Vertrag über die Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

Hinweis:

Dieser Vertrag basiert auf der Mustervertragsanlage des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom e.V.). Die Mustervertragsanlage gilt als ausgewogenes Vertragswerk zwischen Auftraggeber und Auftragnehmer.

Zwischen

dem Auftraggeber als dem Verantwortlichen im Sinne des Datenschutzrechts

und

TELEDATA IT-LÖSUNGEN GMBH

- als Auftragsverarbeiter, nachstehend Auftragnehmer genannt -

über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO).

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den Leistungen der TELEDTA IT-Lösungen GmbH (wie in der Regel in einem gesonderten Vertragswerk, im folgenden „Leistungsvertrag", spezifiziert) ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Leistungsvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Leistungsvertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die in Anlage 1 aufgeführten Daten Bestandteil der Datenverarbeitung.

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Leistungsvertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Leistungsvertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze,

insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

2) Die Weisungen werden anfänglich durch den Leistungsvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Leistungsvertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und liegen dieser Vereinbarung als Anlage 2 bei; er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3) Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

4) Der Auftragnehmer unterstützt, soweit vereinbart, den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Artt. 33 bis 36 DSGVO genannten Pflichten. Der Auftraggeber erstattet dem Auftragnehmer die Kosten für diese Unterstützungsleistung gemäß den jeweils geltenden Dienstleistungssätzen.

5) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

7) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

8) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

9) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Der Auftraggeber erstattet in diesem Fall dem Auftragnehmer die hierdurch entstehenden Kosten gemäß den im Leistungsvertrag vereinbarten Dienstleistungssätzen. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer kostenpflichtigen Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Leistungsvertrag bereits vereinbart.

   In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe-, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Leistungsvertrag bereits vereinbart.

10) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

11) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Der Auftraggeber erstattet in diesem Fall dem Auftragnehmer die hierdurch entstehenden Kosten gemäß den im Leistungsvertrag vereinbarten Dienstleistungssätzen.

§ 4 Pflichten des Auftraggebers

1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt § 3 Abs. 10 entsprechend.

3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten durch Selbstaudits nach.

2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

   Der Auftraggeber stimmt der Benennung eines unabhängigen externen Prüfers durch den Auftragnehmer zu, sofern der Auftragnehmer eine Kopie des Auditberichts zur Verfügung stellt.

Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung gemäß den im Leistungsvertrag vereinbarten Dienstleistungssätzen verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

1) Der Einsatz von Subunternehmern als weitere Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

   Hat der Subunternehmer seinen Sitz außerhalb eines Mitgliedsstaats der Europäischen Union oder eines anderen Vertragsstaats des Abkommens über den Europäischen Wirtschaftsraum (EWR), kommen die Regelungen der Art. 44 ff. DSGVO zur Anwendung. Soweit erforderlich, wird der Auftragnehmer Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 c, d DSGVO im Namen des Auftraggebers mit dem Subunternehmer abschließen. Der Auftraggeber erteilt dem Auftragnehmer hiermit bereits jetzt die hierzu erforderliche Vollmacht.

2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Leistungsvertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

   Die vertraglich vereinbarten Leistungen bzw. Teilleistungen werden unter Einschaltung der in Anlage 3 aufgeführten Subunternehmer durchgeführt.

   Für die dort genannten Subunternehmer erteilt der Auftraggeber schon jetzt seine Zustimmung. Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.

3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

Soweit der Subunternehmer auf Wunsch des Auftraggebers zum Einsatz kommt, trägt der
Auftraggeber die rechtlichen und tatsächlichen Risiken einer Datenübermittlung in Drittländer ohne angemessenes Datenschutzniveau im Sinne des Art. 45 DSGVO.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Leistungsvertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

4) Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

Eine zwischen den Parteien im Leistungsvertrag vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart ist.

[ ] Als insoweit vertretungsberechtigtes Organ oder bevollmächtigter Vertreter des Auftraggebers habe ich die Bestimmungen dieses Vertrags über die Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 DSGVO gelesen, verstanden und stimme diesen zu.

Anlagen:

1. Technische und organisatorische Maßnahmen
2. Datenarten- / Kategorien / Kreis der Betroffenen
3. Unterauftragnehmer

Anlage 1: Technische und organisatorische Maßnahmen

1 Dokumenteninformation

Die EU-Datenschutzgrundverordnung (DSGVO) enthält Vorgaben darüber, wie in technischer und organisatorischer Hinsicht mit personenbezogenen Daten umgegangen werden soll. Dies dient dem Ziel der Datensicherheit. Die Datensicherheit stellt damit einen weiteren und ergänzenden Aspekt des Datenschutzes dar.

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind:

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

3. zu 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 (Zugriffskontrolle),

4. zu 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 (Weitergabekontrolle),

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

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

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

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

Um diesen Geboten der Datensicherheit zu genügen, hat die TELEDATA IT-Lösungen GmbH die nachstehend unter Ziff. 4 ff. beschriebenen Maßnahmen ergriffen.

In diesem Dokument mit aufgenommen sind die jeweils für ihren Anwendungsfall erforderlichen technischen-organisatorischen Maßnahmen der Unterauftragnehmer. Diese sind ebenfalls nach Art. 32 DSGVO sorgfältig ausgewählt und werden laufend überprüft.

Gesetzlich geregelt ist die Datensicherheit in Art. 32 Abs. 1 DSGVO. Die Vorschrift fordert sinngemäß, dass solche technischen und organisatorischen Maßnahmen zu treffen sind, die erforderlich sind, um den Schutz personenbezogener Daten zu gewährleisten.

Für eine automatisierte Verarbeitung (also vor allem per Hard- und Software) nennen die Gesetze (nach DSGVO) verschiedene Kontrollbereiche, die jeweils noch verschiedene Unterpunkte beinhalten:

1. Vertraulichkeit
2. Integrität
3. Verfügbarkeit und Belastbarkeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
5. Pseudonymisierung und Verschlüsselung

Für nicht-automatisierte Verarbeitungen von personenbezogenen Daten (also ohne Computer) sind die oben genannten Kontrollbereiche nach dem Gesetzeswortlaut nicht direkt anwendbar. Es wird jedoch empfohlen, für einen bestmöglichen Schutz auch in diesen Fällen die Datensicherheit in Anlehnung an die Kontrollbereiche zu organisieren.

All diese Maßnahmen stellen wir in der Folge vor, um unseren Informationspflichten aus Art. 32 Abs. 3 lit. c nachzukommen.

2 Versionshistorie

Version	Status	Datum	Verantwortlich	Änderung
1.0	ersetzt durch V 2.0	02.05.2018	Paul/Bücking	Anlage zu § 9 BDSG angepasst auf DSGVO
2.0	ersetzt durch V 3.0	13.03.2020	Paul/Bücking	Anlage 1 § 4.1.2 und 4.1.3 Software MDM von BlackBerry zu Microsoft Intune geändert. Anlage 3: Unterauftragnehmer angepasst. Schriftart angepasst
3.0	ersetzt durch V 4.0	24.01.2022	Paul/Bücking	Unterauftragnehmer angepasst
4.0	In Kraft	19.04.2022	Paul/Bücking	Aktualisierung, Ergänzung, u.a. Microsoft Endpoint Manager (Microsoft Conditional Access) in Ersetzung von MS Intune, Anpassung an Struktur und Inhalt aktueller WP-Anfragenkatalge

3 Organisatorisches

Die TELEDATA IT-LÖSUNGEN GMBH hat gemäß Art. 37 DSGVO einen externen Datenschutzbeauftragten in Person von RA Dr. Jens Bücking bestellt. Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind schriftlich auf das Datengeheimnis sowie auf die Vertraulichkeit verpflichtet. Der Datenschutzbeauftragte führt regelmäßig Überwachungsaudits sowie fachspezifische Schulungen durch. Die TELEDATA IT-LÖSUNGEN GMBH gewährleistet die schriftliche Dokumentation des aktuellen Datenschutz-Niveaus sowie die schriftlichen Arbeitsanweisungen, Richtlinien und Merkblätter für Mitarbeiter. Es existiert ein Datensicherheitskonzept. Zudem sind Verfahren im Bereich Benachrichtigung, Auskunftsersuchen sowie Anliegen zur Berichtigung, Löschung und Sperrung implementiert.

4 Sicherungsmaßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der TELEDATA IT-LÖSUNGEN GMBH zum Datenschutz gemäß Art. 32 DSGVO betrieben werden.

Die Server, Datenbanken sowie die Datensicherung (Backup) werden bei der TELEDATA IT-LÖSUNGEN GMBH oder beauftragten Dritten in professionellen Rechenzentren betrieben und gewartet. Die Unterbeauftragten werden sorgfältig ausgewählt und hinsichtlich ihres Sicherheitsbewusstseins und ihrer Fachkompetenz überprüft.

Einige diesen Bereich betreffenden Sicherungsmaßnahmen der folgenden Prüfliste sind nicht gesondert ausgewiesen, da sie in die Verantwortung der Unterbeauftragten fallen oder aus Gründen der Aufrechterhaltung der Sicherheit durch Vertraulichkeit nicht detailliert veröffentlich werden.

Es wird ausdrücklich darauf hingewiesen, dass die eigentliche Datenverarbeitung auf Servern erfolgt, die im Rechenzentrum der DATEV in Nürnberg/BR Deutschland untergebracht sind. Im Bereich PARTNERasp sind somit die technisch-organisatorischen Maßnahmen der DATEV für das hiesige Auftragsdatenverarbeitungsverhältnis relevant. Sie finden unsere Vereinbarung zur Auftragsdatenverarbeitung mit der DATEV, indem Sie mit dem Internet Explorer oder Microsoft Edge die Webseite www.datev.de/av aufrufen. DATEV unterzieht sich in regelmäßigen Abständen anerkannten Audit- und Zertifizierungsverfahren u.a. in den Bereichen Datenschutz/Datensicherheit, abrufbar unter:

https://www.datev.de/web/de/m/ueber-datev/datenschutz/zertifikate/

4.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.1.1 Zutrittskontrolle

Die Zutrittskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

#	Maßnahmen
	Das Verhalten gegenüber Fremdpersonen ist fester Bestandteil der jährlich stattfindenden Datenschutzschulung. Bei dieser handelt es sich um eine Pflichtveranstaltung; ein Fernbleiben ist zu begründen und wird nur bei Vorliegen eines wichtigen Grundes akzeptiert. Die Schlüsselausgabe ist formalisiert und wird protokolliert. Auf die Sorgfaltspflichten im Umgang mit den Zutrittsmedien wird ebenfalls im Rahmen der Datenschutzschulung eingegangen. Fenster und Türen sind grundsätzlich verschlossen zu halten. Auf einschlägige Mittel der Zugangskontrolle wird an dieser Stelle verwiesen. Der unternehmenseigene Serverraum ist grundsätzlich versperrt; der Zutritt ist exklusiv.

4.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

#	Maßnahmen
	Eine Passwortrichtlinie mit ausreichendem Schutzstandard ist implementiert. Vorgaben zur Komplexität, Länge, Lebensdauer und Historie eines Kennwortes werden durchgesetzt. Der Benutzer wird zudem nach einer bestimmten Anzahl von Falscheingaben automatisch gesperrt. Kennwörter dürfen ferner weder den ganzen noch Teile des Kontonamens des Benutzers beinhalten. Auch die Passwortgrundsätze sind fester Bestandteil der jährlich stattfindenden Datenschutzschulung.

	Weitere Maßnahmen der Zugangskontrolle: Clientsysteme im Netzwerk sind geschützt über sichere Netzwerk Login-Credentials. Sämtliche Programme verfügen über eine benutzerbezogene Datenhaltung, die – soweit möglich – an die Windowsanmeldung gekoppelt ist. An- und Abmeldungen werden protokolliert, sofern und insoweit dies seitens des Auftragnehmers technisch umsetzbar und angemessen ist sowie vom jeweiligen Softwarehersteller unterstützt wird. Regeln- und Zugriffsrechte werden ganz allgemein gemäß den Weisungen der Geschäftsleitung/eines Vorgesetzten und differenziert vergeben. DATEVonline-Anwendungen werden mittels einer 2-Faktor-Authentifizierung abgesichert. Nutzer werden identifiziert; eine Berechtigungsprüfung wird durchgeführt. Die Benutzerverwaltung ist formalisiert; der Kreis der befugten Nutzer begrenzt. Für das Serversystem gilt: Gescheiterte Zugriffsversuche werden protokolliert; die An- und Abmeldedaten sämtlicher Benutzer werden erfasst (Zeitraum: 180 Tage). Angefertigte Protokolldateien werden in Fällen mit einem konkreten Verdachtsmoment unter Beachtung des Vier-Augen-Prinzips ausgewertet. Wird eine RDG-Funktion verwendet, so ist diese mittels einer auf SSL basierenden Technologie abgesichert. Ferner kommen Viwas und DATEVnet zum Einsatz. Datenbankserver sind gesondert und besonders zugriffsgeschützt. Auf der Betriebssystemebene wird überdies sichergestellt, dass eine mehrfache und gleichzeitige Anmeldung über ein Benutzerkonto ausgeschlossen ist. Ganz allgemein ist eine Clean-Desk-Policy vorgegeben und zu beachten. Der Umgang mit verkörperten Daten ist Bestandteil der jährlich stattfindenden Datenschutzschulung (z. B. Unterverschlussnahme, Entnahme aus dem Laufwerk usw.). Es kommt der Microsoft Endpoint Manager (Microsoft Conditional Access) zum Einsatz, über den alle beruflich genutzten Smartphones abgesichert und zentral verwaltet werden (abhängig vom Betriebssystem). Andere Smartphones werden mittels ActiveSync verwaltet. Für die Arbeit mit eigenen Endgeräten existiert eine BYOD-App-Policy Firewalls und Intrusion-Detection-Systemen nach aktuellem Stand der Technik werden für TELEDATA-verwaltete Endgeräte zur Verhinderung und Erkennung von Angriffen eingesetzt und Spamfilter und Virenschutzprogramme (Client und Server) fortlaufend auf dem aktuellsten Stand gehalten (Clients und Server). Bedrohungsschutz ist für die gesamte MS365-Umgebung mit MS-Tools gewährleistet. Eine Firewall- und Network-Policy für TELEDATA-verwaltete Endgeräte mit Vorgaben für den Passwort-Standard liegt vor. Hierdurch ist prüfbar, welcher Verkehr durch eine Firewall erlaubt und welcher verboten ist (Mandatory Access Control: Je nach Absender, Zustelladresse, Protokoll und Sendevorgang erlaubte Datenpakete dürfen passieren (engl. pass), verbotene werden abgelehnt (reject) oder verworfen (deny, drop).

4.1.3 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.

#	Maßnahmen
	Unbefugtes Lesen, Kopieren, Verändern oder Löschen von Datenträgern werden verhindert durch Datenträgerverwaltung-/ Management und gesicherte Schnittstellen. Eine Verwendung externer Datenträger erfolgt nur in Ausnahmefällen in separater Umgebung, es erfolgt ansonsten ein softwareseitigen Ausschluss (via Berechtigungskonzept). Zugriffsbefugnisse werden festgelegt und kontrolliert; dabei wird nach Daten, Programmen und Zugriffsart differenziert. Die zugreifenden Nutzer werden identifiziert. Zugriffe sowie Missbrauchsversuche werden auf einer hohen Gliederungsebene protokolliert. Angefertigte Protokolldateien werden in Fällen mit einem konkreten Verdachtsmoment unter Beachtung des Vier-Augen-Prinzips ausgewertet. Darüber hinaus erfolgt eine Authentisierung mittels Passwort und bei Nutzung der DATEV-online-Anwendungen eine 2-Faktor- Authentifizierung. Es kommt der Microsoft Endpoint Manager (Microsoft Conditional Access) zum Einsatz, über den alle beruflich genutzten Smartphones abgesichert und zentral verwaltet werden (abhängig vom Betriebssystem). Andere Smartphones werden mittels ActiveSync verwaltet. Für die Arbeit mit eigenen Endgeräten existiert eine BYOD-App-Policy. Es besteht ein Freigabeverfahren für neue Nutzer und für Nutzer bei Änderung von Rollen/ Aufgabengebieten.

4.1.4 Trennungsgebot

Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

#	Maßnahmen
	TELEDATA gewährleistet eine Trennungskontrolle durch die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden (insbes. durch Datenbankprinzip, Berechtigungskonzept). Hierzu erfolgen eine Trennung nach unterschiedlichen Sachgebieten und eine logische Trennung von Daten (unternehmensinterne Daten, Kundendaten, sonstige Daten). Die verantwortlichen Mitarbeiter und deren Handlungsspielräume wurden fest zugeordnet.

1.1. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

4.1.5 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.

#	Maßnahmen
	Die TELEDATA IT-Lösungen GmbH ist sich der Tatsache bewusst, dass Wechseldatenträger (z.B. USB-Sticks, externe Festplatten) inventarisiert und verschlüsselt werden müssen. Das Unternehmen bringt die seitens der DATEV angebotene E-Mail-Verschlüsselung zum Einsatz. Die Transportwege der DATEV sind zertifikatsbasiert verschlüsselt. Zugriff von extern erfolgt ausschließlich über gesicherte Verbindungen/ Systeme, es existieren ausschließlich sichere VPN-Zugänge für mobile Arbeitsplätze/ Heimarbeitsplätze. Entsorgungsgut mit schutzwürdigem Inhalt wird physikalisch vernichtet. Dabei wird auf eine ausreichende/angemessene Sicherheitsstufe geachtet, die sich nicht zuletzt an der Schutzklasse des jeweiligen Datenträgers orientiert.

4.1.6 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.

#	Maßnahmen
	Rechteänderungsprotokolle werden geführt, sofern und insoweit dies seitens des Auftragnehmers technisch umsetzbar und angemessen ist sowie vom jeweiligen Softwarehersteller unterstützt wird. Diese Protokolldaten werden gegen Verlust oder Veränderung geschützt, sofern und insoweit dies seitens des Auftragnehmers technisch umsetzbar und angemessen ist sowie vom jeweiligen Softwarehersteller unterstützt wird. Gescheiterte Zugriffsversuche werden protokolliert; die An- und Abmeldedaten sämtlicher Benutzer werden erfasst (Zeitraum: 180 Tage), sofern und insoweit dies seitens des Auftragnehmers jeweils technisch realisierbar und angemessen ist sowie vom jeweiligen Softwarehersteller unterstützt wird. Gemäß dem Datenschutzhandbuch der TELEDATA IT-Lösungen GmbH wird bei einer Auswertung dieser Protokolle nach dem Vier-Augen-Prinzip verfahren.

1.2. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

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

#	Maßnahmen
	Es erfolgen inkrementelle Datenbank- und Systembackups (Gesamtsicherung). Die Datensicherung umfasst die von der TELEDATA IT-Lösungen GmbH genutzten Daten-Server und die dort abgelegten Daten. Zudem werden zusätzliche Server erfasst, die zum Hosting weiterer Funktionen (z.B. CTI) notwendig sind. Das Zeitfenster für die Datensicherung beginnt täglich ab 1:00 Uhr (Mitteleuropäische Zeit). Das Ende bzw. die Dauer der Datensicherung kann je nach Veränderungen der Daten oder Veränderungen im System bzw. der Systemumgebung und dem vorhandenen Datenvolumen variieren. Aufgrund einer Lastverteilung kann eine Aussage, wann die Datensicherung im Einzelnen beginnt und endet, im Vorfeld nicht getroffen werden. Art und Weise sowie technische Realisierung der Datensicherung obliegen der TELEDATA IT-Lösungen GmbH. Es werden 30 tägliche Sicherungspunkte vorgehalten (entspricht 30 Tagen). Die Daten können im Rahmen der Datenrücksicherung auf jeden Endstand vor Beginn einer Sicherung der vorangegangenen 30 Sicherungspunkte wiederhergestellt werden. Nicht in der Datensicherung enthalten sind die Programmserver (Remotedesktopsitzungshosts) der TELEDATA IT-Lösungen GmbH. Es wird eine Erfolgskontrolle der Datensicherung durchgeführt; eventuell auftretende Fehler werden behoben. Daten, die mit MS 365-Diensten verarbeitet werden, unterliegen der Sicherung durch den Dienstleister SkyKick mit einer Sicherungszusage von bis zu 6 Sicherungen/ Tag und ohne Einschränkung bei den Retentionen bzw. Vorhaltezeiträumen.

1.3. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 25 Abs. 1 DSGVO; Art. 32 Abs. 1 lit. d DSGVO)

#	Maßnahmen
	Datenschutz-Management: TELEDATA nutzt ein Datenschutzmanagementsystem (DSMS), in dem alle Maßnahmen, Verfahren, Tätigkeiten etc. im Bereich Datenschutz abgebildet werden. Das DSMS beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen und beinhaltet darüber hinaus einen Maßnahmenplan zur rechtskonformen Umsetzung der EU-Datenschutzgrundverordnung (Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO). Systemmanagement (Monitoring): Interne IT-Systeme werden durch den Einsatz von Sensoren permanent überwacht. Das Monitoring und das Management der gesamten

	Systeme tragen zum Erhalt der Betriebsbereitschaft sowie der Leistungsfähigkeit der Systeme bei. Störungsmanagement: Ungewollte Abweichungen des Systembetriebs, die zu Störungen oder zum Ausfall der Serversysteme führen, stoßen automatisch den internen Störungsmanagementprozess an. Die interne IT führt die erforderlichen Tätigkeiten zur Störungsbehebung an der gesamten TELEDATA-Infrastruktur durch. Change-Management: Neuinstallationen oder Änderungen von Programmen, individuelle Parameter- und Konfigurationsänderungen (nebst Beratungsleistungen und Projektierung) werden im Rahmen eines Änderungsmanagements im Wege der Aufnahme, Prüfung, Spezifikation, Testung und Freigabe wahrgenommen. Incident-Response-Management: Ein internes System zur unverzüglichen Meldung aller Arten von Incidents an die interne IT ist implementiert. In der Anwenderrichtlinie sind Prozesse und Meldewege mit Vorgehen und Verantwortlichen dokumentiert. Zudem kommen Intrusion-Detection-Systeme zur Anwendung. Zudem sind TELEDATA-interne Prozesse zum Umgang mit Datenschutz-/ Datensicherheitsvorfällen, Betroffenenanfragen, Einführung von (neuen) Datenverarbeitungssystemen, ein Dienstleister-/ Lieferantenmanagementsystem usw. implementiert. Entsprechende Vorlagen, Dokumente zum besseren Verständnis sowie zur Dokumentation werden ebenfalls vorgehalten. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO): Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung- und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden.

1.4. Auftragskontrolle

Maßnahmen die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Sollte die TELEDATA IT-LÖSUNGEN GMBH bei der Datenverarbeitung Unterauftragnehmer einsetzen, werden bestimmte Vorgaben umgesetzt. Hierzu zählt die Sicherstellung der technisch-organisatorischen Maßnahmen der Unterauftragnehmer. Zudem stellt die TELEDATA IT-LÖSUNGEN GMBH folgende Voraussetzungen für ein Unterauftragsverhältnis sicher:

#	Maßnahmen
	Die zur Verarbeitung eingereichten Daten werden entsprechend den gesetzlichen Vorschriften nur im Rahmen der Weisungen des jeweiligen Auftraggebers verarbeitet und insbesondere auch nicht an unbefugte Dritte weitergegeben. Der Weisungsrahmen ist insbesondere durch den schriftlich geschlossenen Vertrag zur Datenverarbeitung im Auftrag eindeutig vorgegeben. Gleiches gilt für auftragsbezogene Auskünfte: sie werden ausschließlich an den Auftraggeber oder im Rahmen seiner Weisungen erteilt. Eine flächendeckende Auftragskontrolle ist eingerichtet. Die konkreten Maßnahmen zur Auftragskontrolle beinhalten eine einheitliche und eindeutige Vertragsgestaltung, eine formalisierte Auftragserteilung mit Auftragsformular und

	die Kontrolle der Vertragsausführung. Die Auftragnehmer werden sorgfältig entsprechend den dortigen Datenschutz- und Datensicherheitsstandards ausgewählt.

1.5. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

Entsprechende Verschlüsselungssysteme für Datenträger und mobile Endgeräte sind implementiert (Bitlocker-Verschlüsselung). Verschlüsselungstechnologien bei der Übermittlung von Daten kommen ebenfalls zum Einsatz. Eine Richtlinie zum Umgang mit (mobilen) Datenträgern kommt zur Anwendung. Auch restriktive Zugriffsrechte beim Zugriff auf Server, Datenbanken etc. werden angewandt.

1.6. Externer Datenschutzbeauftragter

Externer Datenschutzbeauftragter gemäß
Art. 37 Datenschutzgrundverordnung (DSGVO):

RA / Fachanwalt IT-Recht Dr. Jens Bücking,
c/o
e|s|b Rechtsanwälte,
Schockenriedstr. 8A,
70565 Stuttgart.

E-Mail: datenschutz@teledata-it.de

Anlage 2: Datenarten- / Kategorien / Kreis der Betroffenen

Art der Daten:

☒ Personenstammdaten (z.B. Name, Anschrift, Geburtsdatum)

☒ Kommunikationsdaten (z.B. Telefon, E-Mail, Fax)

☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☒ Gehaltsdaten und Steuerdaten

☒ Kundenhistorie

☐ Besondere Art personenbezogener Daten (rassische/ethnische Herkunft; politische Meinung; religiöse/philosoph. Überzeugung; Gewerkschaftszugehörigkeit; Gesundheitsdaten; Sexualleben)
Bitte in diesem Fall den Datenschutzbeauftragten informieren.

☒ Vertragsabrechnungs- und Zahlungsdaten

☐ Daten zu Bank- und Kreditkartenkonten

☐ Planungs- und Steuerungsdaten

☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen

☐ Daten zum Krankenversicherungsstatus (z.B. Krankenkasse, Versichertennummer, Status)

☐ Vorgangsbezogene Daten (z.B. Diagnosen, Zuzahlungspflicht, Unfalldatum)

Kreis der Betroffenen:

☒ Kunden des Auftraggebers

☒ Interessenten/Werbekontakte

☒ Beschäftigte

☒ Lieferanten

☒ Handelsvertreter

☒ Ansprechpartner

☒ Beschäftigte von Fremdfirmen

☒ Behörden und sonstige öffentliche Stellen

Anlage 3: Unterauftragnehmer

Eingesetzte Unterauftragnehmer:

- DATEV eG, Nürnberg
- Teamviewer AG, Göppingen
- Anydesk Software GmbH, Stuttgart
- Scutum (Bunk) Sicherheitsdienst GmbH, Schorndorf
- Skykick Inc, Seattle
- Clever Reach, Rastede
- Microsoft Ireland Operations Ltd, Ireland
- mit der TELEDATA IT-Lösungen GmbH im Rechtssinne (§ 15 AktG) verbundene Unternehmen - Freie Mitarbeiter der TELEDATA IT-Lösungen GmbH, die in gleicher Weise auf den Datenschutz verpflichtet worden sind wie deren festangestellte Mitarbeiter: