Azdam pdf-a ot Vertrag über die Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

TerminApp GmbH
Balanstr.73, Building 24, München

nachfolgend: „**Timify**“ genannt

und dem **Kunden**
*(*nachstehend „**Auftraggeber“** genannt*)*

1. Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der in dieser Vereinbarung beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit der Dienstleistung von Timify in Zusammenhang stehen und bei denen Mitarbeiter von Timify oder durch Timify beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

2. Definitionen

(1) Personenbezogene Daten

Nach Art. 4 Abs. 1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

(2) Auftragsverarbeiter

Nach Art. 4 Abs. 8 DS-GVO ist ein Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Speicherung, Pseudonymisierung, Löschung, Herausgabe) des Auftragsverarbeiters mit personenbezogenen Daten gerichtete Anordnung des Auftraggebers. Die Weisungen werden vom Auftraggeber erteilt und können durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Die Weisungen des Auftraggebers sind schriftlich oder per E-Mail zu erteilen.

3. Verantwortlichkeit und Anwendungsbereich

3.1 Timify erbringt im Auftrag des Auftraggebers und im Zusammenhang mit der Bereitstellung der Terminbuchungslösung diverse (Hosting-)Leistungen. Da ausgewählte Mitarbeiter (Admins, Kundenbetreuer) von Timify Zugriff auf personenbezogene Daten haben, ist nach Art. 28 DS-GVO der Abschluss einer Vereinbarung zur Verarbeitung im Auftrag erforderlich.

3.2 Das Eigentum an den vom Auftraggeber bereitgestellten personenbezogenen Daten liegt ausschließlich beim Auftraggeber als "Verantwortlichen" im Sinne der DS-GVO. Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages sowie nach Beendigung des Vertrages jederzeit die Berichtigung, Löschung, Sperrung und Herausgabe von personenbezogenen Daten von Timify verlangen.

4. Gegenstand und Dauer des Auftrages

4.1 Diese Vereinbarung tritt mit ihrer Unterzeichnung (digital) durch beide Parteien in Kraft und endet im Regelfall mit Kündigung des zugrundeliegenden Hauptvertrages (je nach gebuchtem Leistungspaket).

4.2 Der Auftrag umfasst folgende Leistungen:

☒ Bereitstellung einer webbasierten Softwarelösung zur Online-Terminvereinbarung (Terminbuchungen), einschließlich des Raum- und Ressourcenmanagement (Timify) als Software as a Service (SaaS) im Rechenzentrum eines Subunternehmers von Timify;
☒ Support-Tätigkeiten bei Problemen und Störungen im Zusammenhang mit der Nutzung von Timify;
☒ Wartung und Pflege der webbasierten Softwarelösung Timify.

4.3 Der Umfang der Verarbeitung und damit die Menge der eingesetzten (personenbezogenen) Daten sind variabel und richtet sich nach der Nutzungsintensität und den Vorgaben durch den Auftraggeber. Der Zweck dient zur Verwaltung und Steuerung der einzelnen Buchungen.

4.4 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 Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

4.5 Art der Daten

☒	Registrierungs- und Logindaten (z. B. Name, Vorname, Benutzername, E-Mail-Adresse);
☒	Kontaktdaten des Auftraggebers (z. B. Name, Vorname, Ansprechpartner, Kontobesitzer, E-Mail-Adresse);
☒	Zahlungs- und Rechnungsdaten des Auftraggeber (z. B. Bankverbindung);
☒	Nutzungsdaten (z.B. Protokollierung der Nutzeraktivitäten, Log-Files, IP-Adresse);
☒	Terminbucherdaten (z. B. Name, Vorname, E-Mail-Adresse, Telefonnummer, Terminbucher-Details).

4.6 Kategorien der betroffenen Personen

☒	Ansprechpartner auf Seiten des Auftraggebers;
☒	Terminbucher.

5. Technische und organisatorische Maßnahmen (TOM)

5.1 Timify verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen (TOM), die zur Wahrung der anzuwendenden Datenschutzvorschriften angemessen und erforderlich sind. Die Maßnahmen dienen der Datensicherheit und der Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der mit diesem Auftrag in Zusammenhang stehenden Systeme. Dabei werden der 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 natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO berücksichtigt.

5.2 Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der TOM ist als **Anlage A** dieser Vereinbarung beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen TOM erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird Timify im Vorwege mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können von Timify ohne Abstimmung mit dem Auftraggeber umgesetzt werden.

6. Berichtigung, Einschränkung und Löschung von Daten

6.1 Timify darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person (z.B. Terminbucher) sich diesbezüglich unmittelbar an Timify wendet, wird Timify dieses Ersuchen unverzüglich an den Auftraggeber zur Freigabe weiterleiten.

6.2 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

6.3 Nach dem Ende des Vertragsverhältnisses oder früher - nach Aufforderung durch den Auftraggeber - wird Timify sämtliche in seinen Besitz gelangten Datenbestände (sofern vorhanden), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber aushändigen oder nach vorheriger Zustimmung löschen.

7. Besondere Pflichten von Timify

7.1 Eine Verarbeitung personenbezogener Daten, die sich nicht auf die Erbringung der vertragsgegenständlichen Leistungen bezieht, ist Timify untersagt, es sei denn, dass der Auftraggeber dieser ausdrücklich zuvor zugestimmt hat.

7.2 Timify hat einen betrieblichen Datenschutzbeauftragten (Dr. Philipp Herrmann) bestellt. Dieser ist erreichbar über dataprivacy@timify.de.

7.3 Timify wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach deren Auffassung gegen gesetzliche Regelungen verstößt. Timify ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

7.4 Für den Fall, dass Timify feststellt oder Tatsachen die Annahme begründen, dass von Timify für den Auftraggeber verarbeitete personenbezogene Daten einer Verletzung des gesetzlichen Schutzes personenbezogener Daten gem. Art. 33 DS-GVO (Datenschutzverstoß bzw. Datenpanne) unterliegen, z.B. indem diese unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat Timify den Auftraggeber unverzüglich und vollständig u.a. über Zeitpunkt, Art und Umfang des Vorfalls bzw. der Vorfälle in Schriftform oder Textform (per E-Mail) zu informieren.

7.5 Timify stellt auf Anforderung dem Auftraggeber die für dessen Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DS-GVO notwendigen Angaben bezogen auf die in dieser Vereinbarung beschriebenen Verarbeitungstätigkeiten zur Verfügung und führt als Auftragsverarbeiter selbst ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO.

7.6 Timify stellt sicher, dass die mit der Verarbeitung der personenbezogenen Daten des Auftraggebers befassten Mitarbeiter gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO zur Wahrung der Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden. Mitarbeiter von Timify, die aufgrund ihrer (technischen) Funktion einer besonderen Verschwiegenheit/Vertraulichkeit unterliegen (z. B. Administratoren; Entwickler & Programmierer) wurden darüber hinaus (datenschutz-)rechtlich zur Vertraulichkeit verpflichtet. Diese Vertraulichkeitsverpflichtung besteht auch nach dem Vertragsende fort.

7.7 Des Weiteren verpflichtet sich Timify, den Auftraggeber gemäß Art. 28 Abs. 3 lit. f DS-GVO bei der Einhaltung der in Artt. 34 - 36 DS-GVO genannten Pflichten zu unterstützen und auf Anfrage des Auftraggebers mit der Aufsichtsbehörde ggf. zusammenzuarbeiten.

7.8 Timify hat den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, zu informieren. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei Timify ermittelt.

7.9 Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung durch Timify ausgesetzt ist, hat ihn Timify nach besten Kräften zu unterstützen.

7.10 Timify kontrolliert regelmäßig die internen Prozesse sowie die TOM, um zu gewährleisten, dass die Verarbeitung in dem eigenen Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

8. Rechte und Pflichten des Auftraggebers

8.1 Der Auftraggeber hat das Recht, jederzeit Weisungen über Art, Umfang und den Umfang der Datenverarbeitung zu erteilen. Weisungen bedürfen mangels anderslautender Vereinbarung der Textform (mindestens per E-Mail).

Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber (auf Grundlage einer vorherigen Kosten- und Aufwandsschätzung und anschließenden Freigabe/Beauftragung durch den Auftraggeber) zu tragen.

8.2 Der Auftraggeber hat Timify unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

8.3 Dem Auftraggeber obliegen die aus Art. 33 Abs. 1 DS-GVO resultierenden Meldepflichten.

9. Kontrollbefugnisse

9.1 Timify erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte 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).

9.2 Die Kosten für nachweisliche Aufwände einer Kontrolle bei Timify können gegenüber dem Auftraggeber (auf Grundlage einer vorherigen Kosten- und Aufwandsschätzung und anschließenden Freigabe/Beauftragung durch den Auftraggeber) geltend gemacht werden.

10. Unterauftragsverhältnisse mit Subunternehmern

10.1 Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist Timify **ohne gesonderte Genehmigung** des Auftraggebers gestattet, Art. 28 Abs. 2 Satz 2 DS-GVO. Timify muss dafür in jedem Fall dafür Sorge tragen, dass Timify den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. In diesem Fall informiert Timify den Auftraggeber zudem immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter.

10.2 Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

10.3 In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten von Timify und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

10.4 Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

10.5 Zurzeit sind für den Auftragsverarbeiter die in der **Anlage B** dokumentierten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit der Beauftragung der in Anlage B genannten Subunternehmer erklärt sich der Auftraggeber einverstanden.

10.6 Timify informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer. Der Auftraggeber erhält die Möglichkeit, gegen derartige Änderungen Einspruch zu erheben, sofern die bisher vereinbarten und zugesicherten TOM nicht vollständig gewährleistet werden können (§ 28 Abs. 2 Satz 2 DS-GVO).

11. Daten- und Geschäftsgeheimnisse, Geheimhaltungspflichten

11.1 Timify verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, Timify etwaige besondere Geheimnisschutzregeln (Geschäftsgeheimnisse i.S.d. § 2 GeschGehG) mitzuteilen.

11.2 Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieser Vereinbarung erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den oben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

11.3 Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

12. Informationspflichten, Schriftformklausel, Rechtswahl

12.1 Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. Als Gerichtsstand wird das für Timify örtlich zuständige Gericht in München vereinbart.

12.2 Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers bei Timify durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat Timify den Auftraggeber unverzüglich zu verständigen.

12.3 Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

12.4 Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

München, den 15.09.2020

Andreas Knürr (CEO/Geschäftsführer)

TerminApp GmbH

_____

Auftraggeber

Anlage A - Technische und organisatorische Maßnahmen (TOM)

1. Vertraulichkeit

Vertraulichkeit	
Anforderung an die Zutrittskontrolle:	
Timify hat durch geeignete Maßnahmen sicherzustellen, dass Unbefugte keinen Zugang zu Datenverarbeitungsanlagen (insbesondere Telefonsysteme, Datenbanken, Anwendungsserver und angeschlossene Hardware) erhalten, die zur Verarbeitung personenbezogener Daten der Dienstleister, deren Kunden oder unserer Partner genutzt werden.	
Umsetzung durch Timify:	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Außentüren nur mit Schlüssel/Zutrittskarte zu öffnen	Dokumentierte Schlüsselausgabe
Verschlossene Serverräume	Besucherbegleitung durch Beschäftigte
Sicherheitsschlösser	Sorgfältige Auswahl von zutrittsberechtigten Dienstleistern
	Sorgfalt bei Auswahl v. Reinigungskräften

Vertraulichkeit	
Anforderung an die Zugangskontrolle:	
Timify hat durch geeignete Maßnahmen sicherzustellen, dass die Datenverarbeitungssysteme nicht von Unbefugten benutzt werden können.	
Umsetzung durch Timify:	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Authentifikation/Login mit Name und Passwort	Dokumentiertes Benutzermanagement
Verschlossene (interne) Serverräume	Personifizierte Benutzer im Netzwerk
Automatische Bildschirmsperren	
Einsatz einer aktuellen Firewall	
Einsatz eines aktuellen Virenschutzes	
Sichere VPN-Verbindung zum Netzwerk	

Vertraulichkeit	
Anforderung an die Zugriffskontrolle:	
Timify hat durch geeignete Maßnahmen sicherzustellen, dass die für die Datenverarbeitung verwendeten IT-Systeme den autorisierten Benutzern nur einen begrenzten Zugriff erlauben, der durch ihre individuellen Autorisierungsrechte festgelegt wird. Timify muss angemessene Maßnahmen ergreifen, um sicherzustellen, dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.	
Umsetzung durch Timify:	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Anwendungsbezogene Authentifikation mit Benutzername und Passwort	Rollenbasiertes Berechtigungskonzept für Anwendungen und Verzeichnisse
Verschlossene Schränke zur sicheren Aufbewahrung von Dokumenten	Vergabe der Berechtigungen nur nach Freigabe durch den Dateneigner
Benutzung von einer Passwort-Manager-Software-Lösung mit 2FA	Geschützte Aufbewahrung der Datenträger

	Administrative Benutzer sind auf ein Minimum beschränkt und dokumentiert

Vertraulichkeit
Anforderung an die Trennungskontrolle:
Timify hat durch geeignete Maßnahmen sicherzustellen, dass Daten, die für verschiedene Zwecke gesammelt wurden, getrennt verarbeitet werden.
Umsetzung durch Timify:

Technische Maßnahmen	**Organisatorische Maßnahmen**
Daten des Auftraggebers werden auf physikalisch getrennten Systemen gespeichert	Trennung von Zugriffen über die Steuerung des Berechtigungskonzepts
Daten des Auftraggebers werden innerhalb eines Systems mittels Mandantentrennung gespeichert	
Trennung von Produktiv- und Testumgebung	

2. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Pseudonymisierung
Anforderung an die Pseudonymisierung:
Timify hat durch geeignete Maßnahmen sicherzustellen, dass Daten soweit wie möglich pseudonymisiert werden, sofern der Personenbezug für das Ergebnis nicht zwingend erforderlich ist.
Umsetzung durch Timify:

Technische Maßnahmen	**Organisatorische Maßnahmen**
	Pseudonymisierung erfolgt im Umfeld der Auftragsverarbeitung nur auf Weisung des Verantwortlichen (Dienstleisters/Auftraggebers)

3. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Integrität
Anforderung an die Weitergabekontrolle:
Timify hat durch geeignete Maßnahmen sicherzustellen, dass persönliche Daten während der Datenübertragung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.
Umsetzung durch Timify:

Technische Maßnahmen	**Organisatorische Maßnahmen**
VPN-Verbindungen/verschlüsselte Verbindungen/IP Beschränkungen	Verbot des Einsatzes privater Speichermedien
E-Mail-Verschlüsselung (Ende-zu-Ende auf Anfrage)	Verbot der lokalen Speicherung von Kundendaten
SFTP/Https-Verbindungen	
Datenbank-Zugriff ist mit Network Peering-Verbindung gesichert	
Nutzung von Webanwendungs-Firewall (AWS WAF)	
Server-Instanzen werden im privaten Netzwerkbereich abgelegt	

Integrität	
Anforderung an die Eingabekontrolle:	
Timify hat durch geeignete Maßnahmen sicherzustellen, dass nachvollzogen werden kann, wer personenbezogene Daten in die Datenverarbeitungssysteme eingegeben hat oder von wem personenbezogene Daten aus den Datenverarbeitungssystemen gelöscht wurden. Timify darf auch personenbezogene Daten nur zum angegebenen und festgelegten Zweck verarbeiten.	
Umsetzung durch Timify:	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Nachvollziehbarkeit von Eingaben, Änderungen und Löschungen durch personifizierte Benutzer	Unterschiedliche Rechtevergabe nach dem „need to know" Prinzip
Nachvollziehbarkeit bei der Vergabe, Änderung und Löschung von Benutzerberechtigungen	Klare Aufgabenzuweisung für Änderungen und Löschungen
Überwachung und Protokollierung von automatisierten Datenverarbeitungen	Stichprobenprüfung von automatisierten Datenverarbeitungen bzw. Logfiles

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeit und Belastbarkeit	
Anforderung an die Verfügbarkeitskontrolle:	
Timify hat durch geeignete Maßnahmen sicherzustellen, dass personenbezogene Daten nicht unbeabsichtigt verloren gehen oder zerstört werden können.	
Umsetzung durch Timify:	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Regelmäßiges, automatisiertes Patch-Management für Server	Einspielung sicherheitskritischer Patches
Regelmäßiges automatisiertes und dokumentiertes Patch-Management für Endgeräte	Regelmäßige Prüfung der Datensicherungen auf Vollständigkeit und Wiederherstellbarkeit
Räumliche getrennte redundante Datenspeicherung	Notfallplan und Wiederanlaufplan für die IT-Systeme
Einsatz eines hochgesicherten Rechenzentrums (RZ)	Backup & Recovery-Konzept
USV	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutzmanagement	
Umsetzung durch Timify:	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Software-Lösungen für Datenschutz-Management im Einsatz (Audatis)	Benennung eines externen Datenschutzbeauftragten
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit	Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet;

für Mitarbeiter nach Bedarf / Berechtigung	
	Regelmäßige Sensibilisierung der Mitarbeiter
	Einsatz und Betreuung durch einen internen Datenschutzkoordinator
	Privacy Manual (Datenschutzhandbuch)

Incident-Response Management	
Umsetzung durch Timify:	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Einsatz von Firewall und regelmäßige Aktualisierung	Handlungsanweisungen für Beschäftigte für den Umgang mit Datenschutzverletzungen
Einsatz von Spamfilter und regelmäßige Aktualisierung	Geregelte und dokumentierte Prozessbeschreibungen und Kommunikationsabläufe

Privacy by design/default	
Umsetzung durch Timify:	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Fortlaufende Überwachung des Entwicklungsprozesses	Zweckbeschränkung der Datenverarbeitung
Integrierte automatische Code-Tests im Entwicklungsprozess	Einfache Ausübung/Wahrnehmung/Umsetzung der Betroffenenrechte

Auftragskontrolle bei der Auslagerung von Diensten an Dritte	
Anforderung an die Verfügbarkeitskontrolle:	
Timify hat durch sicherzustellen, dass Daten, Übermittlung oder der Zugriff auf personenbezogene Daten erst dann erfolgen, wenn der Dienstleister eine Vereinbarung zur Auftragsverarbeitung (z. B. gemäß Artikel 28 DS-GVO) unterzeichnet hat und die Einhaltung der Regelungen des Datenschutzkonzeptes bestätigt hat.	
Umsetzung durch Timify:	
Technische Maßnahmen	**Organisatorische Maßnahmen**
	Dokumentation der Verarbeitungstätigkeiten
	Sorgfältige Auswahl der Auftragsverarbeiter
	Kein Einsatz von Auftragsverarbeitern, die nicht gemäß Art. 28 DS-GVO/SCC/BCR verpflichtet wurden
	Evaluierung der Dienstleister mit Sitz in den USA (Neubewertung im Hinblick auf das Ende von „Privacy-Shield“)

Anlage B – Subunternehmer

Name und Anschrift	Zweck der Datenverarbeitung	Standort	Grundlage der Datenverarbeitung			
Sendgrid, Inc., 801 California Street, Suite 500 Denver, Colorado 80202 USA	Dienst/Anbieter zum Versand von E-Mails	USA	ADV	AV	SCC	BCR
				X	X	X
Amazon Web Services 410 Terry Avenue North,	Hosting der Timify-Services, einschließlich der Be-	USA	ADV	AV	SCC	BCR

Seattle WA 98109 USA	reitstellung von Rechenleistung und Datenbankspeicherung (die Daten werden jedoch ausschließlich in der EU gespeichert/RZ Frankfurt a. M.)			X	X	
MongoDB, Inc., 3 Shelbourne Building, Crampton Avenue Ballsbridge, Dublin 4, Irland	Anbieter der Datenbank für die App-Anbindung (die Daten werden jedoch ausschließlich in der EU gespeichert/RZ Frankfurt a. M.)	Irland	ADV	AV	SCC	BCR
				X	X	
Intercom Inc., 55 2nd Street 4th Floor San Francisco, CA 94105, USA	Anbieter der Kommunikations- und Chatplattform innerhalb der Terminbuchungslösung (Support)	USA	ADV	AV	SCC	BCR
				X	X	