Vereinbarung zur Auftragsverarbeitung („AV“)

zwischen

nachfolgend „**Auftraggeber“**

und

HQLabs GmbH
Colonnaden 41
20354 Hamburg

nachfolgend **„Auftragsverarbeiter“**

Auftraggeber und **Auftragsverarbeiter**
zusammenfassend „die **Parteien**“

1. Anwendungsbereich

Im Rahmen der Erbringung der zwischen den Parteien bestehenden vertraglichen Leistungsbeziehungen aus dem HQ Softwarenutzungsvertrag (nachfolgend zusammenfassend „Hauptvertrag“ genannt) erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten, für welche der Auftraggeber bzw. die auf Grund des Hauptvertrages ggf. anderweitig abrufberechtigten Gesellschaft(en) datenschutzrechtlich verantwortlich sind (nachfolgend „Auftraggeberdaten“ genannt). Diese AV konkretisiert die Rechte und Pflichten des Auftraggebers und des Auftragsverarbeiters bei der Durchführung des Hauptvertrages im Hinblick auf den Umgang mit Auftraggeberdaten.

2. Auftragsverarbeitung

2. 1. Der Auftragsverarbeiter verarbeitet Auftraggeberdaten im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 28 Abs. 1 DS-GVO (nachfolgend „Auftragsverarbeitung“ genannt). Der Auftraggeber bleibt als „Herr der Daten“ der für die Rechtmäßigkeit der Verarbeitung der Auftraggeberdaten Verantwortliche. Art. 28 Abs. 3 lit. a DS-GVO bleibt unberührt.

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

2. 3. Der Auftragsverarbeiter darf Auftraggeberdaten durch Stellen außerhalb der Sicheren Staaten („Drittland“) nur verarbeiten oder verarbeiten lassen, wenn und soweit (i) für das betreffende Drittland auf Grundlage einer gültigen Entscheidung der Europäischen Kommission ein angemessenes Datenschutzniveau festgestellt ist oder (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.

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

2. 5. Der Auftragsverarbeiter hat dem Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen der von der Auftragsverarbeitung betroffenen natürlichen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten im Rahmen seiner Möglichkeiten zu unterstützen. Sofern die Unterstützungsleistungen des Auftragsverarbeiters über ein für diesen zumutbares und angemessenes Maß hinausgehen, kann der Auftragsverarbeiter gegenüber dem Auftraggeber eine Kostenentschädigung geltend machen. Als Grundlage für eine solche Kostentschädigung gelten die im Hauptvertrag vereinbarten Tagessätze des Auftragsverarbeiters. Der Auftragsverarbeiter wird den Auftraggeber im Vorwege über nach dieser Klausel anfallende Kosten in Kenntnis setzen.

2. 6. Der Auftragsverarbeiter ist verpflichtet, dem Auftraggeber auf Anfrage zeitnah die gegebenenfalls für die Erstellung bzw. die Pflege einer internen Verarbeitungsübersicht erforderlichen Angaben zu machen. Ziff. 2.5 letzter Satz der AV gilt entsprechend.

3. Datenschutzrechtliche Weisungen

3. 1. 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 (nachfolgend „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. Ziffer 3.3 dieser AV bleibt unberührt.

3. 2. 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.).

3. 3. Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung im Sinne von Ziffer 3.1 dieser AV gegen gesetzliche Vorschriften verstößt, denen der Auftragsverarbeiter unterliegt, ist der Auftragsverarbeiter 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. Für die Bestätigung der Weisung gelten die Sätze 3 und 4 der Ziffer 3.1 sowie Ziffer 3.2 sowie 3.3. dieser AV entsprechend.

3. 4. Der Auftragsverarbeiter hat sicherzustellen, dass es den mit der Auftragsverarbeitung befassten Mitarbeitern und anderen für den Auftragsverarbeiter tätigen Personen untersagt ist, die Daten außerhalb der Maßgabe von Ziffer 3.1 dieser AV erteilten Weisungen zu verarbeiten.

4. Datenlöschung

4. 1. Der Auftragsverarbeiter hat ihm überlassene und alle ergänzend verarbeiteten Auftraggeberdaten einschließlich sämtlicher Vervielfältigungen (auch in Archivierungs- und Sicherungsdateien) vollständig und unwiderruflich zu löschen oder zu vernichten (nachfolgend einheitlich „Löschen“ genannt), sobald die Verarbeitung der Auftraggeberdaten nicht mehr für die Erfüllung des in Ziffer 2.4 dieser AV festgelegten Zwecks erforderlich ist. Auftraggeberdaten sind insbesondere nach Beendigung der vertragsgegenständlichen Leistungserbringung wie im Hauptvertrag beschrieben zu löschen, sofern nicht in Anhang 1 dieser AV speziellere Löschpflichten des Auftragsverarbeiters bestimmt 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 Auftragsverarbeiter ist berechtigt die Auftraggeberdaten für einen Zeitraum vom 35 Tagen nach Ablauf der Speicherfristen auf einem Backupspeichermedium zu speichern und anschließend sofort zu löschen. 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

5. 1. Der Auftragsverarbeiter garantiert vorbehaltlich einer einzelfallbezogenen Weisung die Umsetzung der als Anhang 2 dieser AV beigefügten technischen und organisatorischen Maßnahmen zur Daten- und Informationssicherheit, welche der Auftraggeber unter Berücksichtigung der mit der Auftragsverarbeitung im Allgemeinen und den im Rahmen dieser AV verarbeiten Auftraggeberdaten und der dabei verfolgten Verarbeitungszwecke als erforderlich ansieht, um ein dem Risiko für die Rechte und die Freiheit der von der Datenverarbeitung betroffenen natürlichen Personen entsprechendes Schutzniveau für Auftraggeberdaten zu gewährleisten (Art 32 DS-GVO). Der Auftragsverarbeiter darf Änderungen der in Satz 1 in Bezug genommenen 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 in dieser Ziffer 5.1 festgelegten oder in Bezug genommenen Bestimmungen hinaus weitergehende Maßnahmen zu treffen.

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

5. 3. Der Auftragsverarbeiter hat im Übrigen in seinem Verantwortungsbereich die innerbetriebliche Organisation sowie seine internen Abläufe so zu gestalten, dass sie den für den Auftragsverarbeiter unmittelbar 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.

5. 4. Personenbezogene und sonstige Daten oder Informationen, die dem Auftragnehmer im Rahmen der Erfüllung dieses Vertrags bekannt werden, darf der Auftragnehmer nur für Zwecke der beauftragten Leistung verwenden. Der Auftragnehmer verpflichtet sich, die Vertraulichkeit und Integrität der personenbezogenen Daten zu wahren und alle ihm im Zusammenhang mit der Übernahme und Abwicklung des Auftrages bekannt werdenden personenbezogenen Daten und

sonstige unternehmensinterne Umstände, Daten und Informationen (Betriebsgeheimnisse) vertraulich zu behandeln sowie die im Rahmen des Vertrages tätig werdenden Mitarbeiter auch über die Beendigung des Beschäftigungsverhältnisses hinaus auf die Wahrung der Vertraulichkeit schriftlich zu verpflichten und über die Datenschutzpflichten aus diesem Vertrag, die Weisungsgebundenheit der Verarbeitung der Daten und deren Zweckbindung zu belehren. Diese Geheimhaltungspflicht gilt auch über die Beendigung des Vertragsverhältnisses hinaus.

6. Besondere Vorkommnisse

6. 1. 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 auszuschließen.

6. 2. Als Besondere Vorkommnisse im Sinne der Ziffer 6.1 gelten u.a. insbesondere

(a) der Verlust (mobiler) Medien- und/oder Datenträger, die Auftraggeberdaten enthalten (insbesondere Papier, USB-Speicher, CD-ROMs, Festplatten, Tablets, Smartphones oder Laptops, etc.);

(b) sicherheitsrelevante Ereignisse auf Systemen, mittels derer Auftraggeberdaten erhoben oder verwendet werden (insbesondere Viren, Trojaner, Würmer oder Ausnutzen von Schwachstellen);

(c) die öffentliche Zugänglichkeit von Auftraggeberdaten zum Abruf für Dritte (insbesondere über das Internet);

(d) das Entwenden von Auftraggeberdaten (insbesondere durch Mitarbeiter, Dritte oder Unbefugte); sowie

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

7. Beauftragung von Subunternehmern

7. 1. 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 von ihm jeweils beauftragten Subunternehmer dieselben Datenschutzpflichten auferlegt, die zwischen den Parteien der AV gelten und dass dieser die geeigneten technischen und organisatorischen Maßnahmen durchführt, um die Verarbeitung der Auftraggeberdaten gemäß der AV sicherzustellen. Die vom Auftragsverarbeiter zum Zeitpunkt des Abschlusses dieser AV eingesetzten Subunternehmer sind im 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.

7. 2. Keine Subunternehmer im Sinne der Ziffer 7.1 sind Personen, welche mit dem Auftragsverarbeiter arbeitsvertraglich verbunden oder im Rahmen der Arbeitnehmerüberlassung entliehen sind, sofern diese nach Ziffer 5.3 dieser AV geschult und auf die Einhaltung der einschlägigen Datenschutzbestimmungen schriftlich verpflichtet sind.

8. Anfragen Dritter, Kontrollen durch Aufsichtsbehörden

8. 1. Soweit der Auftragsverarbeiter den Inhalt der AV oder besondere Vorkommnisse betreffende Anfragen erhält, 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.

8. 2. Ziffer 8.1 dieser AV gilt entsprechend, soweit Aufsichtsbehörden beim Auftragsverarbeiter Kontrollen ankündigen oder unangekündigt durchführen.

9. Kontroll- und Auskunftsrechte des Auftraggebers

9. 1. 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. Ziff. 5.1 dieser AV, Art. 32 DS-GVO nach. Dabei kann der Nachweis 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 in der Branche üblichen Tagessätze des Auftragsverarbeiters. Der Auftragsverarbeiter wird den Auftraggeber im Vorwege über nach dieser Klausel anfallende Kosten in Kenntnis setzen.

9. 2. 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. 9.2 dieser AV entsprechend.

9. 3. 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 Art. 40 und Art. 42 DS-GVO vorgesehenen Instrumentarien nachweisen kann (zusammenfassend „Compliance-Nachweise“).

10. Haftung, Vertragsstrafe, Außerordentliche Kündigung

10. 1. Die Parteien haften gem. Art. 82 DSGVO.

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

10. 3. 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

11. 1. Sofern zwischen den Parteien wegen der in dieser AV festgelegten oder in Bezug genommenen Leistungen bereits Vereinbarungen zur Datenverarbeitung im Auftrag bestehen, werden diese Vereinbarungen mit Wirksamkeit dieser AV aufgehoben und regelt diese AV abschließend die insoweit bestehenden Rechte und Pflichten der Parteien.

11. 2. 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 dergestalt unterzeichnet werden, dass 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.

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

11. 4. Die in dieser AV festgelegten und in Bezug genommenen Vorschriften gelten vorrangig gegenüber anderen, die Durchführung dieser AV betreffenden vertraglichen Regelungen zwischen den Parteien zur Erhebung und Verwendung von Auftraggeberdaten durch den Auftragsverarbeiter. 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.

Ort, Datum	Ort, Datum
Für Auftragsverarbeiter: Name, Vorname, Funktion	Für Auftraggeber: Name, Vorname, Funktion

Anhang 1: Dokumentation der Auftragsverarbeitung, Löschpflichten und des Datenaustauschs
Anhang 2: Technische und organisatorische Maßnahmen zur Daten – und Informationssicherheit

Anhang 1 - Dokumentation der Auftragsverarbeitung, Löschpflichten und des Datenaustauschs

Angaben zum Auftragsverarbeiter:

Name: HQLabs GmbH
Adresse des Unternehmens: Colonnaden 41, 20354 Hamburg
Geschäftsführer: Nils Lukas Czernig, Daniel Tobias Hagenau, Lucas Alexander Bauche
Registergericht, Registernummer: Hamburg, 122405
Telefon: +49 40 882 1533 0
Externer Datenschutzbeauftragter: PROLIANCE GmbH, Leopoldstr. 21, 80802 München, datenschutzbeauftragter@datenschutzexperte.de

1 Gegenstand, Art und Umfang der Verarbeitung von personenbezogenen Daten

Der Auftragsverarbeiter ist Hersteller und Anbieter von Unternehmenssoftware zur Abwicklung aller projektbezogenen kaufmännischen Prozesse. Hierzu zählen der Vertrieb, die Beratung, Implementierung sowie Integration, Hosting und Support der Lösungen. Die Datenerhebung, -verarbeitung und -nutzung erfolgt zur Ausübung der oben angegebenen Zwecke.
Zu folgenden Personengruppen werden personenbezogene Daten erhoben, verarbeitet und genutzt, sofern diese zur Erfüllung des genannten Zweckes erforderlich sind:

- Kundendaten / Interessentendaten (wie Adressdaten, Vertragsdaten, Angebotsdaten)
- Personaldaten zur Verwaltung von Mitarbeitern, Aushilfen und externen Mitarbeitern
- Daten von Geschäftspartnern (wie Adressdaten, Vertragsdaten)
- Daten von Lieferanten (wie Adressdaten, Vertragsdaten, Funktionsdaten)
- Daten von Kooperations- und Vertriebspartnern (wie Adressdaten, Vertragsdaten)

2 Art der Leistung (Mehrauswahl möglich)

☐	(Teil-)**Geschäftsprozess-Outsourcing** (Kundenservice, Vertrieb, Buchhaltung, Entwicklung, Forderungsmanagement, etc.)	☐	**Hosting** (Daten, Applikation, System, Komponenten)
☐	**Betrieb** (Applikation, System, Komponenten)	☐	**Wartung/Pflege** (Applikation, System, Komponenten)
☐	**Support** (Applikation, System, Komponenten)	☐	**SaaS** (Bitte spezifizieren): HQ Anwendungsbetrieb
☐	**Cloud Services** (Bitte spezifizieren)	☐	**Sonstige** (Bitte spezifizieren):

3 Subunternehmer

Der Auftragsverarbeiter setzt die nachfolgend aufgeführten Subunternehmer als weitere Auftragsverarbeiter ein. (Ggf. Zeilen ergänzen):

Name und Anschrift des Subunternehmers	**Zweck // Vertragsgrundlage // Garantien**
Chargebee Inc., 340 S Lemon Ave # 1537 Walnut, California 91789, USA	Chargebee wird zur Verwaltung unserer Kundenverträge und zur Rechnungsstellung eingesetzt. Zu diesem Zweck wird die Rechnungsadresse, die Emailadresse und der komplette Name des Rechnungsempfängers gespeichert. Außerdem werden die Zahlungsinformationen bei Chargebee hinterlegt. **Vertragsgrundlage**: Data Processing Agreement vom 12.04.2018 **Garantien**: EU-Standard Vertragsklauseln

Segment.io, Inc., 100 California Street, Suite 700 San Francisco, CA 94111 USA	Segment wird eingesetzt, um die Interaktion von den Usern mit der Software zu analysieren und auf Grundlage dieser Daten das Produkt zu optimieren. **Vertragsgrundlage**: Data Processing Agreement vom 04.12.2018 **Garantien**: EU-Standard Vertragsklauseln
Zendesk Inc., 1019 Market St San Francisco, CA 94103 USA	Zendesk wird für den Support Prozess eingesetzt. Kunden Anfragen werden zentral in Zendesk verarbeitet und gespeichert. **Vertragsgrundlage**: Data Processing Agreement vom 19.08.2020 **Garantien**: EU-Standard Vertragsklauseln
Intercom Inc., 55 2nd Street 4th Floor San Francisco, CA 94105 USA	Intercom wird eingesetzt, um den Nutzern der Software die Möglichkeit zu geben mit dem Support und dem Sales Team zu chatten und Usern automatisierte Nachrichten auszuspielen. **Vertragsgrundlage**: Data Processing Agreement vom 29.07.2020 **Garantien**: EU-Standard Vertragsklauseln
T-Systems International GmbH, Hahnstraße 43d 60528 Frankfurt a.M.Germany	Die Software wird im Rechenzentrum der T-Systems gehostet. Es werden die Daten in diesen Rechenzentren verarbeitet und persistent gespeichert. **Vertragsgrundlage**: Data Trustee Agreement vom 02.05.2018
SendGrid, Inc., 1801 California Street, Suite 500 Denver, Colorado 80202 USA	Emails die aus dem Softwareprodukt versendet werden, werden über Sendgrid übermittelt, soweit nicht ein eigener STMP-Server hinterlegt ist. **Vertragsgrundlage**: Data Processing Aggreement vom 12.04.2018 **Garantien**: EU-Standard Vertragsklauseln
LetterXpress, A&O Fischer GmbH & Co. KG, Maybachstraße 9, 21423 Winsen	LetterXpress wickelt die gesamte papiergebundene Briefkommunikation sicher und zuverlässig ab. **Vertragsgrundlage**: Data Processing Agreement vom 18.12.2019
New Relic Inc., 188 Spear Street, Suite 1200, San Francisco, California 94105 USA	New Relic wird eingesetzt, um die Performance der Anwendung zu messen. **Vertragsgrundlage:** Data Processing Agreement vom 09.09.2020 **Garantien:** EU Standard Vertragsklauseln
Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052 USA	Teile der Software werden im Rechenzentrum Azure Global gehostet. Es werden die Daten in diesen Rechenzentren verarbeitet und persistent gespeichert. Das Rechenzentrum befindet sich in Deutschland. **Vertragsgrundlage:** Data Processing Agreement vom 21.07.2020 **Garantien:** EU Standard Vertragsklauseln

4 **Ort der Datenspeicherung** durch den Auftragsverarbeiter oder einen Sub-Unternehmer (Mehrauswahl möglich)

☐	Bundesrepublik Deutschland	☐	Sonstiges Land innerhalb der EU oder des EWR: falls ja, bitte spezifizieren:
☐	Sogenanntes *Sicheres Drittland*; falls ja, bitte spezifizieren:	☐	USA; falls ja, sind mit der Stelle in den USA die EU-Standard Vertragsklauseln geschlossen? Ja ☐ / Nein ☐
☐	Sonstiges Drittland; falls ja, bitte spezifizieren:	☐	Keine Datenspeicherung durch den Auftragsverarbeiter oder einen Sub-Unternehmer

5 Ort der Daten*zugriffs* durch den Auftragsverarbeiter oder einen Sub-Unternehmer (Mehrauswahl möglich)

☐	Aus der Bundesrepublik Deutschland heraus	☐	Aus einem sonstigen Land innerhalb der EU oder des EWR heraus: falls ja, bitte spezifizieren:
☐	Aus einem sogenannten *Sicheren Drittland* heraus; falls ja, bitte spezifizieren:	☐	Aus den USA heraus; falls ja, sind mit der Stelle in den USA die EU-Standard Vertragsklauseln geschlossen? (Ja/Nein)? Ja
☐	Aus seinem sonstigen Drittland heraus; falls ja, bitte spezifizieren:		

6 Geplante sonstige Datenübermittlung in Drittstatten oder an internationale Organisationen durch den Auftragsverarbeiter (Mehrauswahl möglich)

Über die in Punkt 3 – Subunternehmer genannten dritten hinaus findet keine Übermittlung an Drittstaaten oder andere internationale Organisationen statt.

7 Kategorien von Betroffenen der Datenverarbeitung (Mehrauswahl möglich)

☐	Kunden bzw. Ansprechpartner bei Kunden des Auftragsverarbeiters	☐	Mitarbeiter
☐	Lieferanten bzw. Ansprechpartner bei Lieferanten	☐	Sonstige Betroffene, z.B. Interessenten
☐	Nutzer und Kunden von Kunden des Auftragsverarbeiters		

8 Kategorien von personenbezogenen Daten (Mehrauswahl möglich)

☐	**Stammdaten**, d.h. personenbezogene Daten, die erforderlich sind, um das mit einem Betroffenen bestehende Vertragsverhältnis zu begründen, durchzuführen und ggf. zu beenden (Namen, Vorname, Kunden-, Mitarbeiter- oder Vertragsnummern, Informationen über Produkte, Tarife, Unternehmens- oder Abteilungszugehörigkeit, Rechnungsinformationen, Informationen über Kontakthistorie, etc.)	☐	**Verkehrsdaten** (excl. Standortdaten), d.h. Informationen die bei der Initiierung, Aufrechterhaltung und Abwicklung eines konkreten Kommunikationsvorgangs notwendigerweise anfallen, d.h. z.B. einem Kommunikationsvorgang zuordenbare Anschlusskennungen (A- und B-rufnummer), IP-Adressen oder Gerätekennungen (MAC-Adresse, IMEI, etc.), Informationen zu Beginn und Ende von Kommunikationsvorgängen (etwa in CDRs oder Log-Dateien)
☐	**Kontaktinformationen**, d.h. Postadressen, E-Mail-Adressen, Telefonnummer(n), Messenger-IDs, etc.	☐	**Endgerätedaten** (excl. Standortdaten), d.h. aus Endgeräten, etwa über mobile Apps ausgelesene Informationen (Log-Files, Systemzustände, Nutzereinstellungen, etc., Browserinformationen)
☐	**Bankdaten,** d.h. Kontonummer/IBAN, Kredikarten-informationen	☐	**Nutzungsdaten**, d.h. Informationen über Art, Umfang, Dauer und Zeitpunkt der

			Nutzung eines web-basierten Multimedia-Angebots (Webseiten, Videoangebote, etc.)
☐	**Kommunikationsinhalte,** d.h. SMS- oder E-Mail-Inhalte, Voice-Messages, Clickstreams, etc.	☐	**„User generated content“,** d.h. Inhalte (Dokumente, Bilder, Musikdateien, Äußerungen etc.), die Betroffene willentlich und wissentlich selbst erzeugt haben
☐	**Standortdaten** aus Netzwerkkommunikation**,** d.h. Cell-IDs aus Mobilfunkverbindungen, GPS-Koordinaten, IP-Lokalisierung, etc.	☐	**User-Account-Informationen**, d.h. z.B. Benutzername, Passwort, Rechteprofil, Organisationsinformationen, etc.
☐	**Sonstige** (Bitte spezifizieren):		

9 Kategorien besonders schützenswerter personenbezogener Daten (Mehrauswahl möglich)

☐	Daten über die **rassische und ethnische Herkunft** (z.B. Zugehörigkeit zu einer bestimmten Volksgruppe im Rahmen von Asylverfahren)	☐	Daten über **politische Meinungen** (z.B. Wahlentscheidungen oder Parteizugehörigkeiten)
☐	Daten über **religiöse oder weltanschauliche Überzeugungen** (z.B. Informationen über Religionszugehörigkeit im Rahmen der steuerlichen Erfassung)	☐	Daten über die **Gewerkschaftszugehörigkeit**
☐	**Genetische Daten** (z.B. genetische Veranlagungen bzw. bekannte Erbkrankheiten)	☐	**Biometrischen Daten** zur eindeutigen Identifizierung einer natürlichen Person
☐	**Gesundheitsdaten** (z.B. Krankenakten im betriebsmedizinischen Dienst, BEM-Daten, Krankmeldungen)	☐	Daten zum **Sexualleben oder der sexuellen Orientierung** einer natürlichen Person

10 Spezifische Löschpflichten (nur relevant, wenn (i) eine Datenspeicherung Bestandteil der Auftragsverarbeitung ist und (ii) auch während der Vertragslaufzeit Löschroutinen zu implementieren sind):

Die nachfolgend benannten, spezifischen Löschfristen sind umzusetzen:

Der Auftragsverarbeiter hat ihm überlassene und alle ergänzend verarbeiteten Daten einschließlich sämtlicher Vervielfältigungen (auch in Archivierungs- und Sicherungsdateien) vollständig und unwiderruflich nach 35 Tagen zu löschen oder zu vernichten (nachfolgend 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 35 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.

11 Repräsentanten in Fragen des Datenschutzes

Verantwortlicher	
Identität des Datenschutzbeauftragten	PROLIANCE GmbH www.datenschutzexperte.de Leopoldstr. 21 80802 München datenschutzbeauftragter@datenschutzexperte.de
Auftragsverarbeiter	
Identität des Datenschutzbeauftragten bzw. der „Lead-Function“ für Datenschutz	Name: Czernig Vorname: Nils Bezeichnung: Geschäftsführer

Anhang 2 - Technische und organisatorische Maßnahmen zur Daten- und Informationssicherheit

1 Vertraulichkeit der Daten

1.1 Zutrittskontrolle

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

1.1.2 Die Eingänge zu den Räumlichkeiten des Auftragsverarbeiters, in denen Personenbezogene Daten verarbeitet werden, sind mit Sicherheits- oder Magnetkartenschlössern gegen Zutritt Unbefugter gesichert.

1.1.3 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, sowie die in VdS 2333 beschriebenen Sicherungsmaßnahmen der Sicherungsklasse SG1.

1.1.4 Zur Durchführung des Auftrags vom Auftragsverarbeiter verwendete Server sind in einem separat abgesicherten Serverraum oder Rechenzentrum untergebracht, welche durch eine Zutrittskontrollanlage entsprechend Klasse B nach VdS 2367 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

1.2.1 Die zur Durchführung des Auftrags vom Auftragsverarbeiter eingesetzten informationsverarbeitenden Systeme (Client- und Serversysteme) sind durch Authentifikations- und Autorisationssysteme geschützt.

1.2.2 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.

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

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

1.2.5 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 entsprechend den in Ziffer 1.2.6 dieses Anhangs 2 festgelegten Bestimmungen auf ein nur der berechtigten Person bekanntes Passwort umgesetzt; jegliche Weitergabe unterbleibt. Sofern Unbefugte Kenntnis von Zugangsdaten erhalten, zeigt der Auftragsverarbeiter dies dem Verantwortlichen unverzüglich an.

1.2.6 Die Wahl der Passwörter erfolgt in ausreichender Komplexität und Güte. Ausreichende Komplexität und Güte bedeutet mindestens eine Länge von zehn (10) Zeichen bei Nutzung von drei der folgenden 4 Kategorien (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen), keine Verwendung generischer Begriffe oder von Eigennamen sowie die Unzulässigkeit mindestens der letzten drei (3) verwendeten Passwörter.

1.2.7 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 1.2.8 dieses Anhangs 2 entsprechenden Verschlüsselung oder als unumkehrbare kryptographische Prüfsumme (insbesondere bei der Speicherung und der Übertragung im Netzwerk).

1.2.8 Für die Verschlüsselung wird der AES Algorithmus mit 256 Bit und für Password Hashes der HMAC Algorithmus mit 512 Bit verwendet.

1.3 Zugriffskontrolle

1.3.1 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.

1.3.2 Alle verarbeiteten Daten werden verschlüsselt übertragen.

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

1.3.3 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 Personenbezogene Daten mindestens für die Dauer von 90 Tagen protokolliert.

2 Integrität

2.1 Weitergabekontrolle

2.1.1 Personenbezogene Daten können nicht unbefugt kopiert (insbesondere auf externe Datenträger gespeichert), weitergegeben und/oder gelöscht werden.

2.1.2 Datenträger sowie sämtliche Dokumente, sofern sie Personenbezogene Daten enthalten (einschließlich sämtlicher gegebenenfalls vorhandener Sicherungskopien von personenbezogene Daten und Kopien von Originaldokumenten) werden in ordnungsgemäß verschlossenen, und ausschließlich für die Durchführung des Auftrags genutzten Datensicherungsschränken verwahrt, wenn und solange sie nicht nach Maßgabe der Ziffern 2.1.3 oder 2.1.5 dieses Anhangs 2 in der Bearbeitung sind.

2.1.3 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.

2.1.4 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.

2.1.5 Nach Ziffer 2.1.3 dieses Anhangs 2 herausgegebene Originaldokumente oder nach Maßgabe von Ziffer 2.1.4 dieses Anhangs 2 erstellte handschriftliche Aufzeichnungen werden, auch bei auch nur kurzzeitigem Verlassen des Arbeitsplatzes, vor unberechtigtem Zugriff geschützt (“Clean Desk Policy“).

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

2.1.7 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. Sofern Dritte mit der Wartung solcher Systeme betreut sind, gilt Ziffer 1.3.2 dieses Anhangs 2 entsprechend.

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 personenbezogene Daten

sichergestellt, z.B., durch Speicherung der Personenbezogene Daten in einem eigenen Mandanten, in einer eigenen Partition oder unter eindeutigen Identifier getrennt abrufbar. Eine entsprechende Trennung wird auch für personenbezogene Daten selbst realisiert, wenn sie zu verschiedenen Zwecken gespeichert werden.

3 **Verfügbarkeitskontrolle**

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

3.2 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. Bei als „kritisch“ oder sinngemäß qualifizierten Aktualisierungen beträgt die Frist nach Satz 1 höchstens zwei (2) Tage.

3.3 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.

3.4 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

4.1 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 umfassend geschult.

4.2 Am Ende und auf Grundlage des in Ziffer 4.1 dieses Anhangs 2 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 Löschung

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

(a) die datenschutzgerechte nicht wieder herstellbare Löschung sämtlicher, personenbezogene Daten enthaltender, löschbaren elektronischen Datenträger (insbesondere Festplatten, USB-Sticks, Disketten, Bänder) durchführen;

(b) die nachhaltige und irreversible Entfernung von personenbezogene Daten aus Datenbank- oder File-Systemen sowie aus allen anderen löschbaren Speichermedien realisieren; und

(c) sämtliche, personenbezogene Daten enthaltende Papierdokumente und sonstige nicht-gemäß Buchstabe (a) oder (b) dieser Ziffer 5.1 löschbaren Datenträger (einschließlich sämtlicher personenbezogene Daten enthaltener Fehldrucke, Speicherkarten, USB-Sticks, etc.) mit einem handelsüblichen Dokumentenvernichter gemäß 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.

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

6 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.