Vertrag über die Auftragsverarbeitung

der

TerminApp GmbH

Balanstr.73, Building 24, München

nachfolgend: „**TerminApp**“ genannt

Revision am	durch	Vermerk
01.01.2020	TerminApp	Turnusmäßige Überprüfung der technischen und organisatorischen Maßnahmen für den Auftraggeber

Präambel

Im Rahmen der Zusammenarbeit mit dem Kunden (Auftraggeber) und der Bereitstellung der Terminbuchungslösung erhält TerminApp Zugriff auf personenbezogene Daten des Auftraggebers. Um diesen Vorgang datenschutzkonform zu gestalten, schließen die Parteien nachfolgende Vereinbarung über die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten des Auftraggebers.

1. Gegenstand und Dauer des Vertrages

1.1 Gegenstand dieses Vertrages ist die Regelung und Konkretisierung der datenschutzrechtlichen Rechte und Pflichten der Vertragspartner, die sich aus dem Geschäftsverhältnis (Auftrag) mit dem Auftraggeber im Zusammenhang mit der Bereitstellung, Anpassung und Pflege der TIMIFY-Anwendungen ergeben.

1.2 Die Dauer dieses Vertrages sowie Kündigungsfristen entsprechen den Regelungen des zugrundeliegenden Auftrags. Mit Beendigung und/oder Kündigung des Vertragsverhältnisses, bzw. des letzten abgeschlossenen Einzelauftrags, endet auch dieser Vertrag über die Auftragsverarbeitung automatisch, ohne dass es einer gesonderten Kündigung bedarf.

1.3 Das Recht, diesen Vertrag ohne die Einhaltung einer Frist (fristlos) außerordentlich zu kündigen, weil auf Grund der Schwere und der Bedeutung einer erfolgten Pflichtverletzung ein Festhalten am Vertrag nicht zumutbar ist, insbesondere im Falle eines schwerwiegenden Verstoßes gegen Datenschutzvorschriften, bleibt für beide Parteien unberührt.

2. Art und Zweck der Verarbeitung

Der Zweck der Verarbeitung liegt in der Bereitstellung von Terminbuchungslösungen und Softwareapplikationen, einschließlich deren Wartung (Pflege) und Weiterentwicklung, dem Customizing sowie die damit einhergehenden Supportleistungen.

3. Kategorien der betroffenen Personen

Gegenstand der Verarbeitung sind folgende Kategorien von Personen:

Betroffene Personengruppen (Definitionen gemäß/siehe Timify-Datenschutzkonzeption)						
☐	KbP 1.1	Dienstleister	☐	KbP 1.4	Terminbucher	

4. Art der personenbezogenen Daten

Gegenstand der Verarbeitung sind folgende Datenkategorien:

KbP 1.1 – Dienstleister (Definitionen gemäß/siehe Timify-Datenschutzkonzeption)								
☐	KpD 2.1	IP-Adresse	☒	KpD 2.2	E-Mail-Adresse	☒	KpD 2.3	Vorname
☒	KpD 2.4	Nachname	☒	KpD 2.5	Anschrift (Adresse)	☒	KpD 2.6	Rechnungsadresse
☐	KpD 2.7	Buchungs-Details	☐	KpD 2.8	Lieferanschrift	☒	KpD 2.9	Konto-/Kreditkartennummern
☐	KpD 2.10	Bonitätsdaten	☒	KpD 2.11	Kundennummer	☒	KpD 2.12	Telefonnummern
☐	KpD 2.13	Bestellnummer	☒	KpD 2.14	Ticketnummer (contact_in)	☐	KpD 2.15	Werbe-IDs
☐	KpD 2.16	Geburtstag	☐	KpD 2.17	Geburtsort/-land	☐	KpD 2.18	Cookie-Kennung
☐	KpD 2.19	Personalnummer	☐	KpD 2.20	Sozialversicherungsdaten	☐	KpD 2.21	Familienstand
☐	KpD 2.22	Zeugnisse	☐	KpD 2.23	Lebenslauf	☒	KpD 2.24	Passwort & Benutzername
☐	KpD 2.25	Anzahl Kinder	☐	KpD 2.26	Altersversorgungsdaten	☐	KpD 2.27	Gehaltslisten
☐	KpD 2.28	Ausweisdaten	☒	KpD 2.29	Statistikdaten	☐	KpD 2.30	Zugangskartennummer
☐	KpD 2.31	Anschrift	☐	KpD 2.32	Leistungsbewertung	☒	KpD 2.33	Nutzerverhalten
☐	KpD 2.34	Korrespondenz	☐	KpD 2.35	Fotos und Bilder	☐	KpD 2.36	Steuer-ID

KbP 1.4 – Terminbucher (Definitionen gemäß/siehe Timify-Datenschutzkonzeption)								
☐	KpD 2.1	IP-Adresse	☒	KpD 2.2	E-Mail-Adresse	☒	KpD 2.3	Vorname
☒	KpD 2.4	Nachname	☒	KpD 2.5	Anschrift (Adresse)	☐	KpD 2.6	Rechnungsadresse
☒	KpD 2.7	Buchungs-Details	☐	KpD 2.8	Lieferanschrift	☐	KpD 2.9	Konto-/Kreditkartennummern
☐	KpD 2.10	Bonitätsdaten	☐	KpD 2.11	Kundennummer	☒	KpD 2.12	Telefonnummern
☐	KpD 2.13	Bestellnummer	☐	KpD 2.14	Ticketnummer (contact_in)	☐	KpD 2.15	Werbe-IDs
☐	KpD 2.16	Geburtstag	☐	KpD 2.17	Geburtsort/-land	☐	KpD 2.18	Cookie-Kennung

KbP 1.4 – Terminbucher (Definitionen gemäß/siehe Timify-Datenschutzkonzeption)								
☐	KpD 2.19	Personalnummer	☐	KpD 2.20	Sozialversicherungsdaten	☐	KpD 2.21	Familienstand
☐	KpD 2.22	Zeugnisse	☐	KpD 2.23	Lebenslauf	☐	KpD 2.24	Passwort & Benutzername
☐	KpD 2.25	Anzahl Kinder	☐	KpD 2.26	Altersversorgungsdaten	☐	KpD 2.27	Gehaltslisten
☐	KpD 2.28	Ausweisdaten	☒	KpD 2.29	Statistikdaten	☐	KpD 2.30	Zugangskartennummer
☐	KpD 2.31	Anschrift	☐	KpD 2.32	Leistungsbewertung	☐	KpD 2.33	Nutzerverhalten
☐	KpD 2.34	Korrespondenz	☐	KpD 2.35	Fotos und Bilder	☐	KpD 2.36	Steuer-ID

5. Rechte und Pflichten der Vertragspartner

5.1 Weisungsrecht

(1) Der Umgang mit den Daten im Verhältnis zum Auftraggeber erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen, der beschriebenen Prozesse und nach dokumentierter Weisung des Auftraggebers gemäß Art. 29 DS-GVO. TerminApp und jede TerminApp unterstellten Personen, die Zugang zu personenbezogenen Daten des Auftraggebers haben, werden diese Daten ausschließlich im Rahmen der getroffenen Vereinbarungen, der zugrunde liegenden Prozesse und gemäß der festgelegten Zwecke sowie nach Weisung des Auftraggebers verarbeiten.

(2) TerminApp wird nur auf Weisung des Auftraggebers Daten, die im Auftrag verarbeitet werden, berichtigen, löschen oder sperren. Die Erstellung von Kopien erfolgt nur mit vorheriger Zustimmung durch den Auftraggeber. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung der eigenen ordnungsgemäßen Datenverarbeitung oder Dokumentation erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher (insbesondere nationaler) Aufbewahrungspflichten erforderlich sind.

(3) Die Weisungen sind mangels einer anderslautenden Mitteilung des Kunden und Auftraggebers durch ein Mitglied der Geschäftsführung in Textform (z. B. E-Mail) zu erteilen.

(4) TerminApp hat das Recht, aber nicht die Pflicht, die rechtliche Zulässigkeit der Weisungen zu überprüfen. Hiervon abgesehen wird TerminApp den Auftraggeber jedoch unverzüglich informieren, falls TerminApp der Auffassung sind, eine Weisung verstoße gegen Datenschutzvorschriften.

(5) TerminApp verpflichtet sich zur Bestellung eines Datenschutzbeauftragten. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

5.2 Vertraulichkeitsverpflichtung

(1) TerminApp setzt im Zusammenhang mit der Verarbeitung von personenbezogenen Daten nur Mitarbeiter und Beschäftigte ein, die auf die Vertraulichkeit (Verschwiegenheit)

verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden sowie über die bestehende Weisungs- bzw. Zweckbindung belehrt werden (Art. 28 Abs. 3 b) DS-GVO).

(2) TerminApp wird darüber hinaus verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

5.3 Sicherheit der Verarbeitung

(1) TerminApp verpflichten sich, alle technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um das angemessene Schutzniveau für die personenbezogenen Daten des Auftraggebers (sowie insbesondere von dessen Kunden, Beschäftigte und Vertragspartner) zu gewährleisten.

(2) Bei den zu treffenden Maßnahmen handelt es sich um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei werden von TerminApp der jeweilige Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen zu berücksichtigt [siehe hierzu **Anlage 1** - **Technische und organisatorische Maßnahmen**]. Insoweit hat TerminApp das Recht, die Maßnahmen anzupassen, wenn und soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird und die Änderungen nachvollziehbar für den Auftraggeber dokumentiert werden. Änderungen sind dem Auftraggeber vorab mitzuteilen.

(3) Der Auftraggeber hat das Recht - nach Terminvereinbarung -, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch einen vom Auftraggeber beauftragten Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

5.4 Unterauftragsverhältnisse (Subunternehmer)

(1) TerminApp wird Unterauftragnehmer nur nach vorheriger ausdrücklicher, bzw. dokumentierter Zustimmung des Auftraggebers beauftragen oder austauschen.

(2) Hiervon abgesehen stimmt der Auftraggeber der Beauftragung der in [**Anlage 2** - Unterauftragnehmer] aufgeführten Unterauftragnehmer im Rahmen dieses Auftragsverarbeitungsverhältnisses zu. Die Pflicht, mit diesen Unterauftragnehmern vertragliche Vereinbarungen nach Maßgabe des Art. 28 DS-GVO zu schließen, bleibt unberührt.

(3) TerminApp hat in jedem Fall seine Verträge mit Unterauftragnehmer so zu gestalten, dass die Verantwortlichkeiten zwischen TerminApp und dem jeweiligen Unterauftragnehmer klar voneinander abgegrenzt sind und der Auftraggeber dieselben Rechte auch direkt gegenüber dem jeweiligen Unterauftragnehmer hat, wie er sie nach dieser AV-Vereinbarung gegenüber TerminApp hat. Dies umfasst insbesondere direkte Kontrollrechte des Auftraggebers bei dem jeweiligen Unterauftragnehmer. Der Vertrag zwischen TerminApp und einem Unterauftragnehmer muss außerdem hinreichende Garantien dafür bieten, dass vom jeweiligen Unterauftragnehmer die geeigneten technischen und organisatorischen

Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser AV-Vereinbarung und der einschlägigen Datenschutzgesetze erfolgt.

(4) Die weitere Auslagerung durch die genannten Unterauftragnehmer bedarf der ausdrücklichen vorherigen Zustimmung durch den Auftraggeber.

5.5 Unterstützung

(1) TerminApp wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Personen nach Art. 12 bis 23 DS-GVO nachzukommen.

(2) TerminApp verpflichtet sich, unter Berücksichtigung der Art der Verarbeitung und der TerminApp zur Verfügung stehenden Informationen, den Auftraggeber bei der Einhaltung der Pflichten im Zusammenhang mit der Sicherheit personenbezogener Daten (Art. 32 DS-GVO), den Meldepflichten bei Datenpannen gegenüber den Aufsichtsbehörden und den Betroffenen (Art. 33 DS-GVO) sowie im Zusammenhang mit der Erstellung und Pflege von Datenschutz-Folgeabschätzungen und den vorherigen Konsultationen (Art. 35, 36 DS-GVO) zu unterstützen.

(3) Soweit ein Betroffener sich unmittelbar an TerminApp zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird TerminApp die Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(4) Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer betroffenen Person verpflichtet Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird TerminApp den Auftraggeber dabei unterstützen, diese Informationen bereitzustellen. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder die Betroffenen wird TerminApp nur nach vorheriger Weisung, bzw. Zustimmung durch den Auftraggeber erteilen.

(5) TerminApp arbeitet auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen und wird den Auftraggeber über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, unverzüglich informieren.

5.6 Datenrückgabe

(1) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher, nach Aufforderung durch den Auftraggeber - spätestens mit Beendigung des Auftragsverhältnisses - wird TerminApp nach Wahl des Auftraggebers die personenbezogenen Daten löschen und/oder zurückgeben und/oder jegliche Datenverarbeitung im Auftrag einstellen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(2) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Dokumentationen und Informationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen und insoweit tatsächlich benötigt werden oder gesetzlichen Aufbewahrungspflichten unterliegen, sind hiervon ausgenommen.

5.7 Nachweis- und Kontrollrechte

(1) TerminApp ist gemäß Art. 33 Abs. 2 DS-GVO verpflichtet, jede TerminApp bekanntwerdende Verletzung des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden.

(2) TerminApp wird dem Auftraggeber alle erforderlichen Informationen zur Verfügung stellen, um nachzuweisen, dass TerminApp den Verpflichtungen als Auftragsverarbeiter nachkommt.

(3) Änderungen der Verarbeitungsgegenstände und Verfahrensänderungen sind gemeinsam zwischen dem Auftraggeber und TerminApp abzustimmen und schriftlich oder in einem elektronischen Format zu dokumentierten.

(4) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Übermittlung personenbezogener Daten in ein Drittland oder an internationale Organisationen bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 50 DS-GVO erfüllt sind.

(5) Es wird darauf hingewiesen, dass ein Teil der die in der [Anlage 2 - Unterauftragnehmer] genannten Unternehmen Ihren Haupt-Sitz in den USA haben. Diese Unternehmen bieten System-Komponenten an, die in der Terminbuchungslösung zur Anwendung kommen (z. B. Chat- und Supportfunktionen). TerminApp hat mit diesen Unternehmen jedoch entsprechende Verträge über die Auftragsverarbeitung geschlossen. Zudem sind die Unternehmen nach dem sog. „Privacy Shield“ zertifiziert und gewährleisten folglich einen der EU entsprechenden Datenschutz.

6. Haftung

6.1 TerminApp haftet im Innenverhältnis zum Auftraggeber für den durch eine Verarbeitung verursachten Schaden nur, wenn TerminApp

(1) den speziell durch die DS-GVO auferlegten Pflichten für Auftragsverarbeiter nicht nachgekommen ist oder

(2) unter Nichtbeachtung der rechtmäßig erteilten Weisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

6.2 Soweit im Zusammenhang mit der nach dieser AV-Vereinbarung erfolgenden Datenverarbeitung gegen TerminApp oder Auftraggeber Schadensersatzansprüche (Art. 82 DSGVO), Geldbußen (Art. 83 DSGVO) oder andere Sanktionen (Art. 84 DSGVO) angedroht oder geltend gemacht werden, haben sich TerminApp und Auftraggeber darüber jeweils unverzüglich wechselseitig zu informieren. Ohne vorherige Abstimmung mit der jeweils anderen Partei darf die jeweils betroffene Partei keine Stellungnahmen sowie kein Anerkenntnis oder eine vergleichbare Erklärung abgeben; werden sich TerminApp und Auftraggeber betreffend der Art und Weise der Abwehr nicht einig, liegt das Letztentscheidungsrecht beim Auftraggeber als „Herr der Daten“. Zudem haben sich beide Parteien bei der Anspruchsabwehr zu unterstützen.

6.3 Im Übrigen wird auf die gesetzlichen Bestimmungen verwiesen.

6.4 Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt. Hierzu zählt auch die Haftung der Vertragspartner, ihrer gesetzlichen Vertreter und Erfüllungsgehilfen für Schäden, die vorsätzlich oder grob fahrlässig verursacht werden oder die aus der schuldhaften Verletzung des Lebens, des Körpers oder der Gesundheit resultieren.

7. Schlussbestimmungen

7.1 Im Fall von Widersprüchen zwischen diesem Auftragsverarbeitungsvertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Auftragsverarbeitungsvertrages vor.

7.2 Die Einrede des Zurückbehaltungsrechts nach § 273 BGB an den Daten, Teilen davon sowie Datenträgern des Auftraggebers wird ausgeschlossen. Soweit die Daten beim TerminApp durch Beschlagnahme oder Pfändung, durch ein Insolvenzverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, hat TerminApp den Auftraggeber unverzüglich darüber zu informieren. TerminApp hat alle in diesem Zusammenhang Beteiligten zu informieren, dass ausschließlich der Auftraggeber Verantwortlicher und „Herr der Daten“ ist

7.3 Nebenabreden, Änderungen und Ergänzungen dieses Auftragsverarbeitungsvertrages bedürfen der Textform. Dies gilt auch für die Änderung dieser Schriftformvereinbarung.

7.4 Es gelten die gesetzlichen Bestimmungen der Datenschutz-Grundverordnung, im Übrigen das Recht der Bundesrepublik Deutschland.

7.5 Gerichtsstand ist der Sitz von TerminApp.

7.6 Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelungen eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelungen am nächsten kommt.

München, den 26.06.2019

TerminApp GmbH

Kunde

Anlage 1 - Technische und organisatorische Maßnahmen

Gemäß Art. 32 DS-GVO sind geeignete technisch-organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen seitens des Verantwortlichen und der Auftragsverarbeiter zu treffen. TerminApp setzt die Anforderungen in seinem Einflussbereich in Bezug auf diesen Auftragsverarbeitungsvertrag wie folgt um:

1. Pseudonymisierung und Verschlüsselung

Anforderung	Bewertung für diese Auftragsverarbeitung
Unter Pseudonymisierung versteht man das Ersetzen von Identifikationsmerkmalen mit einer für das Identifikationsmerkmal eindeutigen Kennung, dem Pseudonym.	Eine Pseudonymisierung von personenbezogenen Daten erfolgt vorliegend nicht.
Der Einsatz von kryptographischen Verfahren gehört zu den Standardmaßnahmen des technischen Datenschutzes, da damit wirksam die Vertraulichkeit und Integrität der personenbezogenen Daten geschützt werden können.	Eine Verschlüsselung der Kommunikation erfolgt durch die Implementierung von fortlaufend aktualisierter SSL-Zertifikate der Firma GlobalSign. Aufgrund dieser Zertifikate ist die gesicherte Kommunikation zwischen Webserver und Client gewährleistet.

2. Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

2.1 Zugangs- Zutritts- und Zugriffskontrolle sowie Eingabekontrolle

Anforderung					
Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden. Es muss zudem verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können oder von Unbefugten der physische Zugang zu Einrichtungen oder Räumlichkeiten ermöglicht wird, in denen IT-Systeme betrieben und genutzt werden (z.B. Rechenzentren oder Arbeitsräume); Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können; 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.					
Umsetzung					
☒	2.1.1	Rechner verfügen über individuelle Benutzerkennungen	☒	2.1.2	Server verfügen über individuelle Benutzerkennungen
☒	2.1.3	Zwei-Faktor-Authentifizierung	☒	2.1.4	Das Firmennetzwerk ist durch eine Firewall geschützt
☒	2.1.5	Passwortrichtlinie	☒	2.1.6	Datentrennung innerhalb des Firmennetzwerkes
☒	2.1.7	Der Zugang zum System wird gesperrt bei der fehlerhaften Eingabe des Passwortes	☒	2.1.8	Admin haben lokale Administrationsrechte
☒	2.1.9	Virenscanner auf allen Clients	☒	2.1.10	Es besteht ein Zutrittskonzept für Serverräume

☒	2.1.11	Es besteht ein Zutrittskonzept für Arbeitsräume	☒	2.1.12	Der Zutritt und Aufenthalt von Besuchern erfolgt nur in Begleitung von Firmenpersonal
☒	2.1.13	Manuelle Schließanlage der Eingangstüren	☒	2.1.14	Der Zutritt von Reinigungs- und Wartungspersonal zum Gebäude wird dokumentiert
☒	2.1.15	Automatisierte Abmeldung bei Inaktivität	☒	2.1.16	Administratorrechte geregelt

2.2 Belastbarkeit der Systeme

Anforderung					
Der Begriff der Belastbarkeit („Resilienz“) beschreibt die Fähigkeit des Unternehmens, auch bei Störungen und Eingriffen möglichst unbeschadet weiter existieren zu können. Hierzu zählen z. B. die üblichen IT-Schutzmaßnahmen.					
Umsetzung					
☒	2.2.1	Datenträger und Datenspeicher werden zugriffssicher aufbewahrt	☒	2.2.2	Zugang zu Storage-Lösungen wird für Unbefugte physisch verhindert
☒	2.2.3	Datenträger und Datenspeicher werden professionell entsorgt/vernichtet	☒	2.2.4	Datenträger und Datenspeicher unterliegen einem Aufbewahrungs- und Löschkonzept
☒	2.2.5	Storage-System werden räumlich abgeschirmt	☒	2.2.6	Integrität und Manipulationssicherheit bei Storage-Systemen
☒	2.2.7	Mandantenfähigkeit bei den Storage-Systemen	☒	2.2.8	Rollen- und Berechtigungskonzepte
☒	2.2.9	Datensicherheitskonzepte vorhanden	☒	2.2.10	Ansprechpartner genannt, geschult und Verarbeitungsprozesse definiert
☒	2.2.11	Data-Breach-Konzept vorhanden	☒	2.2.12	Incidents-Management vorhanden
☒	2.2.13	Regelmäßige (interne) Datenschutz- und Datensicherheitskontrollen	☒	2.2.14	Backuplösungen zur Widerherstellbarkeit
☒	2.2.15	Kurze Wiederanlaufzeit des Rechenzentrums	☒	2.2.16	Gebäude und Einrichtungen sind je nach Kritikalität gemäß den technischen Standards vor Zerstörung (z. B. Brand) geschützt.
☒	2.2.17	Es bestehen Verträge für die Wartung von IT-Systemen durch externe Unternehmen	☒	2.2.18	Datensicherungsrichtlinie vorhanden
☒	2.2.19	Verschlüsselter Transport von Daten vorhanden	☒	2.2.20	Datenmigrationskonzepte vorhanden
☒	2.2.21	Prüfung der Empfänger (NDA, Compliance)	☒	2.2.22	Aktualisierungsrichtlinie für die Schutzsoftware vorhanden

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

Anforderung					
Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.					
Umsetzung					
☒	3.1	Datenbackupkonzept vorhanden	☒	3.2	Regelmäßige (interne) Datenschutz- und Datensicherheitskontrollen
☒	3.3	Data-Breach-Konzept vorhanden	☒	3.4	Incidents-Management vorhanden
☒	3.5	Trennung von Test- und Produktivdaten gewährleistet			

4. Verfahren, die der regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung dienen.

Anforderung	Bewertung für diese Auftragsverarbeitung
Informationssicherheit ist (auch) ein Prozess, d.h., Sicherheitsprodukte alleine sind nicht ausreichend zur Gewährleistung eines angemessenen Schutzniveaus, und gehört seit langem zum üblichen Verständnis beim Schutz von Informationen (hier: personenbezogene Daten). Auch beim Schutz personenbezogener Daten muss ein geeigneter prozessorientierter Ansatz verfolgt werden, der sich beispielsweise auch in (bereits bestehenden) Informationssicherheitsmanagementsystemen wiederfindet, die um den technischen Datenschutz erweitert werden können.	TerminApp hat fest definierte Zyklen, innerhalb derer die Anforderungen an die Datensicherheit überprüft werden. Hierbei wird auch das o. g. Schutzniveau stets erneut auf den Prüfstand gestellt. Turnusmäßig findet eine Revision anlassunabhängig alle 9 Monate statt.

5. Verfahren zur Gewährleistung, dass Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten

Anforderung	Bewertung für diese Auftragsverarbeitung
Maßnahmen, die gewährleisten, dass personenbezogene Daten vom Auftraggeber nur gemäß deren Weisungen verarbeitet werden. Beschäftigt der Partner einen Unterauftragnehmer, so muss er diesen in gleicher Weise zur Erfüllung der Weisungen und zur Einhaltung des Datenschutzes verpflichten.	Sämtliche Mitarbeiter werden auf die Vertraulichkeit und Verschwiegenheit verpflichtet (Art. 28 Abs. 3 b DS-GVO). TerminApp hat die Mitarbeiter gesondert auf die Weisungsgebundenheit verpflichtet (Art. 29 DS-GVO).

Anlage 2 - Unterauftragnehmer

Name und Anschrift des Unterauftragnehmers	**Zweck der Datenverarbeitung**
E7STUDIO Ltd., bul. Osvobojdenie 32, 4023 Plovdiv, Bulgarien	Technischer Support der Developer-API von Timify
Amazon Web Services EMEA SARL, 5 rue Plaetis, L-2338 Luxemburg	Hosting der Timify-Services
Intercom, Inc. 55 2nd Street, 4th Floor, San Francisco, California, 94105, USA	Anbieter der Kommunikations- und Chatplattform innerhalb der Terminbuchungslösung
Appcues Inc. 54 Canal Street, 5th Floor, Boston, MA 02114, USA	Anbieter der Kommunikations- und Chatplattform innerhalb der Terminbuchungslösung;
Sendinblue SAS 55 Rue d'Amsterdam, 75008 Paris (Frankreich)	Anbieter von E-Mail Kampagnen (z. B. Newsletter)
MongoDB, Inc, 1633 Broadway, 38th Floor, New York, NY 10019, United States (US)	Anbieter der Datenbank für die App-Anbindung (Grundlage ist ein individueller AV-Vertrag, dem der Kunde beitreten kann)
SendGrid, Inc. 1801 California Street, Suite 500, Denver, Colorado 80202	Anbieter einer E-Mail-Marketing Software