zwischen

_____

_____

_____

nachstehend **„Verantwortlicher“**

und

Flexperto GmbH
Neue Grünstr. 27
10179 Berlin

nachstehend **“Auftragsverarbeiter“**

Präambel

Zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht ein Auftragsverhältnis im Sinne des Art. 28 der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, „**DSGVO**“).

Dieser Auftragsverarbeitungsvertrag einschließlich aller Anlagen (nachfolgend gemeinsam als „**Vereinbarung**“ bezeichnet) konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien aus dem zugrundeliegenden Vertrag, der Leistungsvereinbarung und/oder Auftragsbeschreibung einschließlich aller Anlagen (nachfolgend gemeinsam als „**Hauptvertrag**“ bezeichnet). Sofern Bezug auf die Regelungen des Bundesdatenschutzgesetzes (nachfolgend „**BDSG**“) genommen wird, so ist damit das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 in der zum Zeitpunkt ab dem 25. Mai 2018 geltenden Fassung gemeint.

Der Auftragsverarbeiter verpflichtet sich gegenüber dem Verantwortlichen zur Erfüllung des Hauptvertrages und dieser Vereinbarung nach Maßgabe der folgenden Bestimmungen:

1. Anwendungsbereich und Begriffsbestimmungen

1.1. Die nachfolgenden Bestimmungen finden Anwendung auf alle Leistungen der Auftragsverarbeitung im Sinne des Art. 28 DSGVO, die der Auftragsverarbeiter auf Grundlage des Hauptvertrages gegenüber dem Verantwortlichen erbringt sowie alle Tätigkeiten, bei denen es zu einer Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter für den Verantwortlichen kommen kann.

1.2. Sofern in dieser Vereinbarung der Begriff „Datenverarbeitung“ oder „Verarbeitung“ von Daten benutzt wird, ist darunter allgemein die Verwendung von personenbezogenen Daten zu verstehen. Datenverarbeitung oder das Verarbeiten von Daten bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine

andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

1.3. Auf die weiteren Begriffsbestimmungen in Art. 4 DSGVO wird verwiesen.

2. Gegenstand und Dauer der Datenverarbeitung

2.1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag und nach Weisung des Verantwortlichen.

2.2. Gegenstand des Auftrags ist die Bereitstellung einer webbasierten Softwarelösung für die digitale Kommunikation im Rahmen des mit dem Auftragsverarbeiter vereinbarten Umfangs, gemäß dem Hauptvertrag.

2.3. Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages.

3. Art und Zweck der Datenverarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag. Dieser umfasst folgende Tätigkeit(en) und Zweck(e): Bereitstellung einer webbasierten Softwarelösung für die digitale Kommunikation insbesondere zur Terminvereinbarung, Echtzeit-Kommunikation per Videochat und Textchat sowie Austausch von Nachrichten und Dateien sowie ferner die elektronische Unterschrift von Dokumenten.

4. Kategorien betroffener Personen

Die Kategorien der durch den Umgang mit den personenbezogenen Daten im Rahmen dieser Vereinbarung betroffenen Personen umfasst:

- Beschäftigte des Auftraggebers
- Kunden des Auftraggebers
- Interessenten des Auftraggebers
- Bewerber des Auftraggebers
- Zulieferer des Auftraggebers
- Partner des Auftraggebers
- Auftragnehmer des Auftraggebers
- Selbstständig tätige Mitarbeiter des Auftraggebers

5. Art der personenbezogenen Daten

Von der Auftragsverarbeitung sind folgende Datenarten betroffen

- Personenstammdaten
- Kontaktdaten (Telefon, E-Mail)
- Kommunikationsdaten (Audio- und Videostreaming und Screensharing)
- Inhaltsdaten (geteilte Dateien, Textchat, Whiteboard-Inhalte)
- Signaturdaten (Charaktereigenschaften der digitalen Signatur)
- Vertragsdaten (zugrundeliegende rechtliche Dokumente bei digitaler Signatur)
- Kalenderdaten (Datum, Dauer, Verfügbarkeit)

- Kalenderauthentifizierungsdaten
- Metadaten
  - Aktivitätsprotokolle (Log-Files)
  - IP-Adresse
  - Cookies

6. Rechte und Pflichten des Verantwortlichen

6.1. Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie zur Wahrung der Rechte der Betroffenen ist allein der Verantwortliche zuständig und somit für die Verarbeitung Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

6.2. Der Verantwortliche ist berechtigt, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen sind auf Verlangen des Verantwortlichen unverzüglich vom Auftragsverarbeiter schriftlich oder in Textform (z.B. per E-Mail) zu bestätigen.

6.3. Soweit es der Verantwortliche für erforderlich hält, können weisungsberechtigte Personen benannt werden. Diese wird der Verantwortliche dem Auftragsverarbeiter schriftlich oder in Textform mitteilen. Für den Fall, dass sich diese weisungsberechtigten Personen bei dem Verantwortlichen ändern, wird dies dem Auftragsverarbeiter unter Benennung der jeweils neuen Person schriftlich oder in Textform mitgeteilt.

6.4. Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter festgestellt werden.

6.5. Der Verantwortliche ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig nach rechtzeitiger vorheriger Anmeldung zu den üblichen Geschäftszeiten von der Einhaltung der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Verantwortliche kann diese Kontrolle auch durch einen Dritten durchführen lassen.

7. Pflichten des Auftragsverarbeiters

7.1. <u>Datenverarbeitung</u>

Der Auftragsverarbeiter ist verpflichtet, personenbezogene Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des zugrundeliegenden Hauptvertrages sowie nach den Weisungen des Verantwortlichen zu verarbeiten. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragsverarbeiter untersagt. Der Auftragsverarbeiter ist verpflichtet, die zur Datenverarbeitung überlassenen Daten nicht für andere, insbesondere nicht für eigene Zwecke zu verarbeiten.

7.2. <u>Betroffenenrechte</u>

7.2.1. Der Auftragsverarbeiter wird den Verantwortlichen bei der Erfüllung der Rechte der Betroffenen, insbesondere im Hinblick auf Berichtigung, Einschränkung der Verarbeitung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen seiner Möglichkeiten unterstützen. Sollte der Auftragsverarbeiter die in Ziff. 5 dieser Vereinbarung genannten personenbezogenen Daten im Auftrag des Verantwortlichen verarbeiten und sind diese Daten Gegenstand eines Verlangens auf Datenportabilität

gem. Art. 20 DSGVO, wird der Auftragsverarbeiter dem Verantwortlichen den betreffenden Datensatz regelmäßig innerhalb von 5 Werktagen in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen.

7.2.2. Der Auftragsverarbeiter hat auf Weisung des Verantwortlichen die in Ziff. 5 dieser Vereinbarung genannten personenbezogenen Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder die Verarbeitung einzuschränken. Das Gleiche gilt, wenn diese Vereinbarung eine Berichtigung, Löschung oder Einschränkung der Verarbeitung von Daten vorsieht.

7.2.3. Soweit sich eine betroffene Person unmittelbar an den Auftragsverarbeiter zwecks Berichtigung, Löschung oder Einschränkung der Verarbeitung der in Ziff. 5 dieser Vereinbarung genannten personenbezogenen Daten wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich nach Erhalt an den Verantwortlichen weiterleiten.

7.3. Kontrollpflichten

7.3.1. Der Auftragsverarbeiter stellt durch geeignete Kontrollen sicher, dass die im Auftrag verarbeiteten personenbezogenen Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des Hauptvertrages und/oder den entsprechenden Weisungen verarbeitet werden.

7.3.2. Der Auftragsverarbeiter gestaltet sein Unternehmen und seine Betriebsabläufe so, dass die Daten, die er im Auftrag des Verantwortlichen verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

7.3.3. Der Auftragsverarbeiter bestätigt, dass er gem. Art. 37 DSGVO und, sofern anwendbar, gemäß § 38 BDSG einen Datenschutzbeauftragten bestellt hat und die Einhaltung der Vorschriften zum Datenschutz und zur Datensicherheit unter Einbeziehung des Datenschutzbeauftragten überwacht.

Sie können sich jederzeit vertrauensvoll, unter der E-Mail-Adresse datenschutzbeauftragter@flexperto.com oder unter der Postanschrift von Flexperto mit dem Zusatz „z. Hd. Datenschutzbeauftragter“, an ihn wenden.

7.4. Informationspflichten

7.4.1. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darauf aufmerksam machen, wenn eine von dem Verantwortlichen erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

7.4.2. Bei der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten gem. Art. 30 DSGVO durch den Verantwortlichen wird der Auftragsverarbeiter den Verantwortlichen unterstützen und die jeweils erforderlichen Angaben in geeigneter Weise zur Verfügung stellen.

7.4.3. Der Auftragsverarbeiter wird dem Verantwortlichen jeden Verstoß gegen datenschutzrechtliche Vorschriften, gegen die getroffenen Regelungen im

Hauptvertrag und der Vereinbarung und/oder die erteilten Weisungen des Verantwortlichen, der im Zuge der Verarbeitung von Daten durch ihn, bei ihm beschäftigte Personen oder andere mit der Verarbeitung betraute Dritte erfolgt ist, unverzüglich mitteilen.

7.4.4. Für den Fall, dass der Auftragsverarbeiter feststellt, dass von ihm für den Verantwortlichen verarbeitete personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind bzw. der Schutz personenbezogener Daten auf andere Weise verletzt wurde, hat der Auftragsverarbeiter den Verantwortlichen unverzüglich über den Datenschutzvorfall zu informieren. Die Mitteilung des Auftragsverarbeiters über den Datenschutzvorfall wird, sofern möglich, die Einzelheiten des Datenschutzvorfalls sowie Maßnahmen beinhalten, die durch ihn getroffen wurden, um die unrechtmäßige Übermittlung und/oder unbefugte Kenntnisnahme durch Dritte bzw. Verletzung des Schutzes personenbezogener Daten akut und zukünftig zu verhindern. Der Auftragsverarbeiter wird den Vorgang einschließlich der Auswirkungen und Abhilfemaßnahmen dokumentieren und dem Verantwortlichen diese Dokumentation auf Anfrage zur Verfügung stellen. Ferner wird der Auftragsverarbeiter den Verantwortlichen im erforderlichen und zumutbarem Umfang bei der Erfüllung etwaiger Meldepflichten unterstützen.

7.5. Ort der Datenverarbeitung

7.5.1. Die Verarbeitung und Nutzung der Daten findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Eine Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

7.5.2. Für die Verarbeitung personenbezogener Daten außerhalb der EU garantiert der Auftragsverarbeiter, dass die nach den jeweils geltenden Datenschutzvorschriften anwendbaren Voraussetzungen für das Eingreifen eines Erlaubnistatbestandes für die Verarbeitung personenbezogener Daten außerhalb der EU erfüllt sind ("datenschutzrechtliche Rechtfertigung").

7.6. Löschung der personenbezogenen Daten nach Auftragsbeendigung

Nach Beendigung des Hauptvertrages wird der Auftragsverarbeiter sämtliche im Rahmen der Auftragsverarbeitung in seinen Besitz gelangten personenbezogenen Daten nach Wahl des Verantwortlichen entweder löschen oder zurückgeben, sofern nicht nach dem Unionsrecht oder dem Recht der betreffenden Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Eine Löschung ist zu dokumentieren und dem Verantwortlichen auf Anfrage schriftlich oder in Textform zu bestätigen.

8. Kontrollrechte des Verantwortlichen

8.1. Der Verantwortliche ist berechtigt, nach rechtzeitiger vorheriger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Geschäftsbetriebes des Auftragsverarbeiters oder Gefährdung der Sicherheitsmaßnahmen für andere Auftraggeber und auf eigene Kosten, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang selbst oder durch Dritte zu kontrollieren. Die Kontrollen können auch durch Zugriff auf vorhandene branchenübliche Zertifizierungen des Auftragsverarbeiters, aktuelle Testate oder Berichte einer unabhängigen Instanz (wie z.B. Wirtschaftsprüfer, externer

Datenschutzbeauftragter, Revisor oder externer Datenschutzauditor) oder Selbstauskünfte durchgeführt werden. Der Auftragsverarbeiter wird die notwendige Unterstützung zur Durchführung der Kontrollen anbieten.

8.2. Der Auftragsverarbeiter hat eventuelle Kontrollmaßnahmen der Datenschutzaufsichtsbehörde gem. Art. 58 DSGVO und, sofern anwendbar, § 40 BDSG zu dulden. Er wird den Verantwortlichen unverzüglich nach Ankündigung oder Kenntniserlangung über die Durchführung der Kontrollmaßnahme sowie bei anderweitigen Anfragen, Ermittlungen oder Erkundigungen der Datenschutzaufsichtsbehörde, insbesondere auch, wenn diese im Rahmen einer vorherigen Konsultation gem. Art. 36 DSGVO erfolgen, informieren, soweit die Maßnahmen oder Anfragen Datenverarbeitungen betreffen können, die der Auftragsverarbeiter für den Verantwortlichen erbringt.

9. Unterauftragsverhältnisse

9.1. Der Verantwortliche ermächtigt den Auftragsverarbeiter weitere Auftragsverarbeiter gemäß den nachfolgenden Absätzen in Ziff. 9 dieser Vereinbarung in Anspruch zu nehmen. Diese Ermächtigung stellt eine allgemeine schriftliche Genehmigung i. S. d. Art. 28 Abs. 2 DSGVO dar.

9.2. Der Auftragsverarbeiter arbeitet derzeit bei der Erfüllung des Auftrags mit den in der **Anlage 2** benannten Unterauftragnehmern zusammen, mit deren Beauftragung sich der Verantwortliche einverstanden erklärt.

9.3. Der Auftragsverarbeiter ist berechtigt, weitere Auftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen. Der Auftragsverarbeiter wird den Verantwortlichen vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines weiteren Auftragsverarbeiters informieren. Der Verantwortliche kann gegen derartige Änderungen Einspruch erheben. Bei einem Einspruch des Verantwortlichen wird der Auftragsverarbeiter auf die Änderung verzichten oder einen alternativen weiteren Auftragsverarbeiter vorschlagen und mit dem Verantwortlichen abstimmen. Schlägt dies fehl, kann der Verantwortliche diese Vereinbarung sowie den Hauptvertrag mit einer Frist von drei Monaten zum Monatsende kündigen.

9.4. Bei Einschaltung eines weiteren Auftragsverarbeiters werden diesem durch einen Vertrag oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dieser Vereinbarung festgelegt sind. Der Auftragsverarbeiter kontrolliert, dass der weitere Auftragsverarbeiter die zugesicherten und erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragsverarbeiter zu dokumentieren und auf Anfrage dem Verantwortlichen zu übermitteln.

9.5. Nicht als weitere Auftragsverarbeiter sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

10. Vertraulichkeit

10.1. Der Auftragsverarbeiter ist bei der Verarbeitung von Daten für den Verantwortlichen zur Wahrung der Vertraulichkeit verpflichtet.

10.2. Der Auftragsverarbeiter sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist.

10.3. Der Auftragsverarbeiter verpflichtet sich bei der Erfüllung des Auftrags nur Mitarbeiter oder sonstige Erfüllungsgehilfen einzusetzen, die auf die Vertraulichkeit im Umgang mit überlassenen personenbezogenen Daten verpflichtet und in geeigneter Weise mit den Anforderungen des Datenschutzes vertraut gemacht worden sind. Die Vornahme der Verpflichtungen wird der Auftragsverarbeiter dem Verantwortlichen auf Nachfrage nachweisen.

10.4. Sofern der Verantwortliche anderweitigen Geheimnisschutzregeln unterliegt, wird er dies dem Auftragsverarbeiter mitteilen. Der Auftragsverarbeiter wird seine Mitarbeiter entsprechend den Anforderungen des Verantwortlichen auf diese Geheimnisschutzregeln verpflichten.

11. Technische und organisatorische Maßnahmen

11.1. Die in **Anlage 1** beschriebenen technischen und organisatorischen Maßnahmen werden als angemessen vereinbart. Der Auftragsverarbeiter kann diese Maßnahmen aktualisieren und ändern, vorausgesetzt dass das Schutzniveau durch solche Aktualisierungen und/oder Änderungen nicht herabgesetzt wird.

11.2. Der Auftragsverarbeiter beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung gemäß Art 32 i.V.m Art. 5 Abs. 1 DSGVO. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen. Er wird alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Standes der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene ergreifen. Die zu treffenden Maßnahmen umfassen insbesondere Maßnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Maßnahmen, die die Kontinuität der Verarbeitung nach Zwischenfällen gewährleisten. Um stets ein angemessenes Sicherheitsniveau der Verarbeitung gewährleisten zu können, wird der Auftragsverarbeiter die implementierten Maßnahmen regelmäßig evaluieren und ggf. Anpassungen vornehmen.

12. Vergütung

Die Vergütung des Auftragsverarbeiters ergibt sich aus dem zugrundeliegenden Hauptvertrag.

13. Haftung

13.1. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen gemäß den gesetzlichen Regelungen für sämtliche Schäden durch schuldhafte Verstöße gegen diese Vereinbarung sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen, die der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen. Sofern der Hauptvertrag hiervon Abweichendes bestimmt, gehen die Bestimmungen dieses Absatzes vor, soweit dies zulässig ist.

13.2. Eine Ersatzpflicht des Auftragsverarbeiters besteht nicht, sofern der Auftragsverarbeiter nachweist, dass er die ihm überlassenen Daten des Verantwortlichen ausschließlich nach den Weisungen des Verantwortlichen verarbeitet und seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nachgekommen ist.

13.3. Der Verantwortliche stellt den Auftragsverarbeiter von allen Ansprüchen Dritter frei, die aufgrund einer schuldhaften Verletzung der Verpflichtungen aus dieser Vereinbarung oder geltenden datenschutzrechtlichen Vorschriften durch den Verantwortlichen gegen den Auftragsverarbeiter geltend gemacht werden.

14. Sonstiges

14.1. Im Falle von Widersprüchen zwischen den Bestimmungen in dieser Vereinbarung und den Regelungen des Hauptvertrages gehen die Bestimmungen dieser Vereinbarung vor.

14.2. Änderungen und Ergänzungen dieser Vereinbarung setzen die beidseitige Zustimmung der Vertragsparteien voraus unter konkreter Bezugnahme auf die zu ändernde Regelung dieser Vereinbarung. Mündliche Nebenabreden bestehen nicht und sich auch für künftige Änderungen dieser Vereinbarung ausgeschlossen.

14.3. Diese Vereinbarung unterliegt deutschem Recht.

14.4. Sofern der Zugriff auf die Daten, die der Verantwortliche dem Auftragsverarbeiter zur Datenverarbeitung übermittelt hat, durch Maßnahmen Dritter (z.B. Maßnahmen eines Insolvenzverwalters, Beschlagnahme durch Finanzbehörden, etc.) gefährdet wird, hat der Auftragsverarbeiter den Verantwortlichen unverzüglich hierüber zu benachrichtigen.

Auftragsverarbeiter (Flexperto GmbH)	**Lizenznehmer / Verantwortlicher**
Datum: _____	Datum: _____
Name: _____	Name: _____
Position: _____	Position: _____
Unterschrift: _____	Unterschrift: _____

Anlagenverzeichnis

Anlage 1	Technische und organisatorische Maßnahmen des Auftragsverarbeiters
Anlage 2	Unterauftragsverhältnisse gemäß Ziff. 9 der Vereinbarung zur Auftragsverarbeitung
Anlage 3	Klärung zu Art der Daten, Verarbeitung durch Subdienstleister
Anlage 4	Klärung zu Art der Daten, Kreis der Betroffenen und Speicherort

ANLAGE 1

Technische und organisatorische Maßnahmen des Auftragsverarbeiters
Der Auftragsverarbeiter sichert zu, folgende technische und organisatorische Maßnahmen getroffen zu haben:

1. Maßnahmen zur Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.

Beschreibung der Pseudonymisierung:

Innerhalb der Plattform wird auf Datensätze von Personen lediglich mit Referenzen gearbeitet. So wird sichergestellt, dass es innerhalb der Plattform ausschließlich einen Ort gibt, in dem personenbezogene Daten vorliegen. Diese Vorgabe ist software-architektonisch beschrieben und dokumentiert. Im Rahmen der Entwicklung wird die Vorgabe durch Reviews von Codes sowie von technischer Planung vorab der Entwicklung geprüft und sichergestellt. So kann gewährleistet werden, dass:

- Die Daten sensibel verwendet werden. Daten zur Person werden nur zur Verfügung gestellt, wenn die benötigte Funktionalität dies voraussetzt.
- Die Daten schnell und sicher anonymisiert werden können. Das Überschreiben der personenbezogenen Daten hat einen sofortigen und globalen Effekt.

2. Maßnahmen zur Verschlüsselung

Maßnahmen oder Vorgänge, bei denen ein klar lesbarer Text / Information mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine unleserliche, das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird:

- SSL-Verschlüsselung
- Verschlüsselung aller Datenleitungen:
    1. HTTPS/WSS
    2. TCP/IP Sockets
- Verschlüsselte VPN-Verbindung auf Server
- TLS Verschlüsselung über TLS 1.2 Protokoll

3. Maßnahmen zur Sicherung der Vertraulichkeit

3.1. Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren:

Beschreibung des Zutrittskontrollsystems:

Bürostandort:

- Verschluss von Clients in Schränken nach Dienstschluss
- Zutritt des Gebäudes nur über Chipkarten
- Mieterbezogene Chipkartenverwaltung
- Organisationsanweisung zur Ausgabe von Chipkarten

Serverstandort (durch Subdienstleister):

- Gesicherte Fenster (z.B. vergittert, Sicherheitsglas)
- Mit Schloss gesicherte Räume (z.B. Zahlenschloss, Schlüssel, Biometrieschloß, Transponder)
- Gelände durch Zaun mit Bewegungsmeldesystem geschützt
- Dokumentiertes Zutritts-ID-System
- 24/7 Wachpersonal vor Ort

3.2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.

Beschreibung des Zugangskontrollsystems:

- Personalisierte Nutzer-Accounts
- Revisionssicheres, verbindliches Verfahren zur Rücksetzung „vergessener“ Passwörter vorhanden
- Revisionssicheres, verbindliches Verfahren zur Vergabe von Berechtigungen vorhanden
- Richtlinie zum sicheren, ordnungsgemäßen Umgang mit Passworten
- Automatische, passwortgeschützte Bildschirm- und Rechnersperre
- Serversysteme nur mit Konsolenpasswort oder über passwortgeschützte, verschlüsselte Verbindung administrierbar
- Clientsysteme nur nach mindestens passwortgestützter lokaler bzw. zentraler Authentifizierung nutzbar
- Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware (z. B. Virenscanner)
- Drucker nur für berechtigte Personen im Netzwerk zugänglich

3.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beschreibung des Zugriffskontrollsystems:

- Rollenbasiertes Berechtigungskonzept
- Dokumentation der Berechtigungen
- Streng reglementierter Datenbankzugriff
- Direkter Server-Zugriff auf CTO und DevOps beschränkt
- Nur IT- und datenschutzrechtlich geschultes Personal hat Zugriff auf Kundendaten
- Revisionssicheres, verbindliches Verfahren zur Wiederherstellung von Daten aus Backup

- Trennung von Berechtigungsbewilligung (organisatorisch) durch HR und CEO und Berechtigungsvergabe (technisch) durch CTO oder System Administrator

3.4. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

Beschreibung des Trennungskontrollvorgangs:

- Trennung von Entwicklungs-, Test- und Produktivsystemen
- Verarbeitung von personenbezogenen Daten im Auftrag lediglich im Rechenzentrum durch gesicherten Zugriff von Clients am Bürostandort über verschlüsselte Verbindungen
- Die Daten des Auftraggebers und anderer Kunden/Mandanten werden bei einem Dienstleister auf logisch getrennten Systemen verarbeitet.
- Es existiert ein Berechtigungskonzept, das der getrennten Verarbeitung von Daten des Auftraggebers von Daten anderer Kunden/Mandanten Rechnung trägt.

4. Maßnahmen zur Sicherung der Integrität

4.1. Datenintegrität

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden:

Beschreibung der Datenintegrität:

- Redundante Speicher-Systeme und Datenbanken
- Regelmäßige Backups der Speicher-Systeme und Datenbanken
- Deployment neuer Releases und Patches mit Release-/Patch Management
- Funktionstest bei Installation und Releases/Patches durch Qualitätssicherung
- Logging sowohl der Geschäftsprozesse sowie des Release-/Patch Managements
- Regelmäßige Prüfung und Aktualisierung der Versionen von verwendeten Systemen entlang klar definierter Migrationspfade

4.2. Übertragungskontrolle

Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können:

Beschreibung der Übertragungskontrolle:

- Logging der Geschäftsprozesse sowie von Transaktionen von Datensätzen
- Kontrollprozesse, die das manuelle Übertragen von Daten verhindern (Übertragungen finden nur automatisiert statt)

- Klare Sicherheits-Architektur und Kontroll-Gateways, die sicherstellen, dass Daten nur in klar definierten, authentifizierten und autorisierten Richtungen mit verschlüsselten Transportwegen übertragen werden

4.3. Transportkontrolle

Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

Beschreibung der Transportkontrolle:

- Verwendung von TLS sowohl innerhalb öffentlicher als auch privater Netze
- Regelmäßiges Patching der verwendeten kryptographischen Verfahren
- Administrativer System-Zugriff ausschließlich über getrennte Netze und gesonderte Tunnelverbindungen mit passwortgeschützten private/public RSA-Keys
- Regelmäßige Rotation der Zugriffsschlüssel
- Klares Berechtigungskonzept sowohl für administrativen Systemzugriff als auch administrativen Applikationszugriff
- Umfassende und separierte Protokollierungsverfahren für System- und Applikationszugriff

4.4. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Beschreibung des Eingabekontrollvorgangs:

- Sämtliche System- und Programmeingaben werden geloggt
- Netzzugriffe werden geloggt
- Logfile Management
- Protokollierung der Administrationstätigkeiten (Anlegen von Benutzern, Ändern von Benutzerrechten etc.)
- Erstellen von Änderungsbelegen zu den Vorgängen: Erstellung von kritischen Berechtigungen, sämtliche Löschung, Änderung von Daten, sämtliche Arbeiten am Source Code.

5. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

5.1. Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beschreibung des Verfügbarkeitskontrollsystems:

- Unterbrechungsfreie Stromversorgung am Serverstandort
- Archivierungskonzept
- Feueralarmsystem (Büro- und Serverstandort)
- Feuerlöschsystem (Serverstandort)
- Klimaanlage (Serverstandort)

- Vollständiges Backup- und Recoverykonzept mit täglicher Sicherung und katastrophensicherer Aufbewahrung der Datenträger
- Notfall- und Wiederanlaufverfahren mit regelmäßiger Erprobung
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter) und schriftliche Konzeption ihres Einsatzes (Virenschutzkonzept usw.)
- Einsatz von Festplattenspiegelung
- Verfügbarkeit eines Ausweichrechenzentrums
- Vorhalten von einsatzbereiter Zwillingssysteme
- Brandmeldeanlage
- Alarmanlage
- Notfallplan

5.2. Rasche Widerherstellbarkeit

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beschreibung der Maßnahmen zur raschen Widerherstellbarkeit:

- Redundante Auslegung aller Datensicherungs- und Datenbanksysteme sowohl in Hardware als auch in Software
- Summenprüfung zwecks Integritätssicherung der Datensicherungsverfahren
- Regelmäßige Tests der Wiederherstellbarkeit sowohl von Daten und Systemen als auch Services

5.3. Zuverlässigkeit

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

Beschreibung der Maßnahmen zur Zuverlässigkeit:

- Automatisches Monitoring mit InstantMessaging-Benachrichtigungen
- Recovery-Prozesse sind Tool- und Codegestützt. Diese unterliegen damit aller Qualitätssicherungen wie Code-Review Prozesse, Versionssicherheit und Dokumentation
- Notfallpläne mit Verantwortlichkeiten
- Klar definierte Zeitfenster für Wartungen sowie im Rahmen des Release-/Patch Managements
- Regelmäßige Tests

6. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

6.1. Überprüfungsverfahren

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

Beschreibung der Überprüfungsverfahren:

- Prüfung auf datenschutzkonforme und sichere Verarbeitung ist Bestandteil der Planungsprozesse, denen Implementierungen vorausgehen (Security by Design)
- Regelmäßige Prüfung und Dokumentation der Daten, Systeme und Services hinsichtlich des Bedarfs an Vertraulichkeit, Integrität und Verfügbarkeit
- Regelmäßige externe Prüfung durch Kunden
- Geschultes Personal sowie regelmäßige interne und sicherheitsbezogene Hackathons
- OLAs beinhalten Durchführung von Kontrollen
- Regelmäßige interne Revision sämtlicher datenschutzrelevanter Aspekte durch Datenschutzbeauftragten
- Regelmäßige Überprüfung der Zertifizierung aller Subdienstleister
- Formalisierte Prozesse für Datenschutzvorfälle
- Wesentliche Weisungen des Auftraggebers werden dokumentiert

6.2. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

Beschreibung der Maßnahmen zur Auftragskontrolle:

- Datenschutzgerechte Verträge nach Art. 28 DSGVO
- Auftragsdatenverarbeitungsmanagement
- Vertraglich fixierte Ansprechpartner
- Nur von weisungsberechtigten Personen des Auftraggebers werden Weisungen entgegengenommen.
- Zu allen Aktivitäten sind Aufträge des Auftraggebers vorhanden.
- Es kommen nur Subunternehmer zum Einsatz, die von Auftraggeber freigegeben sind.
- Es ist sichergestellt, dass datenschutzrechtliche Regelungen auch an Subunternehmer weitergegeben und von diesen eingehalten werden.
- Eingeschaltete Subunternehmer werden vom Auftragnehmer regelmäßig kontrolliert.

ANLAGE 2
Unterauftragsverhältnisse gemäß Ziff. 9 der Vereinbarung zur Auftragsverarbeitung

1. velia.net Internetdienste GmbH
Funktion/Tätigkeit: Dedicated-Server-Hosting
Sitz [Stadt, Land]: Hanau, Deutschland
Ort der Datenverarbeitung von personenbezogenen Daten: **Deutschland**
Vertragliche Maßnahmen/Garantien: Auftragsverarbeitung
Zertifikate: Der Colocation Space des Dienstleisters ist ISO 27001 zertifiziert.

2. Nexmo Inc. / Vonage
Funktion/Tätigkeit: PaaS für die Video- Audio- Screensharing Streaming Architektur
Sitz [Stadt, Land]: San Francisco, Vereinigte Staaten von Amerika (USA)
Ort der Datenverarbeitung von personenbezogenen Daten: **Deutschland**
Vertragliche Maßnahmen/Garantien: Auftragsverarbeitung, EU-Standardvertragsklauseln
Zertifikate: Das Datencenter ist ISO 27001, 27017 und 27018 zertifiziert.

3. Cronofy Ltd.
Funktion/Tätigkeit: PaaS zur Synchronisierung von Kalenderdaten
Sitz [Stadt, Land]: Nottingham, Vereinigtes Königreich
Ort der Datenverarbeitung von personenbezogenen Daten: **Deutschland**
Vertragliche Maßnahmen/Garantien: Auftragsverarbeitung
Zertifikate: Das Datencenter ist ISO 27001, 27017 und 27018 zertifiziert. Der Dienstleister ist ISO 27001 zertifiziert.

ANLAGE 3

Klärung zu Art der Daten, Verarbeitung durch Subdienstleister

Daten / Subdienstleister	Velia.net	Nexmo	Cronofy
Personenstammdaten	X		
Kontaktdaten (Telefon, E-Mail)	X		
Streaming der Kommunikationsdaten (Audio- und Videostreaming und Screensharing)		X	
(Optional) Speicherung der Kommunikationsdaten (Audio- und Videostreaming und Screensharing)	X	X	
Inhaltsdaten (geteilte Dateien, Textchat, Whiteboard-Inhalte)	X		
Signaturdaten (Charaktereigenschaften der digitalen Signatur)	X		
Vertragsdaten (zugrundeliegende rechtliche Dokumente bei digitaler Signatur)	X		
Kalenderdaten (Datum, Dauer, Verfügbarkeit)			X
Kalenderauthentifizierungsdaten			X
Metadaten / Analysedaten	X	X	
IP-Adresse	X	X	

ANLAGE 4
Klärung zu Art der Daten, Kreis der Betroffenen und Speicherort

Daten / Kreis der Betroffenen	Administrator	Experte	End-Kunde
Personenstammdaten	Deutschland	Deutschland	Deutschland
Kontaktdaten (Telefon, E-Mail)	Deutschland	Deutschland	Deutschland
Streaming der Kommunikationsdaten (Audio- und Videostreaming und Screensharing)		Deutschland	Deutschland
(Optional) Speicherung der Kommunikationsdaten (Audio- und Videostreaming und Screensharing)		Deutschland	Deutschland
Inhaltsdaten (geteilte Dateien, Textchat, Whiteboard-Inhalte)		Deutschland	Deutschland
Signaturdaten (Charaktereigenschaften der digitalen Signatur)		Deutschland	Deutschland
Vertragsdaten (zugrundeliegende rechtliche Dokumente bei digitaler Signatur)		Deutschland	Deutschland
Kalenderdaten (Datum, Dauer, Verfügbarkeit)	Deutschland	Deutschland	Deutschland
Kalenderauthentifizierungsdaten	Deutschland	Deutschland	
IP-Adresse	Deutschland	Deutschland	Deutschland
Metadaten mit Personenbezug	Deutschland	Deutschland	Deutschland

Legende:

Administrator: ist die Nutzerrolle, die über administrationsrechte der Plattform verfügt. Meistens ein Mitarbeiter des Auftraggebers sowie Mitarbeiter des Auftragnehmers.
Experte: ist die Nutzerrolle, die jeweils Online-Sitzungen veranstaltet und steuert. Meistens Mitarbeiter etc. des Auftraggebers, Vertriebspartner etc.
End-Kunde: ist die Nutzerrolle, die Sitzungen anfragt. Meistens Kunden des Auftraggebers

Ein leeres Feld hat die Bedeutung, dass keine Daten für diese Nutzerrolle gespeichert werden.