schriftlich in Textform (z.B. E-Mail) erfolgen.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(5) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Jede Übermittlung der Auftraggeberdaten in ein Land außerhalb von EU/EWR ("Drittland") erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und der Auftraggeber dieser Übermittlung schriftlich zugestimmt hat.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

(5) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(7) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind.

5. Datenschutzbeauftragter des Auftragnehmers

Der Auftragnehmer wird einen Datenschutzbeauftragten nach Art. 37 DSGVO benennen, sofern dieser zu benennen ist. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten auf Anforderung mitteilen.

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

9. Unterauftragsverhältnisse

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der **Anlage 2** zu diesem Vertrag angeben. Der Auftragnehmer informiert den Auftraggeber immer über jede Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.

(3) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten. Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht.

(4) Ist die Beauftragung eines Unterauftragnehmers mit der Übermittlung der Auftraggeber-Daten in ein Land außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) (Drittland) verbunden, gelten zusätzlich die Vorgaben aus Ziff. 4 Abs. 2.

(5) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

11. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

12. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

13. Vergütung

Eine Vergütung des Auftragnehmers nach diesem Vertrag ist stets gesondert und schriftlich zu vereinbaren. Hierzu reicht die einfache Textform z.B. per E-Mail.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Der Auftragnehmer sichert zu, bei Änderungen das bestehende Schutzniveau nicht zu unterschreiten. Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer mit dem Auftraggeber mitteilen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Mitteilung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

15. Dauer des Auftrags

Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

16. Beendigung

Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen.

17. Schlussbestimmungen

Die Einrede des Zurückbehaltungsrechts i.S.d. § 273 BGB wird hinsichtlich der verarbeiteten Daten ausgeschlossen.

Dieser Vertrag wird elektronisch abgeschlossen. Für Nebenabreden ist die Schriftform erforderlich. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Diese Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO tritt mit Zustimmung durch den Auftraggeber in Kraft und ersetzt alle zuvor geschlossenen Vereinbarungen zur Auftragsverarbeitung.

Ort / Datum	Ort / Datum
_____	Susell GmbH
(Auftraggeber)	(Auftragnehmer)

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand, Art und Zweck der Verarbeitung

Der Auftragnehmer stellt für den Auftraggeber eine cloudbasierte Software zur Erstellung und Bereitstellung von Lerninhalten sowie der Verarbeitung von Lernaktivitäten und Lernständen zur Verfügung. Die Software dient dem digitalen Training, Schulung, Ausbildung, Fort- und Weiterbildung sowie zur Kommunikation zwischen den Anwendern. Durch die Nutzung der Software werden persönliche Daten der User gespeichert:

2. Art(en) der personenbezogenen Daten

- E-Mail des Nutzers / Anmeldename
- persönliches Passwort
- Protokolldaten über die Lernaktivität des Nutzers unter Angabe durchgeführter Aktivitäten, Zeitpunkt der Aktivität und anderer Verkehrsdaten
- Vertrags- und Zahlungsdaten

Der Auftraggeber kann selbst festlegen, dass weitere Daten gespeichert und verarbeitet werden wie

- Vorname, Nachname, Titel, Anrede
- Geburtsdatum
- Anmeldename und persönliches Kennwort
- Adresse, Stadt, Land
- weitere Daten, die der Nutzer in seinem Profil einstellt

3. Kategorien betroffener Personen

- Mitarbeiter des Auftraggebers
- Kunden des Auftraggebers
- Teilnehmende / Lehrer / Schüler / Studierende
- Externe Trainer des Auftraggebers

Anlage 2 - Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten (»Unterauftragnehmer«).
Dabei handelt es sich derzeit um nachfolgende Unternehmen:

- DigitalOcean, LLC. (Server & Hosting)
  Rechenzentrum: Frankfurt am Main (Deutschland)
  Unternehmenssitz: 101 Avenue of the Americas, New York, NY 10013 (USA)

- Amazon Web Services Inc. (Datei-Speicher & E-Mail-Versand)
  Rechenzentrum: Frankfurt am Main (Deutschland)
  Unternehmenssitz: 410 Terry Avenue North, Seattle, Washington 98109-5210 (USA)

- Streamdiver GmbH (Videoverarbeitung & -hosting)
  Unternehmenssitz: Lakeside B06, 9020 Klagenfurt am Wörthersee (Österreich)

- Rustici Software, LLC (SCORM-Verarbeitung & -hosting)
  Unternehmenssitz: 210 Gothic Ct #100, Franklin, TN 37067 (USA)

- FlowMate GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
  Unternehmenssitz: Harry-Blum-Platz 2, 50678 Cologne, Germany

- Kombo Technologies GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
  Unternehmenssitz: Kottbusser Damm 25-26, 10967 Berlin, Germany

Nur bei Nutzung des eCommerce Moduls für die Abwicklung von Zahlungen:
Stripe: Zahlungsdienstleistungen; Dienstanbieter: Stripe, Inc., 510 Townsend Street, San Francisco, CA 94103, USA; Website: https://stripe.com/de; Datenschutzerklärung: https://stripe.com/de/privacy

Der Auftragnehmer kann nach Maßgabe dieses Vertrages weitere Unterauftragnehmer einsetzen.
Sofern der Auftraggeber die vom Auftragnehmer im Kundenkonto angebotenen Integrationen zu Drittanbietern nutzt (z.B. Integration von Konten des Auftraggebers von Microsoft Teams, Zoom, Stripe oder ein HR Management System) stellt der Auftragnehmer lediglich eine technische Anbindung her ohne die Drittanbieter selbst als eigene Unterauftragnehmer einzusetzen. In diesen Fällen sind die Drittanbieter Auftragsdatenverarbeiter für den Auftraggeber.

Anlage 3 - Technische und organisatorische Maßnahmen (TOA)

Art. 32 DSGVO bestimmt, dass die verantwortliche Stelle technische- und organisatorische Maßnahmen treffen muss. Diese müssen unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen getroffen werden. Diese Maßnahmen müssen die Pseudonymisierung, die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit als auch die Fähigkeit, Systeme nach einem Zwischenfall rasch wiederherstellen zu können, mit einbeziehen.

Weiter muss ein Verfahren implementiert werden, was die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen Maßnahmen gewährleistet.

Die Susell GmbH speichert selbst keine Daten auf eigenen Servern in eigenen Räumlichkeiten, sondern hostet sämtliche Daten in der Cloud bei den in der Anlage gelisteten Subdienstleistern.

Die folgenden technischen- und Organisatorischen Maßnahmen (TOA) wurden durch die Susell GmbH getroffen bzw. die eingesetzten Subdienstleister getroffen:

I. Vertraulichkeit

Vertraulichkeit bedeutet, dass die Daten nur von befugten Personen erhoben, verarbeitet, genutzt usw. werden dürfen.

Die Vertraulichkeit der Datenverarbeitung wird durch die folgenden Maßnahmen gesichert:

1. Zutrittskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte;
Verantwortlich hierfür sind:

Susell GmbH
Unternehmenssitz: Joachimstrasse 7, 10119 Berlin

- Getroffene Maßnahmen:
- Manuelles Schließsystem
- Alarmanlage
- Schlüsselregelung

Die Susell GmbH speichert selbst keine Daten auf eigenen Servern in eigenen Räumlichkeiten, sondern hostet sämtliche Daten in der Cloud bei den in der Anlage gelisteten Subdienstleistern. Ergänzend und im Detail wird daher auf die jeweiligen Maßnahmen der einzelnen Unterauftragsnehmer verwiesen:

DigitalOcean, LLC. (Server & Hosting)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 101 Avenue of the Americas, New York, NY 10013 (USA)

Amazon Web Services Inc. (Datei-Speicher & E-Mail-Versand)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 410 Terry Avenue North, Seattle, Washington 98109-5210 (USA)

Streamdiver GmbH (Videoverarbeitung & -hosting)
Unternehmenssitz: Lakeside B06, 9020 Klagenfurt am Wörthersee (Österreich)

Rustici Software, LLC (SCORM-Verarbeitung & -hosting)
Unternehmenssitz: 210 Gothic Ct #100, Franklin, TN 37067 (USA)

FlowMate GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Harry-Blum-Platz 2, 50678 Cologne, Germany

Kombo Technologies GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Kottbusser Damm 25-26, 10967 Berlin, Germany

2. Zugangskontrolle

Verwehrung des Zugriffs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte;

Verantwortlich hierfür sind:

Susell GmbH
Unternehmenssitz: Joachimstrasse 7, 10119 Berlin

Getroffene Maßnahmen:

- Einsatz von sicheren VPN-Verbindungen
- Verschlüsselung von Datenträgern und mobilen Geräten
- Anti-Viren-Software
- Authentifizierung über Passworteingabe.

Die Susell GmbH speichert selbst keine Daten auf eigenen Servern in eigenen Räumlichkeiten, sondern hostet sämtliche Daten in der Cloud bei den in der Anlage gelisteten Subdienstleistern. Ergänzend und im Detail wird daher auf die jeweiligen Maßnahmen der einzelnen Unterauftragsnehmer verwiesen:

DigitalOcean, LLC. (Server & Hosting)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 101 Avenue of the Americas, New York, NY 10013 (USA)

Amazon Web Services Inc. (Datei-Speicher & E-Mail-Versand)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 410 Terry Avenue North, Seattle, Washington 98109-5210 (USA)

Streamdiver GmbH (Videoverarbeitung & -hosting)
Unternehmenssitz: Lakeside B06, 9020 Klagenfurt am Wörthersee (Österreich)

Rustici Software, LLC (SCORM-Verarbeitung & -hosting)
Unternehmenssitz: 210 Gothic Ct #100, Franklin, TN 37067 (USA)

FlowMate GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Harry-Blum-Platz 2, 50678 Cologne, Germany

Kombo Technologies GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Kottbusser Damm 25-26, 10967 Berlin, Germany

3. Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Verantwortlich hierfür sind:

Susell GmbH
Unternehmenssitz: Joachimstrasse 7, 10119 Berlin

Getroffene Maßnahmen:

- Rollenberechtigungskonzept
- Minimale Anzahl an Administratoren
- Verwaltung der benutzerrechte durch Administratoren

Die Susell GmbH speichert selbst keine Daten auf eigenen Servern in eigenen Räumlichkeiten, sondern hostet sämtliche Daten in der Cloud bei den in der Anlage gelisteten Subdienstleistern. Ergänzend und im Detail wird daher auf die jeweiligen Maßnahmen der einzelnen Unterauftragsnehmer verwiesen:

DigitalOcean, LLC. (Server & Hosting)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 101 Avenue of the Americas, New York, NY 10013 (USA)

Amazon Web Services Inc. (Datei-Speicher & E-Mail-Versand)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 410 Terry Avenue North, Seattle, Washington 98109-5210 (USA)

Streamdiver GmbH (Videoverarbeitung & -hosting)
Unternehmenssitz: Lakeside B06, 9020 Klagenfurt am Wörthersee (Österreich)

Rustici Software, LLC (SCORM-Verarbeitung & -hosting)
Unternehmenssitz: 210 Gothic Ct #100, Franklin, TN 37067 (USA)

FlowMate GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Harry-Blum-Platz 2, 50678 Cologne, Germany

Kombo Technologies GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Kottbusser Damm 25-26, 10967 Berlin, Germany

4. Trennungsgebot

Durch das Trennungsgebot wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Verantwortlich hierfür sind:

Susell GmbH
Unternehmenssitz: Joachimstrasse 7, 10119 Berlin

Getroffene Maßnahmen:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- logische Mandantentrennung
- Verschlüsselung von Datensätzen
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

5. Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten;

Verantwortlich hierfür sind:

Susell GmbH
Unternehmenssitz: Joachimstrasse 7, 10119 Berlin

Getroffene Maßnahmen:

- Mandantentrennung
- Digitales Berechtigungskonzept (z.B. Active Directory)
- Einrichtung und Verwendung von individuellen Benutzernamen
- Vergabe von Zugriffsberechtigungen

Die Susell GmbH speichert selbst keine Daten auf eigenen Servern in eigenen Räumlichkeiten, sondern hostet sämtliche Daten in der Cloud bei den in der Anlage gelisteten Subdienstleistern. Ergänzend und im Detail wird daher auf die jeweiligen Maßnahmen der einzelnen Unterauftragsnehmer verwiesen:

DigitalOcean, LLC. (Server & Hosting)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 101 Avenue of the Americas, New York, NY 10013 (USA)

Amazon Web Services Inc. (Datei-Speicher & E-Mail-Versand)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 410 Terry Avenue North, Seattle, Washington 98109-5210 (USA)

Streamdiver GmbH (Videoverarbeitung & -hosting)
Unternehmenssitz: Lakeside B06, 9020 Klagenfurt am Wörthersee (Österreich)

Rustici Software, LLC (SCORM-Verarbeitung & -hosting)
Unternehmenssitz: 210 Gothic Ct #100, Franklin, TN 37067 (USA)

FlowMate GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Harry-Blum-Platz 2, 50678 Cologne, Germany

Kombo Technologies GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Kottbusser Damm 25-26, 10967 Berlin, Germany

II. Integrität

Integrität bedeutet, dass die Systeme und die dort hinterlegten Daten korrekt, unverändert, und verlässlich sind.

Die Integrität der Daten wird durch folgende Maßnahmen sichergestellt:

1. Eingabekontrolle

Durch die Eingabekontrolle wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind.

Verantwortlich hierfür sind:

Susell GmbH
Unternehmenssitz: Joachimstrasse 7, 10119 Berlin

Getroffene Maßnahmen:

- Mandantentrennung
- Digitales Berechtigungskonzept (z.B. Active Directory)
- Einrichtung und Verwendung von individuellen Benutzernamen
- Vergabe von Zugriffsberechtigungen
- Vergabe von Änderungs- Lösch- und Bearbeitungsrechten aufgrund eines Rollenberechtigungskonzeptes

Die Susell GmbH speichert selbst keine Daten auf eigenen Servern in eigenen Räumlichkeiten, sondern hostet sämtliche Daten in der Cloud bei den in der Anlage gelisteten Subdienstleistern. Ergänzend und im Detail wird daher auf die jeweiligen Maßnahmen der einzelnen Unterauftragsnehmer verwiesen:

DigitalOcean, LLC. (Server & Hosting)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 101 Avenue of the Americas, New York, NY 10013 (USA)

Amazon Web Services Inc. (Datei-Speicher & E-Mail-Versand)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 410 Terry Avenue North, Seattle, Washington 98109-5210 (USA)

Streamdiver GmbH (Videoverarbeitung & -hosting)
Unternehmenssitz: Lakeside B06, 9020 Klagenfurt am Wörthersee (Österreich)

Rustici Software, LLC (SCORM-Verarbeitung & -hosting)
Unternehmenssitz: 210 Gothic Ct #100, Franklin, TN 37067 (USA)

FlowMate GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Harry-Blum-Platz 2, 50678 Cologne, Germany

Kombo Technologies GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Kottbusser Damm 25-26, 10967 Berlin, Germany

2. Weitergabekontrolle

Bei der Weitergabekontrolle wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports, ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Verantwortlich hierfür sind:

Susell GmbH
Unternehmenssitz: Joachimstrasse 7, 10119 Berlin

Getroffene Maßnahmen:

- Weitergabe in anonymisierter oder pseudonymisierter Form
- Vereinbarte Löschfristen
- Verschlüsselung von Datenträgern

3. Auftragskontrolle

Durch die Auftragskontrolle wird gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Verantwortlich hierfür sind:

Susell GmbH
Unternehmenssitz: Joachimstrasse 7, 10119 Berlin

Getroffene Maßnahmen:

- Auswahl aller Auftragnehmer unter Sorgfaltsgesichtspunkten
- vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- laufende Kontrolle aller Auftragnehmer

III. Verfügbarkeit und Belastbarkeit

Verfügbarkeit bedeutet, dass Daten zur Verfügung stehen, wenn sie gebraucht werden. Das Schutzziel »Belastbarkeit« wird nicht in der DSGVO legaldefiniert und hat auch keine Entsprechung im IT-Grundschutz. Nach gegenwärtiger Auffassung ist unter »Belastbarkeit« die Widerstandsfähigkeit von Systemen gemeint, wie sie im Bereich des Notfallmanagements eine Rolle spielt.
Diese Schutzziele werden durch die folgenden Maßnahmen sichergestellt:

1. Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind;

Verantwortlich hierfür sind:

Susell GmbH
Unternehmenssitz: Joachimstrasse 7, 10119 Berlin

Getroffene Maßnahmen:

- Backups

Die Susell GmbH speichert selbst keine Daten auf eigenen Servern in eigenen Räumlichkeiten, sondern hostet sämtliche Daten in der Cloud bei den in der Anlage gelisteten Subdienstleistern. Ergänzend und im Detail wird daher auf die jeweiligen Maßnahmen der einzelnen Unterauftragsnehmer verwiesen:

DigitalOcean, LLC. (Server & Hosting)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 101 Avenue of the Americas, New York, NY 10013 (USA)

Amazon Web Services Inc. (Datei-Speicher & E-Mail-Versand)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 410 Terry Avenue North, Seattle, Washington 98109-5210 (USA)

Streamdiver GmbH (Videoverarbeitung & -hosting)
Unternehmenssitz: Lakeside B06, 9020 Klagenfurt am Wörthersee (Österreich)

Rustici Software, LLC (SCORM-Verarbeitung & -hosting)
Unternehmenssitz: 210 Gothic Ct #100, Franklin, TN 37067 (USA)

FlowMate GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Harry-Blum-Platz 2, 50678 Cologne, Germany

Kombo Technologies GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Kottbusser Damm 25-26, 10967 Berlin, Germany

2. Belastbarkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden. Verantwortlich hierfür ist:

Verantwortlich hierfür sind:

Susell GmbH
Unternehmenssitz: Joachimstrasse 7, 10119 Berlin

Getroffene Maßnahmen:

- Regelmäßige Überwachung der Serverlast
- Stresstests

Die Susell GmbH speichert selbst keine Daten auf eigenen Servern in eigenen Räumlichkeiten, sondern hostet sämtliche Daten in der Cloud bei den in der Anlage gelisteten Subdienstleistern. Ergänzend und im Detail wird daher auf die jeweiligen Maßnahmen der einzelnen Unterauftragsnehmer verwiesen:

DigitalOcean, LLC. (Server & Hosting)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 101 Avenue of the Americas, New York, NY 10013 (USA)

Amazon Web Services Inc. (Datei-Speicher & E-Mail-Versand)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 410 Terry Avenue North, Seattle, Washington 98109-5210 (USA)

Streamdiver GmbH (Videoverarbeitung & -hosting)
Unternehmenssitz: Lakeside B06, 9020 Klagenfurt am Wörthersee (Österreich)

Rustici Software, LLC (SCORM-Verarbeitung & -hosting)
Unternehmenssitz: 210 Gothic Ct #100, Franklin, TN 37067 (USA)

FlowMate GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Harry-Blum-Platz 2, 50678 Cologne, Germany

Kombo Technologies GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Kottbusser Damm 25-26, 10967 Berlin, Germany

3. Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können. Verantwortlich hierfür ist:

Verantwortlich hierfür sind:

Susell GmbH
Unternehmenssitz: Joachimstrasse 7, 10119 Berlin

Getroffene Maßnahmen:

- Backups

Die Susell GmbH speichert selbst keine Daten auf eigenen Servern in eigenen Räumlichkeiten, sondern hostet sämtliche Daten in der Cloud bei den in der Anlage gelisteten Subdienstleistern. Ergänzend und im Detail wird daher auf die jeweiligen Maßnahmen der einzelnen Unterauftragsnehmer verwiesen:

DigitalOcean, LLC. (Server & Hosting)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 101 Avenue of the Americas, New York, NY 10013 (USA)

Amazon Web Services Inc. (Datei-Speicher & E-Mail-Versand)
Rechenzentrum: Frankfurt am Main (Deutschland)
Unternehmenssitz: 410 Terry Avenue North, Seattle, Washington 98109-5210 (USA)

Streamdiver GmbH (Videoverarbeitung & -hosting)
Unternehmenssitz: Lakeside B06, 9020 Klagenfurt am Wörthersee (Österreich)

Rustici Software, LLC (SCORM-Verarbeitung & -hosting)
Unternehmenssitz: 210 Gothic Ct #100, Franklin, TN 37067 (USA)

FlowMate GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Harry-Blum-Platz 2, 50678 Cologne, Germany

Kombo Technologies GmbH (Bereitstellung von Schnittstellen zu Drittanbieter Software)
Unternehmenssitz: Kottbusser Damm 25-26, 10967 Berlin, Germany

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Die getroffenen Maßnahmen müssen einer regelmäßigen Kontrolle unterzogen werden. Auch sind sie dem jeweils entsprechendem
Stand der Technik anzupassen und aktuell zu halten. Im Unternehmen wird ein solches regelmäßiges Kontroll- und Evaluierungskonzept wie folgt umgesetzt

- Auftragskontrolle der Dienstleister in regelmäßigen Intervallen
- Regelmäßige Mitarbeiterschulungen- und Prüfungen
- Regelmäßige Prüfung der technischen Komponenten und des Backup- und Recoverykonzepts
- Wartungsprotokolle technischer Komponente
- Regelmäßiges Einspielen von Patches und Softwareupdates