revent Work

Workflow Collaboration Software

| reventwork.com
| moin@reventwork.com
| 040 28483260

Revent GmbH
Sillemstraße 60A
20257 Hamburg

Vereinbarung zur Auftragsverarbeitung („AV“)

Vertragsnummer: AV_01_2021

Zwischen den
Anwendern der Webanwendung „Revent Work“
- im Folgenden Auftraggebern -

und der
Revent GmbH
Sillemstraße 60A
20257 Hamburg
- im Folgenden Auftragsverarbeiter –

- zusammen im Folgenden „die Parteien“ –

wird folgende Vereinbarung zur Auftragsdatenverarbeitung geschlossen.

1. Anwendungsbereich

Der Auftragsverarbeiter erhält im Zuge seiner Leistungserbringung Zugriff auf personenbezogene Daten, für die der Auftrageber datenschutzrechtlich verantwortlich ist. Grundlage für die Leistungserbringung und deren Durchführung ist der Revent Work Softwarenutzungsvertrag, im Folgenden „Hauptvertrag“. Diese AV konkretisiert die Rechte und Pflichten des Auftraggebers und des Auftragsverarbeiters bei der Durchführung des Hauptvertrags im Umgang mit Auftraggeberdaten.

2. Anwendungsbereich

Der Auftragsverarbeiter verarbeitet Auftraggeberdaten im Auftrag und nach Weisung des Auftraggebers im Sinne des Artikel 28 Abs. 1 DSGVO, im Folgenden „Auftragsverarbeitung“. Der Auftraggeber bleibt stets als „Herr der Daten“ der für die Rechtmäßigkeit der Verarbeitung der Auftraggeberdaten Verantwortliche. Artikel 28 Abs. 3 lit. a DSGVO bleibt davon unberührt.

Die Verarbeitung und Nutzung der Daten findet primär im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der EU oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum („sichere Staaten“) statt.

Der Auftragsverarbeiter darf die Auftraggeberdaten durch Stellen außerhalb der sicheren Staaten („Drittland“) nur verarbeiten oder verarbeiten lassen, wenn und im Falle dessen

(i) für das betreffende Drittland auf Grundlage einer gültigen Entscheidung der Europäischen Kommission ein angemessenes Datenschutzniveau festgestellt ist oder

| reventwork.com
| moin@reventwork.com
| 040 28483260

Revent GmbH
Sillemstraße 60A
20257 Hamburg

(ii) die Verarbeitung auf Grundlage und nach Maßgabe der jeweils gültigen EU- Standardvertragsklauseln („SCC“) erfolgt, welche dem Auftraggeber vorzulegen und mit der im Drittland ansässigen Stelle („Datenimporteur“) schriftlich zu vereinbaren sind. Sofern der Datenimporteur und der Auftragsverarbeiter nicht identisch sind, hat der Auftragsverarbeiter diesen SCC beizutreten. Die in dieser AV festgelegten Bestimmungen bleiben unberührt.

Der Auftragsverarbeiter darf die Auftragsverarbeitung ausschließlich nach Maßgabe und in dem Umfang der in Anhang 1 zu dieser AV festgelegten oder in Bezug genommenen Bestimmungen durchführen, insbesondere nur im Rahmen des dort festgelegten Zwecks.

Der Auftragsverarbeiter ist darüber hinaus angehalten, den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen der von der Auftragsverarbeitung betroffenen natürlichen Personen gemäß Kapitel III der DSGVO sowie bei der Einhaltung der in Artikel 33 bis 36 DSGVO genannten Pflichten im Rahmen seiner Möglichkeiten zu unterstützen. Sofern die Unterstützung des Auftragsverarbeiters ein angemessenes und zumutbares Maß übersteigt, kann der Auftragsverarbeiter gegenüber dem Auftraggeber eine Aufwandsentschädigung geltend machen. Als Grundlage für eine solche Aufwandsentschädigung gelten die im Hauptvertrag vereinbarten Tagessätze des Auftragsverarbeiters. Der Auftragsverarbeiter wird den Auftraggeber im Vorweg über etwaig anfallende Kosten in Kenntnis setzen.

Ferner ist der Auftragsverarbeiter verpflichtet, dem Auftraggeber auf Anfrage zeitnah die für die Erstellung bzw. die Pflege einer internen Verarbeitungsübersicht erforderlichen Angaben zu machen.

3. Datenschutzrechtliche Weisungen

Der Auftragsverarbeiter ist verpflichtet, den datenschutzrechtlichen Weisungen des Auftraggebers zur Verarbeitung von Auftraggeberdaten, insbesondere zur Speicherung, Löschung, Sperrung oder Berichtigung von Auftraggeberdaten uneingeschränkt zu folgen. Die datenschutzrechtlichen Weisungen werden anfänglich durch diese AV festgelegt und können jederzeit durch im Einzelfall erteilte Weisungen geändert, ergänzt oder ersetzt werden (im Folgenden „einzelfallbezogene Weisungen“ genannt). Einzelfallbezogene Weisungen haben mindestens in Textform (schriftlich oder per E- Mail) zu erfolgen. In begründeten Einzelfällen können einzelfallbezogene Weisungen auch mündlich erteilt werden, müssen dann aber vom Auftraggeber unverzüglich und mindestens in Textform bestätigt werden. Einzelfallbezogene Weisungen dürfen nur durch Personen erteilt werden, welche aufgrund ihrer organschaftlichen Stellung oder ihrer besonderen Funktion den Auftraggeber insoweit vertreten (z.B. Datenschutzbeauftragter, Chief Security Officer, Partner-Manager, etc.).

| reventwork.com
| moin@reventwork.com
| 040 28483260

Revent GmbH
Sillemstraße 60A
20257 Hamburg

Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen gesetzliche Vorschriften verstößt, denen der Auftragsverarbeiter unterliegt, ist der Auftragsverarbeiter unmittelbar verpflichtet, den Auftraggeber hierauf unverzüglich hinzuweisen, sowie berechtigt, die Ausführung der betreffenden Weisung bis zur Entscheidung durch den Auftraggeber auszusetzen. Die Entscheidung ist nachweisbar mindestens in Textform an den Auftragsverarbeiter zu übermitteln.

Der Auftragsverarbeiter hat zu jeder Zeit sicherzustellen, dass es den mit der Auftragsverarbeitung befassten Mitarbeitern und anderen für den Auftragsverarbeiter tätigen Personen untersagt ist, die Daten anders als nach in dieser Ziffer 3 dieser AV erteilten Weisungen zu verarbeiten.

4. Datenlöschung

Der Auftragsverarbeiter hat ihm überlassene und alle ergänzend zu verarbeiteten Auftraggeberdaten einschließlich sämtlicher Vervielfältigungen (auch in Archivierungs- und Sicherungsdateien) vollständig und unwiderruflich zu löschen oder zu vernichten (im Folgenden vereinheitlicht „Löschen“ genannt), sobald die Verarbeitung der Auftraggeberdaten nicht mehr für die Erfüllung des in Ziffer 2 dieser AV festgelegten Zwecks erforderlich ist. Auftraggeberdaten sind insbesondere nach Beendigung der vertragsgegenständlichen Leistungserbringung zu löschen, sofern nicht in Anhang 1 dieser AV speziellere Löschpflichten des Auftragsverarbeiters bestimmend sind.

Soweit Auftraggeberdaten nach Beendigung der vertragsgegenständlichen Leistungserbringung gesetzlichen Aufbewahrungs- und Speicherpflichten des Auftragsverarbeiters (etwa gemäß §§ 145 bis 147 AO, § 257 HGB) unterliegen, hat die Löschung der Auftraggeberdaten unverzüglich zum Ende des Aufbewahrungs- bzw. Speicherzeitraums zu erfolgen; Auftraggeberdaten sind während dieses Zeitraums von jeglicher Verarbeitung auszuschließen. Der Auftraggeber hat den Auftragsverarbeiter über das Vorliegen der zuvor genannten Aufbewahrungs- und Speicherfristen zu unterrichten.

5. Technische und Organisatorische Maßnahmen zur Daten- und Informationssicherheit

Der Auftragsverarbeiter garantiert vorbehaltlich einer einzelfallbezogenen Weisung die Einhaltung der in Anhang 2 dieser AV beigefügten technischen und organisatorischen Maßnahmen zur Daten- und Informationssicherheit, die der Auftraggeber unter Berücksichtigung der Auftragsverarbeitung im Allgemeinen und den im Rahmen dieser AV verarbeiten Auftraggeberdaten und der dabei verfolgten Verarbeitungszwecke im Speziellen als erforderlich erachtet. Ziel der Maßnahmen ist es, ein solches angemessenes Schutzniveau für Auftraggeberdaten zu gewährleisten, was dem Risiko für die Rechte und die Freiheit der von der Datenverarbeitung betroffenen natürlichen Personen entspricht (Art 32 DS-GVO).

| reventwork.com
| moin@reventwork.com
| 040 28483260

Revent GmbH
Sillemstraße 60A
20257 Hamburg

Der Auftragsverarbeiter darf Änderungen der technischen und organisatorischen Maßnahmen zur Daten- und Informationssicherheit vornehmen, sofern daraus keine negativen Änderungen für das Schutzniveau der Rechte und die Freiheit der von der Datenverarbeitung betroffenen natürlichen Personen resultieren. Über solche Änderungen ist der Auftraggeber rechtzeitig zu informieren. Dem Auftragsverarbeiter steht es frei, über die hier festgelegten oder in Bezug genommenen Bestimmungen hinaus weitergehende Maßnahmen zu treffen.

Der Auftragsverarbeiter hat ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Daten- und Informationssicherheit einzusetzen (Artikel 32 Abs. 1 lit. d DSGVO).

Der Auftragsverarbeiter hat darüber hinaus in seinem Verantwortungsbereich die innerbetriebliche Organisation und seine internen Abläufe so zu gestalten, dass sie den geltenden gesetzlichen Bestimmungen zum Datenschutz gerecht werden, insbesondere im Hinblick auf die Bestellung eines Datenschutzbeauftragten, der vorzunehmenden datenschutzrechtlichen Kontrollen und datenschutzrechtlichen Schulungen, Unterweisungen und Verpflichtungen sowie der Erstellung und Pflege einer Dokumentation der im Auftrag erfolgenden Datenverarbeitungen.

6. Besondere Vorkommnisse

Sobald dem Auftragsverarbeiter bzw. von ihm im Rahmen der Auftragsverarbeitung eingesetzten natürlichen oder juristischen Personen Anhaltspunkte für ein besonderes Vorkommnis bekannt werden, ist der Auftragsverarbeiter verpflichtet, den Auftraggeber unverzüglich ab dem Zeitpunkt des Bekanntwerdens über das besondere Vorkommnis, insbesondere über Zeitpunkt, Ursachen und Ausmaß, zu informieren, sämtliche erforderlichen und angemessenen Sofortmaßnahmen, z.B. das Trennen von Netzwerkverbindungen oder das forensische Sichern von Beweisen, einzuleiten, um entstandene oder unmittelbar drohende Gefährdungen für die Integrität und Vertraulichkeit der Auftraggeberdaten zu minimieren.

Als besondere Vorkommnisse gelten unter anderem

(i) der Verlust (mobiler) Medien- und/oder Datenträger, die Auftraggeberdaten enthalten (insbesondere Papier, USB-Speicher, CD-ROMs, Festplatten, Tablets, Smartphones oder Laptops, etc.);
(ii) sicherheitsrelevante Ereignisse auf Systemen, mittels derer Auftraggeberdaten erhoben oder verwendet werden (insbesondere Viren, Trojaner, Würmer oder Ausnutzen von Schwachstellen);
(iii) die öffentliche Zugänglichkeit von Auftraggeberdaten zum Abruf für Dritte (insbesondere über das Internet);
(iv) das Entwenden von Auftraggeberdaten (insbesondere durch Mitarbeiter, Dritte oder Unbefugte); sowie

| reventwork.com
| moin@reventwork.com
| 040 28483260

Revent GmbH
Sillemstraße 60A
20257 Hamburg

(v) die unbefugte Übermittlung an oder die anderweitige unbefugte Kenntnisnahme von Auftraggeberdaten an bzw. durch Dritte.

7. Beauftragung von Subunternehmern

Der Auftraggeber berechtigt den Auftragsverarbeiter, Subunternehmer in die Auftragsverarbeitung einzubeziehen. Einer gesonderten vorherigen Zustimmung durch den Auftraggeber bedarf es nicht. Der Auftragsverarbeiter garantiert, dass er dem beauftragten Subunternehmer dieselben Pflichten zum Datenschutz auferlegt, die zwischen den Parteien dieser AV gelten und dass dieser ebenfalls geeigneten technischen und organisatorischen Maßnahmen durchführt, um die Verarbeitung der Auftraggeberdaten gemäß der AV nachzukommen. Die vom Auftragsverarbeiter zum Zeitpunkt des Abschlusses dieser AV eingesetzten Subunternehmer sind in Anhang 1 aufgeführt. Der Auftragsverarbeiter informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Subunternehmers. Ein Subunternehmerverhältnis liegt vor, wenn der Auftragsverarbeiter weitere Auftragsverarbeiter mit hauptvertraglich vereinbarten (Teil-) Leistungen beauftragt und der Subunternehmer zum Zwecke der Erfüllung dieser Beauftragung Zugriff auf Auftraggeberdaten erhält. Auf Verlangen des Auftraggebers hat der Auftragsverarbeiter den Abschluss, der mit dem Subunternehmer geschlossenen Vereinbarungen gegenüber dem Auftraggeber nachzuweisen. Der Nachweis hat in Textform zu erfolgen. Erhebt der Auftraggeber gegen die beabsichtigte Änderung eines Subunternehmerverhältnisses Einspruch, so ist der Auftragsverarbeiter berechtigt, die AV sowie den Hauptvertrag außerordentlich zu kündigen.

Keine Subunternehmer sind Personen, welche mit dem Auftragsverarbeiter arbeitsvertraglich verbunden oder im Rahmen der Arbeitnehmerüberlassung entliehen sind, sofern diese nach Ziffer 5 dieser AV geschult und auf die Einhaltung der einschlägigen Datenschutzbestimmungen schriftlich verpflichtet sind.

8. Anfragen Dritter, Kontrollen durch Aufsichtsbehörden

Soweit der Auftragsverarbeiter Anfragen erhält, die den Inhalt der AV oder besondere Vorkommnisse betreffende, hat er es vorbehaltlich bestehender gesetzlicher und behördlicher Verpflichtungen zu unterlassen, entsprechende Auskünfte zu erteilen und ist verpflichtet, den Auftraggeber unverzüglich über die Anfrage zu informieren.

9. Kontroll- und Auskunftsrechte des Auftraggebers

Vor dem Beginn der AV und sodann jederzeit stellt der Auftragsverarbeiter sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragsverarbeiter dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gem. Kapitel 5 dieser AV nach (Artikel 32 DSGVO). Dabei kann der Nachweis

| reventwork.com
| moin@reventwork.com
| 040 28483260

Revent GmbH
Sillemstraße 60A
20257 Hamburg

der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage von aktuellen Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT- Sicherheit- oder Datenschutzaudit erbracht werden. Der Auftraggeber und von diesem beauftragte Dritte sind ab der Durchführung der AV berechtigt, nach schriftlicher Vorankündigung von dreißig (30) Kalendertagen die Geschäftsräume des Auftragsverarbeiters zu betreten, um sich von der Einhaltung sämtlicher oder einzelner in dieser AV festgelegter und in Bezug genommener Bestimmungen zu überzeugen. Der Auftragsverarbeiter gewährt dem Auftraggeber oder von diesem beauftragten Dritten – soweit diese im gleichen Maße Verschwiegenheits- und Vertraulichkeitsverpflichtungen eingehen, wie sie zwischen den Parteien der vorliegenden AV gelten – die erforderlichen Zutritts-, Zugangs-, Auskunfts- und Einsichtsrechte, ausschließlich bezogen auf solche Teile der Datenverarbeitung, die für den Auftraggeber relevant sind. Gleiches gilt für die für den Auftraggeber zuständige(n) Aufsichtsbehörde(n). Über einen solchen Kontrolltermin wird ein schriftliches Protokoll erstellt, welches den genauen Zeitpunkt, Umfang, Inhalt und die Dauer des Kontrolltermins beschreibt. Kommt es häufiger als einmal jährlich zu einem solchen Kontrolltermin, ist der Auftragsverarbeiter dazu berechtigt gegenüber dem Auftraggeber eine Kostenentschädigung für die auf seiner Seite im Zusammenhang mit dem Kontrolltermin entstandenen Aufwendungen geltend zu machen. Als Grundlage für eine solche Kostentschädigung gelten die im Hauptvertrag vereinbarten bzw. in der Branche üblichen Tagessätze des Auftragsverarbeiters. Der Auftragsverarbeiter wird den Auftraggeber im Vorweg über etwaig anfallende Kosten in Kenntnis setzen.

Der Auftraggeber ist berechtigt, das in 9.1 dieser AV festgelegte Kontroll- und Auskunftsrecht auch durch die Anforderung eines Selbstaudits („Self-Assessments“) auszuüben, d.h. durch das Einfordern einer Selbstauskunft des Auftragsverarbeiters, im Rahmen dessen der Auftragsverarbeiter wahrheitsgemäß und unverzüglich, d.h. im Regelfall innerhalb von dreißig (30) Werktagen, Auskunft über den Grad der Umsetzung der in dieser AV festgelegten oder in Bezug genommenen Bestimmungen, insbesondere der technischen und organisatorischen Maßnahmen zur Daten- und Informationssicherheit zu geben hat. Kommt es häufiger als einmal jährlich zu einem solchen Self-Assessment, gilt die Kostenreglung der Ziff. 9.1 dieser AV entsprechend.

Die Parteien können abweichend festlegen, dass der Auftragsverarbeiter die Einhaltung der in dieser AV festgelegten oder in Bezug genommenen Garantien und Verpflichtungen auch auf andere Weise, insbesondere durch die in Artikel 40 und Art. 42 DSGVO vorgesehenen Instrumentarien nachweisen kann (zusammenfassend „Compliance-Nachweise“).

| reventwork.com
| moin@reventwork.com
| 040 28483260

Revent GmbH
Sillemstraße 60A
20257 Hamburg

10. Haftung, Vertragsstrafe, Außerordentliche Kündigung

Die Parteien haften gem. Art. 82 DSGVO.

Im Innenverhältnis haftet der Auftragsverarbeiter nur für in seiner Sphäre liegendes Verschulden gegenüber dem Auftraggeber. Die Haftungsregelungen des Hauptvertrags bleiben im Innenverhältnis unberührt.

Diese Vereinbarung kann beidseitig aus wichtigem Grund gekündigt werden. Insbesondere dann, wenn nicht nur geringe Verstöße gegen die Bestimmungen dieser Vereinbarung vorliegen

11. Aufhebung bisheriger Regelungen zur Auftragsverarbeitung / Schlussbestimmungen

Sofern zwischen den Parteien bereits Vereinbarungen zur Datenverarbeitung im Auftrag bestehen, werden diese Vereinbarungen mit Wirksamkeit dieser AV aufgehoben und durch diese AV neu geregelt.

Die Parteien sind sich einig, dass diese AV mittels elektronischer Signatur unterzeichnet werden soll und alternativ in Schriftform abgefasst werden kann. Sie kann mittels elektronischer Signatur wirksam unterzeichnet werden, sodass die Parteien die jeweils von ihnen unterzeichneten Exemplare in elektronischer Form als PDF austauschen. Eine Unterzeichnung kann ebenfalls durch den digitalen Online-Registrierungsprozess des Auftragsverarbeiters erfolgen. Der Auftraggeber garantiert, dass die signierende oder den Online-Registrierungsprozess abschließende Person (Bevollmächtigter) über sämtliche zum Abschluss dieser AV erforderlichen Vollmachten und Vertretungsberechtigungen verfügt. Der Auftraggeber wird sich sämtliche Erklärungen des Bevollmächtigten zurechnen lassen. Änderungen dieser AV einschließlich ihrer Anhänge unterliegen ebenfalls den in dieser Ziffer geregelten Formerfordernissen.

Diese AV unterliegt deutschem Recht. Gerichtsstand für Streitigkeiten aus dieser AV entspricht der Regelung des Hauptvertrags.

Die in dieser AV festgelegten und in Bezug genommenen Vorschriften gelten vorrangig gegenüber anderen Regelungen, die die Erhebung und Verwendung von Auftraggeberdaten durch den Auftragsverarbeiter betreffen. Sollte eine Bestimmung dieser AV und /oder ihrer Änderungen beziehungsweise Ergänzungen unwirksam sein oder werden, so wird hierdurch die Gültigkeit der übrigen Bestimmungen im Vertrag nicht berührt. Die Parteien trifft bei Unwirksamkeit einer Bestimmung die Pflicht, über eine wirksame und zumutbare Ersatzregelung zu verhandeln, die dem von den Parteien mit der unwirksamen Bestimmung verfolgten wirtschaftlichen Zweck am nächsten kommt.

| reventwork.com
| moin@reventwork.com
| 040 28483260

Revent GmbH
Sillemstraße 60A
20257 Hamburg

Anhang 1

Dokumentation der Auftragsverarbeitung, Löschpflichten und des Datenaustauschs

Angaben zum Auftragsverarbeiter:

Name: Revent GmbH
Adresse: Sillemstraße 60A, 20257 Hamburg
Geschäftsführer: Tim Hübner, Stephan Scheele
Registergericht, Registernummer: Hamburg, 136520
Telefon: +49 40 28483260

1. Gegenstand, Art und Umfang der Verarbeitung von personenbezogenen Daten

Der Auftragsverarbeiter ist Hersteller und Anbieter von Unternehmenssoftware zur Aufnahme, Darstellung, Ausführung und Automatisierung von Geschäftsprozessen. Zum Leistungsangebot zählen neben vorvertraglichen Notwendigkeiten (Akqusie, Vertrieb) die Beratung, Implementierung, Integration, Hosting und Wartung der Software. Die Datenerhebung, -verarbeitung und -nutzung erfolgt zur Ausübung all dieser oben angegebenen Zwecke.

2. Kreis der Betroffenen und Art der Daten

Zu folgenden Personengruppen werden personenbezogene Daten erhoben, verarbeitet und genutzt, sofern diese zur Erfüllung des genannten Zweckes erforderlich sind:

Interne und externe Mitarbeiter des Auftraggebers

- Berufliche Kontaktdaten, Organisationsdaten zur Userverwaltung: Name, Vorname, Geschlecht, E-Mail-Adresse, Telefonnummer, Foto
- Daten zu beruflichen Verhältnissen und Arbeitsabläufen: Berufsbezeichnung, Prozessrolle, Organisationszugehörigkeit, Log-File Informationen, Arbeitszeit, Abwesenheitszeit, Tätigkeit, User-generated Content (z.B. Kommentare, Nachrichten)

Geschäftskunden, Lieferanten und sonstige Geschäftspartner des Auftraggebers

- (Berufliche) Kontaktdaten, Organisationsdaten zur Userverwaltung: Name, Vorname, Geschlecht, E-Mail-Adresse, Telefonnummer, Foto
- Daten zu beruflichen Verhältnissen und Arbeitsabläufen: Berufsbezeichnung, Prozessrolle, Organisationszugehörigkeit, Log-File Informationen, Tätigkeit, User-generated Content (z.B. Kommentare, Nachrichten)
- Arbeitsablauf-spezifische Daten mit eindeutiger Zweckbindung (z.B. Lieferadresse)

Endkunden / Privatkunden des Auftraggebers

- Kontaktdaten, Organisationsdaten zur Userverwaltung: Name, Vorname, E-Mail-Adresse, Telefonnummer
- Daten zu Arbeitsabläufen: Log-File Informationen, User-generated Content (z.B. Kommentare, Nachrichten)
- Arbeitsablauf-spezifische Daten mit eindeutiger Zweckbindung (z.B. Lieferadresse)

3. Art der Leistung und Zweck der Datenverarbeitung

Die Verarbeitung personenbezogener Daten erfolgt zum Zweck der Bereitstellung der Software Anwendung Revent Work, mit deren Hilfe die Abbildung und Ausführung von Geschäftsprozessen des Auftraggebers erfolgt. Das bedeutet insbesondere

- Hosting (Daten, Applikation, System, Komponenten)
- Betrieb (Applikation, System, Komponenten)
- Wartung/Pflege (Applikation, System, Komponenten)
- Support (Applikation, System, Komponenten)
- Weiterentwicklung (Applikation, System, Komponenten)

4. Datenschutzbeauftragter

Datenschutzbeauftragter des Auftragnehmers ist:

ePrivacy GmbH
vertreten durch Prof. Dr. Christoph Bauer
Große Bleichen 21, 20354 Hamburg

Zu allen Fragen und Anliegen bezüglich Ihrer Daten, wenden Sie sich gerne an privacy@reventwork.com.

Sollten Sie direkt mit unserem Datenschutzbeauftragten kommunizieren wollen (bspw. weil Sie ein besonders sensibles Anliegen haben), kontaktieren Sie diesen bitte auf dem Postweg, da die Kommunikation per E-Mail immer Sicherheitslücken aufweisen kann.

Bitte geben Sie bei der Anfrage an, dass sich ihr Anliegen auf die Firma REVENT GmbH bezieht.

5. Subunternehmer

Der Auftragsverarbeiter setzt die nachfolgenden Subunternehmer als weitere Auftragsverarbeiter bei Abschluss dieses Vertrags ein:

Microsoft Ireland Operations Ltd, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland
Zum Betrieb der Anwendung und zur primären Datenverarbeitung werden Teile der Software in Rechenzentren der Microsoft Corporation (Azure) gehostet und Anwendungsdaten in persistenten Datenbanken

| reventwork.com
| moin@reventwork.com
| 040 28483260

Revent GmbH
Sillemstraße 60A
20257 Hamburg

gespeichert. Das komplette Hosting der Anwendung erfolgt in europäischen Rechenzentren. Es kann nicht ausgeschlossen werden, dass Microsoft Daten an das Mutterunternehmen, die Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, mit Sitz in den USA, weiterleitet. Im Fall eines Datenexports hat sich Microsoft jedoch dazu verpflichtet, die Standards und Vorschriften der Datenschutzgrundverordnung einzuhalten, indem die europäischen Standard-Vertragsklauseln respektiert werden, welche als geeignete Garantie für eine Übermittlung von Daten in ein Drittland fungieren können.

- Vertragsgrundlage: Data Processing Agreement
- Garantien: EU Standard Vertragsklauseln

ADN Advanced Network Digital Distribution GmbH, Josef-Haumann-Straße 10, 44866 Bochum, Deutschland
Die ADN fungiert als Zwischenhändler zum Bezug von Microsoft Office und Azure Lizenzpaketen. Für den Fall einer Funktionsstörung auf Seiten Microsofts ist ADN unser primärer Supportkontakt zur Fehlerbehebung.

- Vertragsgrundlage: Auftragsverarbeitungsvertrag

Twilio Limited, 25-28 Wall Quay, North Wall, Dublin 1, Ireland
Die Firma Twilio wird eingesetzt, um innerhalb der Anwendung Video-Telefonie, SMS- und E-Mail-Versand zu ermöglichen. Hierfür wird die E-Mail-Adresse bzw. die Handynummer an Twilio weitergegeben. Es kann nicht ausgeschlossen werden, dass Twilio Daten auch an sein Mutterunternehmen, die Twilio Inc. mit Sitz in den USA, weiterleitet. Im Fall eines Datenexports hat sich Twilio jedoch dazu verpflichtet, die Standards und Vorschriften der Datenschutzgrundverordnung zu respektieren, indem sie zusätzlich zu den europäischen Standard-Vertragsklauseln sog. Binding Corporate Rules abgeschlossen haben, welche als geeignete, zusätzliche Garantie für eine Übermittlung von Daten in ein Drittland fungieren können. Der E-Mail-Dienst wird von der Firma SendGrid (ein Produkt von Twilio mit Sitz in 1801 California Street, Suite 500, Denver, Colorado 80202, USA) zur Verfügung gestellt. Vertragspartner im Sinne dieser AV ist jedoch Twilio. Auch hier kann ein Datenexport nicht ausgeschlossen werden. Im Fall eines Datenexports von Daten im Zuge des E-Mail-Dienstes hat sich SendGrid bzw. Twilio ebenfalls dazu verpflichtet, die Standards und Vorschriften der Datenschutzgrundverordnung einzuhalten, indem die europäischen Standard-Vertragsklauseln respektiert werden, welche als geeignete Garantie für eine Übermittlung von Daten in ein Drittland fungieren können. Twilio weist drauf hin, dass die Binding Corporate Rules hier keine Anwendung finden, da zusätzliche Tracking-Mechanismen (bspw. Web-Beacons) in die E-Mails eingebaut werden, um die Funktionalität des Dienstes sicherstellen zu können. (bspw. die Zustellung zu überprüfen). Dennoch wir ein hohes Datenschutzniveau zugesagt.

- Vertragsgrundlage: Data Processing Agreement
- Garantien: EU Standard Vertragsklauseln

Whereby AS, Gate 1 no. 107, 6700 Måløy, Norway
Whereby Embedded wird eingesetzt, um innerhalb der Anwendung Video-Telefonate zu ermöglichen.

- Vertragsgrundlage: Data Processing Agreement
- Garantien: EU Standard Vertragsklauseln

6. Spezifische Löschpflichten

Der Auftragsverarbeiter hat ihm überlassene und alle ergänzend verarbeiteten Daten einschließlich sämtlicher Vervielfältigungen (auch in Archivierungs- und Sicherungsdateien) vollständig und unwiderruflich nach 30 Tagen zu löschen oder zu vernichten (im Folgenden einheitlich „löschen“ genannt), in welchem die Verarbeitung der Daten nicht mehr für die Erfüllung des Zwecks der Verarbeitung (Auftragszweck) erforderlich ist. Die Backups von Datenbanken werden bis zu 30 Tage lang vorgehalten. Daher ist es technisch nicht möglich eine frühere Löschung zu garantieren.

Personenbezogene Daten sind insbesondere nach Beendigung der vertragsgegenständlichen Leistungserbringung zu löschen, sofern hier nicht speziellere Löschpflichten des Auftragsverarbeiters bestimmt sind.

Soweit personenbezogene Daten gesetzlichen Aufbewahrungs- und Speicherpflichten des Auftragsverarbeiters (etwa gemäß §§ 145 bis 147 AO, § 257 HGB) unterliegen, hat die Löschung der Daten unverzüglich zum Ende des Aufbewahrungs- bzw. Speicherzeitraums zu erfolgen; personenbezogene Daten sind während dieses Zeitraums zu sperren.

7. Repräsentant in Frage des Datenschutzes (intern)

Beim Auftragsverarbeiter in der zuständigen Funktion für Datenschutz und Empfänger für Weisungen:

Tim Hübner, Geschäftsführer / CTO
Kommunikationskanal: privacy@reventwork.com

Vertretung:
Stephan Scheele, Geschäftsführer

| reventwork.com
| moin@reventwork.com
| 040 28483260

Revent GmbH
Sillemstraße 60A
20257 Hamburg

Anhang 2

Technische und organisatorische Maßnahmen zur Daten- und Informationssicherheit

1. Vertraulichkeit der Daten

1.1. Zutrittskontrolle

Zutritt zu den Räumlichkeiten des Auftragsverarbeiters, die zur Durchführung des Auftrags verwendet werden, ist auf die zur Durchführung des Auftrags erforderlichen Personen beschränkt.

Die Eingänge zu den Räumlichkeiten des Auftragsverarbeiters, in denen personenbezogene Daten verarbeitet werden, sind mit Schließzylindern gegen Zutritt Unbefugter gesichert.

Türen, Tore und Fenster der Räumlichkeiten des Auftragsverarbeiters, in denen personenbezogene Daten verarbeitet werden, sind außerhalb der Betriebszeiten fest verschlossen; Türen, Tore und Fenster in Keller und Erdgeschoss sowie alle weiteren leicht zu erreichenden Zugänge zu diesen Räumen sind derart ausgeführt, dass diese Unbefugten nur erheblich erschwert zugänglich sind, etwa durch einbruchhemmende Türen, Tore, Fenster und Schlösser und/oder den Einsatz einer Einbruchmeldeanlage.

Zur Durchführung des Auftrags vom Auftragsverarbeiter verwendete Server sind in einem separat abgesicherten Serverraum oder Rechenzentrum untergebracht, welche durch eine Zutrittskontrollanlage gegen den Zutritt Unbefugter gesondert gesichert sind. Diese Räume sind einbruchhemmend geschützt und mindestens gemäß den Vorgaben der Sicherungsklasse SG1 nach VdS 2333 ausgeführt. Der Zutritt zu diesen Räumlichkeiten ist auf das zur Wartung und Instandsetzung sowie auf die im Übrigen konkret erforderlichen Rollen und Personen beschränkt.

1.2. Zugangskontrolle

Die zur Durchführung des Auftrags vom Auftragsverarbeiter eingesetzten informationsverarbeitenden Systeme (Client- und Serversysteme) sind durch Authentifikations- und Autorisationssysteme geschützt.
Identifikations- und Authentifikationsinformationen (insbesondere in Form von Benutzernamen und Passwörtern), welche mit der Zugangsberechtigung zu den zur Durchführung des Auftrags eingesetzten informationsverarbeitenden Systemen verbunden sind, werden nur an die mit der Durchführung des Auftrags beauftragten Personen und lediglich in dem für die jeweilige Aufgabe erforderlichen Umfang vergeben.

Jede Vergabe von Zugangsberechtigungen wird für die Laufzeit des Auftrags dokumentiert.

| reventwork.com
| moin@reventwork.com
| 040 28483260

Revent GmbH
Sillemstraße 60A
20257 Hamburg

Alle Zugänge und Kennungen („Accounts“) werden ausschließlich personenspezifisch vergeben. Die Benutzung von Accounts durch mehrere Personen (Gruppen-Accounts) unterbleibt grundsätzlich.

Identifikations- und Authentifikationsinformationen werden ausschließlich persönlich verwendet. Ein in solchen Informationen enthaltenes Passwort wird als Initialpasswort vergeben und wird unverzüglich nach dem Erhalt durch die berechtigte Person auf ein nur der berechtigten Person bekanntes Passwort umgesetzt; jegliche Weitergabe unterbleibt. Wenn möglich, wird eine 2-Faktor-Authenfizierung implementiert. Sofern Unbefugte Kenntnis von Zugangsdaten erhalten, zeigt der Auftragsverarbeiter dies unverzüglich an.

Die Wahl der Passwörter erfolgt in ausreichender Komplexität und Güte.

Der Auftragsverarbeiter hält Authentifikationsdaten (insbesondere Passwörter und kryptographische Schlüssel) gegenüber Unbefugten streng geheim, bewahrt diese nicht im Klartext auf und verwendet diese ausschließlich unter Einsatz einer Ziffer 8 dieses Anhangs 2 entsprechenden Verschlüsselung oder als unumkehrbare kryptographische Prüfsumme (insbesondere bei der Speicherung und der Übertragung im Netzwerk).

1.3. Zugriffskontrolle

Sofern personenbezogene Daten zur Durchführung des Auftrags auf informationsverarbeitenden Systemen des Auftragsverarbeiters gespeichert sind, ist für sämtliche Zugriffe auf personenbezogene Daten ein abgestuftes und geeignet granulares Rechtesystem eingerichtet und technisch implementiert. Dadurch ist sichergestellt, dass die Zugriffsrechte so gestaltet sind, dass sie nur den für die Leistungserbringung eingesetzten Mitarbeiter jeweils für die Erfüllung der konkreten Aufgaben im notwendigen Umfang Zugriff auf die personenbezogenen Daten erlauben. Dabei ist die Vergabe von Administratorenrechte auf das zwingend erforderliche Maß an Mitarbeitern des Auftragsverarbeiters begrenzt.

Alle verarbeiteten Daten werden verschlüsselt übertragen. Alle personenbezogenen Daten werden verschlüsselt in unseren Datenbanksystemen abgelegt. Jeder Zugriff erfolgt ebenfalls über verschlüsselte Datenkanäle.

Sofern personenbezogene Daten auf informationsverarbeitenden Systemen des Auftragsverarbeiters gespeichert sind, werden sämtliche Zugriffe auf personenbezogene Daten (einschließlich des lesenden, verändernden und löschenden Zugriffs) nach Benutzer, Datum, Uhrzeit und den jeweils betroffenen Daten protokolliert.

1.4. Eingabekontrolle

Die Eingabe, Änderung und Löschung von Daten in den verwendeten Server-Systemen wird automatisiert protokolliert. Die Eingabe,

| reventwork.com
| moin@reventwork.com
| 040 28483260

Revent GmbH
Sillemstraße 60A
20257 Hamburg

Änderung und Löschung von Daten in den verwendeten Server-Systemen ist durch das Verwenden individueller Benutzernamen nachvollziehbar. Die Vergabe von Rechten zu Eingabe, Änderung und Löschung von Daten in den verwendeten Server-Systemen erfolgt auf Basis eines Berechtigungskonzepts. Dateien und Dokumente werden in Dokumentenmanagement-Systemen gespeichert, die Eingaben und Änderungen automatisch mit Datum und Benutzerkennung protokollieren. Vor der Installation neuer Programme und Updates auf den verwendeten Serversystemen wird deren Integrität durch Funktionstests sichergestellt.

2. Integrität

2.1. Weitergabekontrolle

Personenbezogene Daten können nicht unbefugt kopiert (insbesondere auf externe Datenträger gespeichert), weitergegeben und/oder gelöscht werden. Datenträger, sowie sämtliche Dokumente, sofern sie personenbezogene Daten enthalten (einschließlich sämtlicher gegebenenfalls vorhandener Sicherungskopien von personenbezogenen Daten und Kopien von Originaldokumenten) werden in ordnungsgemäß verschlossenen Datensicherungsschränken verwahrt, wenn und solange sie nicht in der Bearbeitung sind.

Originaldokumente, die personenbezogene Daten enthalten, werden durch die den Prozess verantwortlich leitenden Personen an die zur Leistungserbringung eingesetzten Personen herauszugeben und von diesen nach Arbeitsschluss wieder entgegengenommen.

Den bei der Durchführung des Auftrags beschäftigten Personen ist die Anfertigung von handschriftlichen Aufzeichnungen nur in dem zur Leistungserbringung erforderlichen Umfang und auf besonders gekennzeichneten Arbeitsmitteln (z.B. paginiertes oder farbiges Papier) gestattet.

Herausgegebene Originaldokumente oder erstellte handschriftliche Aufzeichnungen werden, auch bei auch nur kurzzeitigem Verlassen des Arbeitsplatzes, vor unberechtigtem Zugriff geschützt (“Clean Desk Policy“).

Die den bei der Durchführung des Auftrags beim Auftragsverarbeiter beschäftigten Personen nutzen ausreichend gesicherte Client-Systeme. Alle Client-Systeme sind mit Firewall und Virenschutz versehen und werden regelmäßig auf gängige Sicherheitsstandards überprüft.

Auf Durchführung des Auftrags vom Auftragsverarbeiter verwendeten Server- Systemen mit nicht-flüchtigem Speicher, z.B. Netzwerkdrucker oder Scanner, werden personenbezogene Daten nicht über den unmittelbar zur Vertragsdurchführung erforderlichen Umfang hinaus gespeichert.

| reventwork.com
| moin@reventwork.com
| 040 28483260

Revent GmbH
Sillemstraße 60A
20257 Hamburg

2.2. Trennungsgebot

Sofern personenbezogene Daten auf informationsverarbeitenden Systemen des Auftragsverarbeiters gespeichert sind, wird eine vollständige Trennung der personenbezogene Daten von personenbezogenen Daten anderer Auftraggeber realisiert und dadurch die jederzeitige und vollständige Identifizier- und Löschbarkeit von personenbezogenen Daten sichergestellt, z.B. durch Speicherung der personenbezogene Daten in einem eigenen Mandanten, in einer eigenen Partition oder durch eindeutige Identifier getrennt abrufbar. Eine entsprechende Trennung wird auch für personenbezogene Daten selbst realisiert, wenn sie zu verschiedenen Zwecken gespeichert werden.

3. Verfügbarkeitskontrolle

Vom Auftragsverarbeiter zur Durchführung des Auftrags verwendete Server-Systeme werden durch Firewalls geschützt, welche diese Server-Systeme gegen nicht betriebsnotwendige Zugriffe sichern.

Sämtliche gegebenenfalls vom Auftragsverarbeiter zur Durchführung des Auftrags verwendete Software wird aktualisiert gehalten und sicherheitsrelevante Aktualisierungen (insbesondere Updates, Patches, Fixes) werden unverzüglich eingespielt, nachdem diese vom Hersteller der Software allgemein verfügbar gemacht und vom Auftragsverarbeiter im Rahmen eines dem Stand der Technik entsprechenden Verfahren getestet werden.

Originaldokumente, die personenbezogene Daten enthalten, sowie beim Auftragsverarbeiter rechtmäßig auf informationsverarbeitenden Systemen gespeicherte personenbezogene Daten werden durch technische und organisatorische Maßnahmen vor Verlust durch zufällige, fahrlässige oder vorsätzliche Löschung oder Veränderung geschützt.

Sicherungskopien von beim Auftragsverarbeiter rechtmäßig auf informationsverarbeitenden Systemen gespeicherten personenbezogene Daten werden nach denselben Maßgaben wie Originaldaten behandelt, insbesondere gegen unbefugten Zugriff gesichert.

4. Auftragskontrolle

Über die allgemeinen Grundsätze sowie über die sich aus dieser AV ergebenden spezifischen Anforderungen des Datenschutzes, einschließlich der Datensicherheit, werden die beim Auftragsverarbeiter zur Durchführung des Auftrags beschäftigten Personen vor dem Einsatz beim Auftragsverarbeiter zur Durchführung des Auftrags und sodann regelmäßig geschult.

Am Ende und auf Grundlage des festgelegten Schulungsprozesses werden die beim Auftragsverarbeiter zur Durchführung des Auftrags beschäftigten Personen auf die Vertraulichkeit und den Schutz personenbezogener Daten verpflichtet. Diese Verpflichtung erstreckt sich auf das Fernmeldegeheimnis und die damit verbundenen Grundsätze und

Anforderungen an die Vertraulichkeit der Telekommunikation, wenn dies nach Maßgabe des konkreten Auftrags erforderlich ist, insbesondere wenn der Auftrag den Zugriff auf Verkehrsdaten umfasst.

5. Datenschutzfreundliche Voreinstellung, privacy-by-default

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

6. Löschung

Besteht nach Maßgabe des Auftrags für den Auftragsverarbeiter eine Pflicht zur Löschung von personenbezogenen Daten, wird der Auftragsverarbeiter

(i) die datenschutzgerechte nicht wieder herstellbare Löschung sämtlicher, personenbezogene Daten enthaltender, löschbaren elektronischen Datenträger (insbesondere Festplatten, USB-Sticks, Disketten, Bänder) durchführen;
(ii) die nachhaltige und irreversible Entfernung von personenbezogenen Daten aus Datenbank- oder File-Systemen sowie aus allen anderen löschbaren Speichermedien realisieren; und
(iii) sämtliche, personenbezogene Daten enthaltende Papierdokumente und sonstige nicht-gemäß Buchstabe (i) oder (ii) löschbaren Datenträger (einschließlich sämtlicher personenbezogene Daten enthaltener Fehldrucke, Speicherkarten, USB-Sticks, etc.) mit einem handelsüblichen Dokumentenvernichter der Sicherheitsstufe 3 gemäß DIN-Norm 32757 oder einem mindestens gleichwertigen Verfahren vernichten, wobei defekte magnetische Datenträger, die nicht wie oben angegeben mechanisch vernichtet werden können (z.B. defekte Festplatten), sind mittels eines zugelassenen Löschgerätes nach DIN 33858 gelöscht werden.

Die Löschung wird für die Dauer der Laufzeit des Auftrags protokolliert.

7. Regelmäßige Überprüfung

Die in diesem Anhang 2 aufgeführten Maßnahmen werden mindestens einmal jährlich durch die Geschäftsführung und die IT-Leitung in Zusammenarbeit mit dem Datenschutzbeauftragten überprüft. Für den Fall, dass bei der Überprüfung herauskommt, dass sich technologische Standards oder organisatorische Prozesse geändert haben und solche Änderungen eine Anpassung der hier aufgelisteten Maßnahmen erforderlich machen, werden die dadurch erforderlich werdenden Anpassung unverzüglich umgesetzt. Dabei wird der Grundsatz der Angemessenheit beachtet. Änderungen werden zudem auf ad hoc Basis durchgeführt, sofern dies aus Gründen der Sicherheit erforderlich ist. Die Überprüfung sowie daraus resultierende Änderungen werden dokumentiert und abgelegt.

revent Work

Workflow Collaboration Software

| reventwork.com
| moin@reventwork.com
| 040 28483260

Revent GmbH
Sillemstraße 60A
20257 Hamburg

_____, den _____

Ort, Datum

_____

Revent GmbH
Geschäftsführung

_____, den _____

Ort, Datum

_____

Auftraggeber