Allgemeine Geschäftsbedingungen zur Auftragsverarbeitung gemäß Art. 28 und 29 DSGVO (Anlage 2 zu den Allgemeine Geschäftsbedingungen Trendradar)

I. Allgemeines

Diese Anlage (im Folgenden „Auftragsverarbeitungsvertrag“) konkretisiert die Verpflichtungen zum Datenschutz, die sich aus dem vom Kunden abgeschlossenen Vertrag über das Produkt Trendradar (nachfolgend „**Hauptvertrag**“) ergeben.

Der Provider stellt dem Kunden eine Software as a Service Lösung (im Folgenden „**Anwendung**“) zur Unterstützung im Strategie- und Innovationsmanagement zur Verfügung. Gegenstand des Hauptvertrages ist überdies ein Service Level Agreement. Im Zuge der Lizenzierung, Softwarepflege, Wartung und Aktualisierung ist es unter Umständen erforderlich, dass der Provider personenbezogene Daten verarbeitet oder hierauf zugreifen kann, für die der Kunde im Sinne des Datenschutzrechts verantwortlich ist.

Für diese Verarbeitung von personenbezogenen Daten im Auftrag ist der Provider Auftragsverarbeiter im Sinne des § 4 Nr. 8 DSGVO (Im Folgenden „**Auftragsverarbeiter**“) und der Kunde verantwortliche Stelle des § 4 Abs. Nr 7 DSGVO (im Folgenden „**Verantwortlicher**“).

Der vorliegende Auftragsverarbeitungsvertrag ist nur gültig in Verbindung mit einem gültigen Hauptvertrag.

II. Wesentliche Inhalte der Auftragsverarbeitung

(1) Gegenstand der Verarbeitung

Der Auftragsverarbeiter stellt dem Verantwortlichen eine Software as a Service Lösung zur Unterstützung im Strategie- und Innovationsmanagement zur Verfügung. Die Bereitstellung der Anwendung erfolgt durch den Auftragsverarbeiter, die Nutzung der Anwendung erfolgt durch den Verantwortlichen.

- Gegenstand dieses Auftragsverarbeitungsvertrags ist die damit einhergehende Verarbeitung von personenbezogenen Daten des Verantwortlichen die im Rahmen der Anlage von Nutzern bzw. Nutzung der Anwendung bei Nutzung der Anwendung gespeichert und verarbeitet werden.
- Für die Durchführung des Hauptvertrages mit dem Verantwortlichen ist der Zugriff auf personenbezogene Daten durch den Auftragsverarbeiter notwendig.

(2) Dauer der Verarbeitung

Die Dauer der Verarbeitung richtet sich nach der Laufzeit des Hauptvertrags.

(3) Zweck und Art der Verarbeitung

Der Verantwortliche legt die Nutzer in der Anwendung an und verwaltet deren Zugriffsberechtigungen

Im Rahmen der Nutzung Anwendung können unter Umständen auch personenbezogene Daten eingegeben werden bei der Eingabe von Kommentaren oder Angaben im Nutzerprofil.

Im Rahmen der Auftragsverarbeitung soll der Auftragsverarbeiter die personenbezogenen Daten für folgende Zwecke verarbeiten:

(i) Verarbeitungen in Übereinstimmung mit der Durchführung des Hauptvertrages und dieses Auftragsverarbeitungsvertrages.

(ii) Verarbeitungen, damit der Verantwortliche die Anwendung nutzen kann;

(iii) Verarbeitungen, um die angemessene und dokumentierte Anweisung des Verantwortlichen bzgl. der Verarbeitung zu erfüllen, sofern die Anweisung mit den Bedingungen des Hauptvertrags übereinstimmen;

(iv) Verarbeitungen, die nach den für den Auftragsverarbeiter oder für den Verantwortlichen geltenden Gesetze erforderlich sind, sofern die Parteien sich gegenseitig informieren, es sei denn das Gesetz verbietet eine solche Information aufgrund gewichtiger Gründe des öffentlichen Interesses.

(4) Art der personenbezogenen Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten:

- Es werden Personenstammdaten und Kommunikationsdaten verarbeitet, nämlich: Name, Vorname, Mailadresse (Log-in-Daten und im Rahmen der Nutzung der Anwendung) von Beschäftigten des Verantwortlichen)
- Es werden besondere personenbezogene Daten verarbeitet, nämlich: keine

(5) Kategorien der von der Datenverarbeitung betroffenen Personen

- Beschäftigte des Verantwortlichen,

(6) Anonyme Informationen

„Anonyme Informationen" sind Informationen, die keine Identifizierung einer Person ermöglichen, wie z. B. zusammengefasste und analytische Informationen. Die Verarbeitung von anonymen Informationen stellt keine Verarbeitung von personenbezogenen Daten im Sinne der Datenschutzgesetze dar. Der Auftragsverarbeiter ist berechtigt, anonyme Informationen in Bezug auf die Nutzung der Anwendung zum Zweck der Bereitstellung, Verbesserung und Bekanntmachung der Produkte und Services des Auftragsverarbeiters sowie für andere Geschäftszwecke zu sammeln und zu verwenden, weiterzugeben und zu veröffentlichen.

(7) Ort der Verarbeitung

Die Verarbeitung von Daten erfolgt ausschließlich innerhalb der Europäischen Union. Eine Datenverarbeitung in Ländern, die nicht Mitgliedstaat der Europäischen Union sind (nachfolgend „Drittstaaten"), darf nur unter der weiteren Bedingung erfolgen, dass die Voraussetzungen der Artikel 44, 45, 46 oder Artikel 49 DSGVO erfüllt sind.

III. Verarbeitung auf Weisung

(1) Grundsatz

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf (durch den Hauptvertrag, diesen Auftragsverarbeitungsvertrag oder individuell) erteilte Weisung des Verantwortlichen, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche hat das Recht, jederzeit ergänzende Weisungen zu erteilen. Mündliche Weisungen wiederholt der Verantwortliche unverzüglich in Textform.

(2) Erteilung und Empfang von Weisungen

Der Verantwortliche hat zu Vertragsbeginn einzelne zur Weisung befugte Personen in Textform (per E-Mail) zu benennen.

Für den Fall, dass sich die weisungsberechtigte(n) Person(en) beim Verantwortlichen ändern, wird der Verantwortliche dies dem Auftragsverarbeiter unverzüglich in Textform (Per E-Mail) mitteilen.

Zur Entgegennahme von Weisungen berechtigte Personen auf Seiten des Auftragsverarbeiters ist der jeweiligen Geschäftsführer.

Für den Fall, dass sich die zum Empfang von Weisungen berechtigte(n) Person(en) beim Auftragsverarbeiter ändern, wird der Auftragsverarbeiter dies dem Verantwortlichen unverzüglich in Textform (per E-Mail) mitteilen.

(3) Dokumentationspflicht
Der Auftragsverarbeiter hat die Weisung des Verantwortlichen hinreichend zu dokumentieren. Die elektronische Form der Dokumentation genügt.

(4) Informationspflicht bei Zweifeln an der Rechtmäßigkeit der Weisung
Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darüber informieren, wenn eine vom Verantwortlichen erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Die Beurteilung der Zulässigkeit der Datenverarbeitung durch den Verantwortlichen ist für den Auftragsverarbeiter bindend. Der Auftragsverarbeiter und der Verantwortliche haften einander für Schäden, die ihnen aus einer Durchführung oder einer Aussetzung der Durchführung entstehen, die auf einer rechtlichen Fehleinschätzung der anderen Partei beruht.

IV. Verpflichtung zur Vertraulichkeit und zur Einhaltung des Datenschutzes

(1) Der Auftragsverarbeiter setzt bei der Durchführung der Leistungen nur Beschäftigte ein, die entweder vertraglich zur Vertraulichkeit verpflichtet wurden oder gesetzlich zur Verschwiegenheit verpflichtet sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

(2) Der Auftragsverarbeiter versichert, nur Mitarbeiter einzusetzen, die zur Wahrung von Geschäftsgeheimnissen des Auftraggebers verpflichtet wurden und auf § 23 GeschGehG hingewiesen wurden.

(3) Sofern einschlägig versichert der Auftragsverarbeiter, nur Mitarbeiter einzusetzen, die auf die Wahrung des Fernmeldegeheimnisses entsprechend § 88 TKG verpflichtet wurden, sofern die Mitarbeiter des Auftragsverarbeiters – auftragsgemäß – auf Daten des Auftraggebers mittels Mittel der Telekommunikation wie Telefon oder E-Mail zugreifen können. Der Auftragsverarbeiter sichert in diesen Fällen auch zu, dass die eingesetzten Mitarbeiter auf die sich daraus ergebenden besonderen Geheimhaltungspflichten belehrt wurden.

V. Sicherheit der Datenverarbeitung

(1) Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos im Sinne von Artikel 32 Abs. 1 DSGVO zu berücksichtigen. Die konkreten technischen und organisatorischen Maßnahmen werden in Anlage 2.1 aufgelistet. Sie unterliegen dem technischen Fortschritt und der Weiterentwicklung.

(2) Wesentliche Änderungen, die die Integrität, Vertraulichkeit, Belastbarkeit oder Verfügbarkeit der Maßnahmen beeinträchtigen können, bedürfen der Zustimmung des Verantwortlichen. Der Verantwortliche darf die Zustimmung nicht unbillig verweigern. Das durch die mit diesem Vertrag vereinbarten Maßnahmen gewährleistete Schutzniveau darf nicht unterschritten werden. Änderungen sind hinreichend zu dokumentieren. Der Verantwortliche kann jederzeit eine aktuelle Beschreibung der vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen anfordern.

VI. Unterauftrag

(1) Inanspruchnahme von Unterauftragnehmern

Der Auftragsverarbeiter darf weitere Auftragsverarbeiter in Anspruch nehmen. Der Auftragsverarbeiter hat den Verantwortlichen mindestens vier Wochen vorher über jede Inanspruchnahme oder Ersetzung eines weiteren Auftragsverarbeiters in Textform (per E-Mail) zu informieren. Der Verantwortliche kann der Inanspruchnahme

oder Ersetzung eines weiteren Auftragsverarbeiters ohne Nennung eines Grundes binnen einer Frist von zwei Wochen ab Zugang der Information des Auftragsverarbeiters in Textform widersprechen.

Widerspricht der Verantwortliche, ist es dem Auftragsverarbeiter gestattet, den Auftragsverarbeitungsvertrag und den Hauptvertrag fristlos zu kündigen.

Die in der Anlage 2.2 benannten „weiteren Auftragsverarbeiter“ sind zum Zeitpunkt des Vertragsabschlusses zur Erbringung der Auftragsverarbeitung beauftragt.“

(2) Modalitäten des Unterauftrags

Der Auftragsverarbeiter darf weitere Auftragsverarbeiter nur in Anspruch nehmen, wenn diese in demselben Umfang vertraglich gegenüber dem Auftragsverarbeiter zur Einhaltung des Datenschutzes verpflichtet sind, wie der Auftragsverarbeiter gegenüber dem Verantwortlichen aus diesem Vertrag. Der Vertrag zwischen dem Auftragsverarbeiter und dem weiteren Auftragsverarbeiter muss insbesondere hinreichende Garantien dafür bieten, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Der Auftragsverarbeiter hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

Der Auftragsverarbeiter hat den weiteren Auftragsverarbeiter sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen dem Verantwortlichen und dem Auftragsverarbeiter getroffenen Vereinbarungen einhalten kann. Der Auftragsverarbeiter hat sich insbesondere vorab und regelmäßig während der Vertragsdauer zu vergewissern, dass der weitere Auftragsverarbeiter die nach den Vorgaben der DSGVO 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.

(3) Abgrenzung

Nicht als Unterauftragsverhältnisse sind Dienstleistungen anzusehen, die der Auftragsverarbeiter bei Dritten als reine Nebenleistung in Anspruch nimmt, um seine geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der

Auftragsverarbeiter für den Verantwortlichen erbringt, Post- und Kurierdienste, Transportleistungen und Bewachungsdienste. Der Auftragsverarbeiter ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen getroffen wurden, um den Schutz personenbezogener Daten des Verantwortlichen zu gewährleisten. Wartungs- und Pflegeleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit die Wartung und Prüfung solche IT-Systeme betreffen, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen aus diesem Vertrag genutzt werden.

VII. Unterstützung des Verantwortlichen bei der Erfüllung von Betroffenenrechten

(1) Soweit eine Mitwirkungsleistung des Auftragsverarbeiters für die Wahrung von Betroffenenrechten durch den Verantwortlichen erforderlich ist, wird der Auftragsverarbeiter den Verantwortlichen nach Möglichkeit mit den ihm zur Verfügung stehenden Informationen unterstützen.

(2) Der Auftragsverarbeiter haftet nicht, wenn das Ersuchen der betroffenen Person vom Verantwortlichen nicht richtig oder nicht fristgerecht beantwortet wird und der Auftragsverarbeiter dies nicht zu verschulden hat. Der Verantwortliche stellt den Auftragsverarbeiter insoweit von jeglichen Ansprüchen Dritte frei, gleich ob mittelbar oder unmittelbar durch das nicht richtig oder nicht fristgerecht beantworte Ersuchen bedingt.

(3) Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragsverarbeiter geltend machen.

VIII. Unterstützung des Verantwortlichen bei der Erfüllung eigener Pflichten

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der der dem Auftragsverarbeiter zur Verfügung stehenden Informationen dabei, die dem Verantwortlichen obliegenden Pflichten,

- ein dem Risiko angemessenes Schutzniveau zu gewährleisten,
- die Verletzung des Schutzes personenbezogener Daten an Aufsichtsbehörden unverzüglich und möglichst binnen 72 Stunden zu melden,

- den in Bezug auf eine Verletzung Betroffenen zu benachrichtigen,
- eine Datenschutz-Folgenabschätzung durchzuführen und ggf. vor Verarbeitung die zuständige Aufsichtsbehörde zu konsultieren,

zu erfüllen.

(2) Der Auftragsverarbeiter wird den Verantwortlichen von auftragsbezogenen Störungen im Betriebsablauf, Verletzungen von Datenschutzbestimmungen (auch durch Weisungen des Verantwortlichen), Kontrollen und Maßnahmen der Aufsichtsbehörden und anderen Unregelmäßigkeiten unverzüglich unterrichten.

(3) Der Verantwortliche und der Auftragsverarbeiter arbeiten gem. Artikel 31 DSGVO auf Anfrage der Aufsichtsbehörde mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(4) Der Auftragsverarbeiter wirkt bei der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten im Sinne von Artikel 30 Abs. 1 DSGVO durch den Verantwortlichen mit und wird dem Verantwortlichen die dafür benötigten Informationen – soweit möglich und bei dem Auftragsverarbeiter vorhanden - bereitstellen. Insbesondere wird er dem Verantwortlichen einen Auszug aus seinem Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 Abs. 2 DSGVO mitteilen, damit dieser sein Verzeichnis von Verarbeitungstätigkeiten erstellen kann.

(5) Ferner wird der Auftragsverarbeiter den Verantwortlichen – sofern rechtlich zulässig – unverzüglich darüber informieren, wenn eine Aufsichtsbehörde bei dem Auftragsverarbeiter Kontrollhandlungen oder Maßnahmen unternimmt, die sich auf diese Auftragsverarbeitung beziehen.

(6) Für diejenigen Aufwände, die dem Auftragsverarbeiter durch die Erbringung von Unterstützungs- oder Dokumentationsleistungen nach den vorstehenden Ziffern 7 und 8.1, 8.3, 8.4 Satz 1 dieses Auftragsverarbeitungsvertrages für den Verantwortlichen entstehen, steht dem Auftragsverarbeiter ein Anspruch auf Zahlung der für die Leistungserbringung vereinbarten üblichen Vergütung zu, der sich aus der Preisliste des Auftragsverarbeiters ergibt.

IX. Löschung und Rückgabe

(1) Der Auftragsverarbeiter hat nach Abschluss der Erbringung der Verarbeitungsleistungen die personenbezogenen Daten sowie Unterlagen, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Verantwortlichen entweder datenschutzgerecht zu löschen oder zurückzugeben, sofern der Verantwortliche die Daten nicht selbständig mit Hilfe der Anwendung abrufen oder löschen kann oder sofern nicht nach

dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung bzw. Aufbewahrung besteht. Dies gilt nicht für anonyme Informationen (Ziffer 2.6). Dies betrifft auch etwaige Datensicherungen beim Auftragsverarbeiter. Der Auftragsverarbeiter hat die Löschung in geeigneter Weise zu dokumentieren. Bestehen gesetzliche Aufbewahrungspflichten, hat die Löschung der Daten nach Ende der Aufbewahrungspflicht zu erfolgen.

(2) Vor Abschluss der Erbringung der Vertragsleistungen darf der Auftragsverarbeiter nicht mehr benötigte Daten erst nach vorheriger Zustimmung durch den Verantwortlichen löschen, es sei denn es sind vertraglich frühere Löschfristen festgelegt.

(3) Der Verantwortliche hat das Recht, die vollständige und vertragsgemäße Rückgabe oder Löschung der Daten beim Auftragsverarbeiter zu kontrollieren. Dies kann auch nach vorheriger Anmeldung mit angemessener Frist durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragsverarbeiters erfolgen.

X. Ermöglichung von Kontrollen und Zurverfügungstellung von Informationen

(1) Der Verantwortliche hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen, um die Einhaltung der gesetzlichen Vorschriften zum Datenschutz, der zwischen den Vertragsparteien getroffenen vertraglichen Regelungen und der Weisungen des Verantwortlichen durch den Auftragsverarbeiter jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragsverarbeiter ist dem Verantwortlichen gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle erforderlich ist.

(3) Der Verantwortliche kann eine Einsichtnahme in die vom Auftragsverarbeiter für den Verantwortlichen verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen. Der Verantwortliche kann hierzu nach vorheriger Anmeldung mit angemessener Frist die Kontrolle in der Betriebsstätte des Auftragsverarbeiters zu den jeweils üblichen Geschäftszeiten vornehmen. Der Verantwortliche wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragsverarbeiters durch die Kontrollen nicht unverhältnismäßig zu stören.

(4) Für diejenigen Aufwände, die dem Auftragsverarbeiter durch die Erbringung von Unterstützungs- oder Dokumentationsleistungen nach den vorstehenden Ziffern 10.1 – 10.3 entstehen, steht dem Auftragsverarbeiter ein Anspruch auf Zahlung der für die Leistungserbringung vereinbarten üblichen Vergütung zu.

(5) Der Auftragsverarbeiter kann die Einhaltung der technischen und organisatorischen Maßnahmen durch geeignete Bestätigungen, wie z. B. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheits-abteilung, Datenschutzauditoren, Qualitätsauditoren), nachweisen.

XI. Kündigung

Die Kündigung richtet sich nach dem Hauptvertrag.

XII. Schlussbestimmungen

(1) Sollte das Eigentum des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu informieren. Der Auftragsverarbeiter wird die Gläubiger über die Tatsache, dass es sich um personenbezogene Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Erweiterungen und Änderungen dieses Auftragsverarbeitungsvertrages sind zu Ihrer Wirksamkeit schriftlich zu formulieren und nur wirksam, wenn beide Vertragsparteien zustimmen. Die Wahrung der Textform reicht aus.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

(4) Die Regelungen des Hauptvertrags bezüglich Rechtswahl und Wahl des zuständigen Gerichts für Rechtsstreitigkeiten gelten auch für diese Vereinbarung.

Dieser Vertrag wird elektronisch geschlossen und ist ohne Unterschrift gültig.

Anlagenverzeichnis:

- Anlage 2.1: TOM’s
- Anlage 2.2: Unterauftragsverarbeiter Stand Abschluss des Auftragsverarbeitungsvertrages

Anlage 2.1 zu den Allgemeinen Geschäftsbedingungen Auftragsverarbeitungsvertrag: Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

Die technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO werden einerseits durch den Auftragsdatenverarbeiter gewährleistet und andererseits durch die ITONICS GmbH, Emilienstr. 9, 90489 Nürnberg („Der Anwendungs-Lizenzierende“). von der der Auftragsanbieter die Anwendung über seine Unternehmensmutter, die Evangelische Bank eG, Ständeplatz 19, 34117 Kassel, bereitgestellt bekommt.

Der Zugriff auf die personenbezogenen Daten des Verantwortlichen erfolgt ausschließlich über Arbeitsplatzrechner des Auftragsverarbeiters bzw. im Falle des Supports und der Wartung über die Arbeitsplatzrechner seiner Unterauftragsverarbeiter (Anlage 2.2).

I. Maßnahmen zur Gewährleistung der Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

(1) Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

a) Zutrittskontrolle durch den Anwendungs-Lizenzierenden

Die Zutrittskontrolle beinhaltet nach eigenen Angaben des Anwendungs-Lizenzierenden das Folgende:

- Schlüssel-Verwaltung mit dokumentierter Schüsselvergabe
- Türsicherung (elektrischer Türöffner usw.)
- Alarmanlage, Videoüberwachung
- Definition von Sicherheitszonen und Ladezonen und Handlungsanweisungen an Mitarbeiter

b) Zutrittskontrolle durch den Auftragsverarbeiter

Die personenbezogenen Daten des Verantwortlichen werden auf Servern des Anwendungs-Lizenzierenden bzw. von diesem Beauftragten verarbeitet.

Eine Kontrolle des Zutritts findet beim Auftragsverarbeiter durch folgende Maßnahmen statt.

Bürogebäude Ständeplätz 19, 34117 Kassel

Technische Maßnahmen	Organisatorische Maßnahmen
☒Manuelles Schließsystem	☒Empfang mit Anmeldung und Besuchsregistrierung
☒Sicherheitstüren und -schlösser	☒Schlüsselchipregelung / Schlüsselchipliste, Schlüsselchipausgabe
☐Biometrische Zugangssperren	☒Protokollierung der Besucher
☒Chipkarten-/Transponder-Schließsystem	☒Sorgfältige Auswahl von Sicherheitspersonal
☒Lichtschranken / Bewegungsmelder	☒ Funktions- und rollenbasierte Zutrittsberechtigungen für Serverraum
☒Schließsystem mit Codesperre	☒Videoüberwachung der Zugänge

Bürogebäude Hardenbergstr. 32, 10623 Berlin

Technische Maßnahmen	Organisatorische Maßnahmen
☒Manuelles Schließsystem	☐Empfang mit Anmeldung und Besuchsregistrierung
☒Sicherheitstüren und -schlösser	☒Schlüsselchipregelung / Schlüsselchipliste, Schlüsselchipausgabe
☐Biometrische Zugangssperren	☐Protokollierung der Besucher

☒Chipkarten-/Transponder-Schließsystem	☒Sorgfältige Auswahl von Sicherheitspersonal
☒Lichtschranken / Bewegungsmelder	☐ Funktions- und rollenbasierte Zutrittsberechtigungen für Serverraum
☒Schließsystem mit Codesperre	☐Videoüberwachung der Zugänge

(2) Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

a) Zugangskontrolle durch den Anwendungs-Lizenzierenden

Die Zugangskontrolle beinhaltet nach eigenen Angaben des Anwendungs-Lizenzierenden das Folgende:

- Kennwortverfahren (u. a. Sonderzeichen, Mindestlänge, regelmäßige Wechsel des Kennworts, Richtlinie für Passwortkomplexität)
- Automatische Sperrung (z. B. Auto-Logout)
- Einrichtung eines Benutzerstammsatzes pro User
- Verschlüsselung von Datenträgern
- Zwei-Faktor-Authentifizierung

b) Zugangskontrollen durch den Auftragsverarbeiter

Auf Seiten des Auftragsverarbeiters findet der Zugriff auf die Anwendung über Arbeitsplatzrechner statt. Es wurden folgende Maßnahmen zur Zugangskontrolle getroffen:

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒Authentifikation mit Benutzer und Passwort	☒Benutzerberechtigungen verwalten
☒Einsatz von Anti-Viren-Software	☒Erstellen von Benutzerprofilen

☐Einsatz von VPN-Technologie	☒Passwortvergabe / Passwortregeln
☒Verschlüsselung von Smartphones	☒Sorgfältige Auswahl des Reinigungspersonals (Unterauftragsverarbeiter zu 1. bzgl. Bürogebäude in Kassel, eigene Auswahl für Bürogebäude in Berlin)
☐Sperren von externen Schnittstellen (z.B. USB-Anschlüsse)	
☐Verschlüsselung von Datenträgern	

(3) Zugriffskontrolle

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

a) Zugriffskontrolle durch den Anwendungs-Lizenzierenden

Die Zugriffskontrolle beinhaltet nach eigenen Angaben des Anwendungs-Lizenzierenden das Folgende:

- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen, Objekte)
- Definierte Freigabeprozesse für Zugriffsberechtigungen
- Verschlüsselung der Daten

b) Zugriffskontrolle durch den Auftragsverarbeiter

Folgende Maßnahmen wurden vom Auftragsverarbeiter zur Zugriffskontrolle getroffen:

Technische Maßnahmen	**Organisatorische Maßnahmen**

☒ Funktions- und rollenbasiertes Berechtigungskonzept	☒Erstellen eines Berechtigungskonzepts für die Anwendung
☐Verschlüsselung von Datenträgern (auch mobilen) bei dem Unterauftragsverarbeiter zu 1.	☒Anzahl der Administratoren in der Anwendung auf das „Notwendigste“ reduzieren
☒Protokollierung von Zugriffen auf die Anwendung, insbesondere bei der Eingabe, Änderung und Löschung von Daten	☒Verwaltung der Benutzerrechte durch Systemadministratoren in der Anwendung
☐Verschlüsselung von Daten in der Anwendung	☐Regelung von Zugriffsberechtigung auf Daten
	☒Regelung zum Entzug von Zugriffsberechtigungen
	☒Passwortvorgaben inkl. Länge
	☒Einsatz von Dienstleistern zur Akten- und Datenvernichtung
	☒Ordnungsgemäße Vernichtung von Datenträgern

II. Maßnahmen zur Gewährleistung der Integrität gem. Art. 32 Abs. 1 lit. b DSGVO

(1) Weitergabekontrolle

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

a) Weitergabekontrolle durch den Anwendungs-Lizenzierenden
Die Weitergabekontrolle beinhaltet nach eigenen Angaben des Anwendungs-Lizenzierenden das Folgende:

- Verschlüsselung / VPN-Tunnelverbindungen
- Elektronische Signatur
- Protokollierung
- Transportsicherung

b) Weitergabekontrolle durch den Auftragsverarbeiter
Die bereitgestellte Anwendung stellt sicher, dass die Kommunikation stets über ein kryptografisches Verschlüsselungsverfahren mit aktuellen Sicherheitsstandards erfolgt. Ein gesicherter physischer Transport von Daten findet nicht statt. Sofern gewünscht oder erforderlich kann der E-Mail-Transport verschlüsselt werden.

Der Auftragsverarbeiter hat zudem folgende Maßnahmen zur Weitergabekontrolle getroffen:

Technische Maßnahmen	**Organisatorische Maßnahmen**
☐Einsatz von Firewall (s.o.)	☒Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

(2) Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

a) Eingabekontrolle durch den Anwendungs-Lizenzierenden
Die Eingabekontrolle beinhaltet nach eigenen Angaben des Anwendungs-Lizenzierenden das Folgende:

- Protokollierungs- und Protokollauswertungssysteme

b) Eingabekontrolle durch den Auftragsverarbeiter
Der Auftragsverarbeiter hat folgende Maßnahmen getroffen:

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
	☒ Protokollierung der Systemzugriffe und der Eingaben und Änderungen
	☒ Eingabe, Änderung oder Löschung von Daten erfolgt nach dokumentierter ausdrücklicher Weisung des Verantwortlichen
	☒Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

III. Weisungsgebundene Verarbeitung der Daten

(1) Auftragskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

a) Auftragskontrolle durch den Anwendungs-Lizenzierenden
Die Auftragskontrolle beinhaltet nach eigenen Angaben des Anwendungs-Lizenzierenden das Folgende:

- Eindeutige Vertragsgestaltung
- Formalisiertes Change-Management

- Lieferantenmanagement und Risikobewertung
- Nachkontrollen durch interne und externe Auditierung

b) Auftragskontrolle durch den Auftragsverarbeiter

Der Auftragsverarbeiter stellt dem Verantwortlichen mit der Anwendung Funktionalitäten zur Verfügung, mit denen der Verantwortliche personenbezogene Daten selbständig bearbeiten, ändern, einsehen und löschen kann, ohne den Auftragsverarbeiter anzuweisen, ausgenommen Benutzerdaten.

Sofern der Auftragsverarbeiter bei Anlage von Konten, Lizensierung der Anwendung, Wartung und Pflege der Anwendung personenbezogene Daten im Auftrag verarbeitet, erfolgt dies auf Basis des vorliegenden Auftragsverarbeitungsvertrags. Weisungen und durchzuführende Änderungen werden schriftlich dokumentiert, offene Fragen werden geklärt.

Der Auftragsverarbeiter setzt bezüglich der Entwicklung, Wartung und Pflege der Anwendung Unterauftragsverarbeiter ein.

Folgende Maßnahme werden diesbezüglich von dem Auftragsverarbeiter getroffen:

Technische Maßnahmen	**Organisatorische Maßnahmen**
	☒Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
	☒Laufende Überprüfung der Auftragnehmer und seiner Tätigkeiten
	☒Weisungen in Text- oder Schriftform an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. Art. 28 DSGVO

	☒Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags Verpflichtung der Mitarbeiter der Auftragnehmer auf das Datengeheimnis
	☒Vorherige Prüfung der bei einem Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation
	☒Wirksame Kontrollrechte gegenüber Auftragnehmern vereinbaren

IV. Gewährleistung der Verfügbarkeit gem. Art. 32 Abs. 1 lit. b, c DSGVO:

(1) Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

a) Verfügbarkeitskontrolle durch den Anwendungs-Lizenzierenden
Die Verfügbarkeitskontrolle beinhaltet nach eigenen Angaben des Anwendungs-Lizenzierenden das Folgende:

- Spiegeln von Festplatten, z. B. RAID-Verfahren
- Virtualisierungstechniken
- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte Aufbewahrung von Datenkopien
- Virenschutz, Firewall
- Definierte Testverfahren zu Leistung und Kapazität
- Permanente Überwachung der Verfügbarkeit, Kapazität sämtlicher Kundensysteme durch technische Überwachungseinrichtungen
- Backup/Restore Verfahren
- Notfallplan und Testpläne
- Datenspiegelung zwischen Rechenzentren
- Virtualisierungstechniken

b) Verfügbarkeitskontrolle durch Auftragsverarbeiter
Folgende Maßnahmen wurden vom Auftragsverarbeiter getroffen:

Technische Maßnahmen	**Organisatorische Maßnahmen**
☐Feuerlöschgeräte in Serverräumen	☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort (bei dem Anwendungs-Lizenzierenden)
☒Feuer- und Rauchmeldeanlagen	☐Erstellen eines Backup- & Recovery-konzepts
☐Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	☐Erstellen eines Notfallplans
☐Klimaanlage in Serverräumen	☐Testen von Datenwiederherstellung
☐Schutzsteckdosenleisten in Serverräumen	
☐Unterbrechungsfreie Stromversorgung (USV)	

(2) Trennungsgebot und Zweckbindungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden

a) Zweckbindungskontrolle durch den Anwendungs-Lizenzierenden
Die Zweckbindungskontrolle beinhaltet nach eigenen Angaben des Anwendungs-Lizenzierenden das Folgende:

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Einsatz mandantenfähiger Software

- Getrennte Systeme für Entwicklung, Test und Produktion
- Virtuell getrennte Produktionssysteme

b) Zweckbindungskontrolle durch den Auftragsverarbeiter

Die vom Auftragsverarbeiter zur Verfügung gestellte Anwendung ist für die Verwendung durch verschiedenste Unternehmen/Kunden konzipiert und implementiert worden, so dass von Beginn an die Mandantenfähigkeit (Abtrennung der Daten in getrennte Bereiche) gewährleistet wurde.

Die Benutzerkonten sind verschiedenen Nutzerkreisen (Kunden) zugewiesen. Eine Eingabe oder das Bearbeiten von Daten von Kunden anderer Nutzerkonten ist aufgrund der Softwarearchitektur nicht möglich und wurde während der Programmierung der Software sichergestellt. Es findet eine Trennung von Produktiv-, und Testsystem statt. Es findet eine Festlegung von rollenbasierten Datenbankrechten statt.

Es wurden darüber hinaus folgende Maßnahmen getroffen:

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒Trennung von Produktiv- und Testsystem Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden	☒Erstellung eines Berechtigungskonzepts
	☒Festlegung von Datenbankrechten
	☒Logische Mandantentrennung (softwareseitig) Versehen der Datensätze mit Zweckattributen/Datenfeldern

V. Gewährleistung der Belastbarkeit der Systeme und Dienste gem. Art. 32 Abs. 1 lit. b DSGVO

Systeme sind belastbar, wenn sie so widerstandsfähig, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.

(a) Maßnahmen zur Widerstandsfähigkeit und Ausfallsicherheit durch Anwendungs-Lizenzierenden

Die Widerstandsfähigkeit und Ausfallsicherheit beinhalten nach eigenen Angaben des Anwendungs-Lizenzierenden das Folgende:

- Monitoringsysteme
- Skalierbarkeit virtueller Systemumgebungen
- Codeoptimierungen

(b) Maßnahmen zur Belastbarkeit durch Auftragsverarbeiter

Zudem hat der Auftragsverarbeiter folgende Maßnahmen getroffen:

Technische Maßnahmen	**Organisatorische Maßnahmen**
☐ Um Ausfällen vorzubeugen, werden umfangreiche Berechnungen oder große Mengen von Anfragen auf mehrere parallel arbeitenden Systeme verteilt	☐ Es besteht ein Prozess zur Vorbereitung auf Sicherheitsverletzungen und Systemstörungen sowie zur Identifizierung, Eingrenzung, Beseitigung und Erholung von selbigen (Incident-Response-Prozess)
☒Regelmäßige Anpassung der Anwendung an den Stand der Technik	☐Dokumentierte Vorgehensweise zum Umgang mit Datenpannen und Sicherheitsvorfällen (ITONICS GmbH)
	☒Dokumentation und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

	☒Updates und Patches werden softwareseitig über die Anwendung rechtzeitig eingespielt

VI. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d DSGVO:

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

(a) Verfahren des Anwendungs-Lizenzierendens
Der Hosting-Anbieter wendet nach eigenen Angaben die folgenden Verfahren zur Überprüfung, Bewertung und Evaluierung an:

- Datenschutz-Management
  Ein systematischer Management Ansatz stellt sicher, dass die vorhandenen Regelungen umgesetzt und kontinuierlich verbessert werden:
  - Regelmäßige Unterweisung und Online- Trainings aller Mitarbeiter zu Datenschutz und Informationssicherheit
  - Führen eines internen Handbuchs zum Datenschutz und zur Informationssicherheit
  - Dokumentenlenkung und klare Verantwortlichkeiten in allen Funktionsbereichen
  - Regelmäßige Überprüfung der Wirksamkeit von technischen und organisatorischen Maßnahmen

- Incident-Response-Management
  Maßnahmen, die eine zeitnahe Reaktion und das Einleiten von Gegenmaßnahmen bei Störungen des Datenschutzes, gewährleisten:
  - Definierter interner Prozess bei Datenschutzverstößen
  - Einbeziehung eines externen Datenschutzbeauftragten und interner Datenschutzkoordinatoren
  - Definierte Meldeprozesse zu den Datenschutzkontakten von Kunden

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
  Maßnahmen, die die Verarbeitung auf den jeweiligen Verarbeitungszweck beschränken:
  - Datenschutz und -sicherheit werden in der Planung, Design und Entwicklung von IT-Systemen berücksichtigt
  - Verankerung von Datenschutz in den Entwicklungs- und Implementierungsprozessen
  - Löschkonzepte
  - Rechte und Rollenkonzepte
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung imSinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers:
  - Eindeutige Vertragsgestaltung
  - Formalisiertes Change-Management
  - Lieferantenmanagement und Risikobewertung
  - Nachkontrollen durch interne und externe Auditierung

(b) Verfahren des Auftragsverarbeiters
Es werden folgende Maßnahmen getroffen:

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒Festgelegte Prüfroutine	☒Evaluation von Prüfungsberichten/Revision
☒Datenschutzfreundliche Voreinstellungen	☒Auftragsverarbeitung nur mit entsprechender Weisung des Auftraggebers
	☒Auftragskontrolle
	☒Datenschutz-Management

Anlage 2.2 zu den Allgemeinen Geschäftsbedingungen Auftragsverarbeitungsvertrag: Weitere Auftragsverarbeiter

Folgende „weitere Auftragsverarbeiter“ sind zum Zeitpunkt des Vertragsabschlusses zur Erbringung der Auftragsverarbeitung beauftragt:

1. Evangelische Bank eG, Ständeplatz 19, 34117 Kassel
2. ITONICS GmbH, Emilienstr. 9, 90489 Nürnberg