Ergänzende Bedingungen Auftragsverarbeitung der telegra GmbH (Gesamt-Version 2-5-0 I ab 01.02.2026)

1. Vertragspartner

Vertragspartner sind die telegra GmbH, Oskar-Jäger-Straße 125, 5825 Köln (im Folgenden „telegra“ genannt) und der Kunde, der kein Verbraucher im Sinne von § 13 BGB ist.

2. Geltungsbereich

2.1 Diese „Ergänzenden Bedingungen Auftragsverarbeitung“ (im Folgenden „AVV“ genannt) regeln die datenschutzrechtlichen Rechte und Pflichten der Vertragspartner, sofern und soweit bei der Erfüllung des zugrundeliegenden (Rahmen)Dienstleistungsvertrages und der jeweiligen Einzelleistungsverträge nach den AGB, BGB und den mitgeltenden Vertragsdokumenten personenbezogene Daten des Kunden („Auftraggeber-Daten“) von telegra in dessen Auftrag verarbeitet werden und keine andere AVV zwischen den Vertragsparteien geschlossen wurde.

2.2 Diese AVV findet auf alle Leistungen Anwendung, die von vornherein Gegenstand von Einzelleistungsverträgen sind oder durch die nachträgliche (Hinzu)Beauftragung werden und bei deren Verrichtung und Erfüllung der Auftragsverarbeiter, seine Beschäftigten oder durch den Auftragsverarbeiter nach Maßgabe dieser Vereinbarung einbezogene Unterauftragsverarbeiter, Auftraggeber-Daten verarbeiten.

2.3 Der Kunde hat telegra im Rahmen der Sorgfaltspflichten als Dienstleister ausgewählt. Diese AVV enthält nach dem Willen der Vertragspartner und insbesondere des Kunden den schriftlichen Auftrag zur Auftragsverarbeitung i.S.v. Art. 28 Datenschutzgrundverordnung (DSGVO) und regelt die Rechte und Pflichten der Vertragspartner im Zusammenhang mit der Datenverarbeitung.

2.4 Gegenstand, Art der Daten, Kategorien betroffener Personen sowie Art und Zweck der Verarbeitung der Auftraggeber-Daten ergeben aus **Anlage 1** dieser AVV.

3. Definitionen

3.1 Im Sinne dieser AVV bezeichnet der Begriff **„Auftragsverarbeiter“** eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. „Auftragsverarbeiter“ im Rahmen dieser AVV ist telegra.

3.2 **"Verantwortlicher“** die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. „Verantwortlicher“ im Rahmen dieser AVV ist der Kunde.

3.3 **„Verarbeitung"** bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

3.4 **„Dritter“** bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

3.5 **„Unterauftragsverarbeiter“** bezeichnet den Vertragspartner des Auftragsverarbeiters, der von diesem mit der Durchführung bestimmter Verarbeitungen für den Verantwortlichen beauftragt wird.

3.6 **„Sub-Unterauftragsverarbeiter“** bezeichnet den Vertrags-partner des Unterauftragsverarbeiters, der von diesem mit der Durchführung bestimmter Verarbeitungen für den Verantwortlichen beauftragt wird.

4. Rechte und Pflichten des Kunde

4.1 Der Kunde ist Verantwortlicher (Art. 4 Ziffer 7. DSGVO) für die Verarbeitung der Auftraggeber-Daten durch den Auftragsverarbeiter. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem Kunden.

4.2 Der Kunde wird in seinem Verantwortungsbereich dafür sorgen, dass die gesetzlich notwendigen Voraussetzungen geschaffen werden, damit der Auftragsverarbeiter die vereinbarten Leistungen datenschutzkonform erbringen kann. Er wird insbesondere etwaig erforderliche Einwilligungen bei betroffenen Personen einholen.

4.3 Der Kunde hat das Recht, Weisungen zu Zweck, Art und Umfang der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter zu erteilen. Als grundsätzliche Weisungen sind die AGB, BGB und mitgeteilten Vertragsdokumente sowie diese AVV zu verstehen. Alle späteren Weisungen wird der Kunde schriftlich (Textform) erteilen. Er wird diese mit dem Begriff

„Weisung“ bezeichnen und per E-Mail möglichst an service@telegra.de richten. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Kunde unverzüglich in Textform bestätigen. Der Kunde ist berechtigt, dem Auftragsverarbeiter eine weisungsberechtigte Person zu benennen. Macht er von diesem Recht Gebrauch, wird er den Auftragsverarbeiter unverzüglich schriftlich über einen Wechsel der weisungsberechtigten Person unterrichten.

4.4 Der Kunde ist berechtigt, sich auf eigene Kosten vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der Datenschutzvorschriften und der Umsetzung der Pflichten des Auftragsverarbeiters aus dieser AVV zu überzeugen. Der Auftragsverarbeiter wird die hinreichende Umsetzung, insbesondere der technischen und organisatorischen Sicherheitsmaßnahmen, auf Anforderung durch Zertifizierungen, Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer) oder Eigenerklärungen belegen.

4.5 Der Kunde hat ferner das Recht, die Einhaltung der Datenschutzvorschriften und der Pflichten des Auftragsverarbeiters aus dieser AVV in zu begründenden Fällen vor Ort zu kontrollieren. Der Kunde kann die Kontrollen selbst durchführen oder durch einen von ihm beauftragten Dritten auf seine Kosten durchführen lassen. Vom Kunden mit der Kontrolle beauftragte Personen oder Dritte sind mit Beauftragung nachweislich zur Wahrung der Vertraulichkeit zu verpflichten. Sollte ein vom Kunden beauftragter Prüfer in einem Wettbewerbsverhältnis zum Auftragsverarbeiter stehen, hat der Auftragsverarbeiter hiergegen ein Einspruchsrecht. Der Kunde wird dem Auftragsverarbeiter Kontrollen mit angemessener Vorlaufzeit und unter Nennung des Prüfers ankündigen, eine unterzeichnete Verschwiegenheitserklärung nachweisen und bei der Durchführung der Kontrolle auf Geschäftsbetrieb und Betriebsabläufe beim Auftragsverarbeiter Rücksicht nehmen.

4.6 Der Kunde wird den Auftragsverarbeiter bei Verdacht auf Datenschutzverletzungen und/oder Fehlern oder Unregelmäßigkeiten bei der Verarbeitung der Auftraggeber-Daten unverzüglich und vollständig informieren und den Auftragsverarbeiter bei der Abwehr von Ansprüchen Betroffener oder Dritter sowie bei der Abwehr von Sanktionen durch Aufsichtsbehörden bezogen auf die Auftraggeber-Daten zeitnah und umfänglich unterstützen.

5. Rechte und Pflichten des Auftragsverarbeiters

5.1 Der Auftragsverarbeiter verarbeitet die Auftraggeber-Daten ausschließlich zur Erfüllung des zugrundeliegenden Vertragsverhältnisses nach den AGB, BGB und den mitgeltenden Vertragsdokumenten, dieser AVV und dokumentierter Weisungen des Kunden, es sei denn, er ist durch das Recht der Union oder nationales Recht zur Verarbeitung verpflichtet. In diesem Falle teilt der Auftragsverarbeiter dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Auftragsverarbeiter verwendet die Auftraggeber-Daten für keine anderen Zwecke und wird ihm überlassene Auftraggeber-Daten ohne Zustimmung des Kunden nicht an unberechtigte Dritte weitergeben.

5.2 Der Auftragsverarbeiter wird eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz bestellen und hierbei sicherstellen, dass für den Datenschutz-beauftragten keine Interessenskonflikte entstehen. Der Datenschutzbeauftragte ist unter folgenden Kontaktdaten erreichbar:

E-Mail: datenschutz@telegra.de

5.3 Der Auftragsverarbeiter wird alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeber-Daten treffen.

5.4 Der Auftragsverarbeiter wird die Verarbeitung der Auftraggeber-Daten des Kunden nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchführen. Jede Verlagerung in ein Drittland wird unter Berücksichtigung der besonderen Voraussetzungen der Art. 44 ff DSGVO und des in den Ziffern 7.2 - Ziffern 7.5 dieser AVV festgelegten Verfahrens erfolgen.

5.5 Der Auftragsverarbeiter unterstützt den Kunden dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der entsprechend in Art. 12 – 23 DSGVO (Auskunft, Löschung etc.) genannten Rechte der betroffenen Person nachzukommen. Er wird Weisungen des Kunden ohne schuldhaftes Zögern durchführen und den Kunden über die erfolgte Umsetzung informieren.

5.6 Der Auftragsverarbeiter wird den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei seinen in den Artikeln 32 bis 36 genannten Pflichten unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Kunden wird der Auftragsverarbeiter nur nach vorheriger Weisung durchführen.

5.7 Der Auftragsverarbeiter wird den Kunden unverzüglich darauf aufmerksam machen, wenn eine vom Kunden erteilte Weisung seiner Meinung nach gegen die DSGVO oder andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

5.8 Der Auftragsverarbeiter wird ihm erteilte Weisungen und deren Umsetzung dokumentieren und für ihre Geltungsdauer und anschließend noch für ein volles Kalenderjahr nach Beendigung des betroffenen Einzelleistungsvertrages aufbewahren.

5.9 Der Auftragsverarbeiter wird die Auftraggeber-Daten getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht geschuldet.

5.10 Wird der Kunde durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen, wird der Auftragsverarbeiter den Kunde unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen im erforderlichen Umfang unterstützen, soweit Auftraggeber-Daten von der Verarbeitung betroffen sind.

5.11 Der Auftragsverarbeiter stellt dem Kunden alle erforderlichen Unterlagen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten gemäß Ziffer 4.4 dieser AVV zur Verfügung und ermöglicht ihm Überprüfungen - einschließlich Inspektionen - gemäß Ziffer 4.5 dieser AVV und trägt zu deren Durchführung bei.

6. Technische und organisatorische Maßnahmen

6.1 Auftragsverarbeiter und Kunde müssen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau i.S.v. Art. 32 DSGVO bei der Verarbeitung der Auftraggeber-Daten zu gewährleisten.

6.2 Die vom Auftragsverarbeiter als geeignet angesehenen und getroffenen Maßnahmen sind in **Anlage 2** zu dieser AVV niedergelegt. Der Kunde, dem diese im Zeitpunkt des Vertragsschlusses bekannt sind, akzeptiert diese und trägt die Verantwortung dafür, dass die Maßnahmen für die Risiken der zu verarbeitenden Auftraggeber-Daten ein angemessenes Schutzniveau bieten.

6.3 Eine Änderung der getroffenen Sicherheitsmaßnahmen, insbesondere deren Weiterentwicklung, bleibt dem Auftragsverarbeiter vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen wird der Auftragsverarbeiter dokumentieren.

6.4 Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse und die technischen und organisatorischen Maßnahmen auf ihre Wirksamkeit, um die Verarbeitung der Auftraggeber-Daten in seinem Verantwortungsbereich im Einklang mit der DSGVO durchzuführen. Der Auftragsverarbeiter wird insoweit ein innerbetriebliches Verfahren zur regelmäßigen Überprüfung zur Gewährleistung der Sicherheit der Verarbeitung implementieren.

6.5 Der Kunde wird die Sicherheit der Verarbeitung und die Angemessenheit des Schutzniveaus ebenfalls regelmäßig prüfen und den Auftragsverarbeiter unverzüglich informieren, sollten die getroffenen Sicherheitsmaßnahmen seinen Anforderungen nicht oder nicht mehr genügen.

7. Unterauftragsverhältnisse und Verarbeitung in einem Drittland

7.1 Der Auftragsverarbeiter ist berechtigt, zur Erfüllung seiner Leistungen im Rahmen dieser AVV Unter- und Sub-Unterauftragsverarbeiter mit Genehmigung des Kunden einzusetzen. Er wird diese unter besonderer Berücksichtigung der Eignung der getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählen.

7.2 Für die bereits bei Abschluss der AVV bestehenden Unter- und Sub-Unterauftragsverhältnisse gilt die Genehmigung vom Kunden als erteilt. Die Unter- und Sub-Unterauftragsverarbeiter ergeben sich aus **Anlage 3** dieser AVV.

7.3 Der Kunde erteilt dem Auftragsverarbeiter darüber hinaus die allgemeine Genehmigung für den künftigen Einsatz von weiteren Unter- und/oder Sub-Unterauftragsverarbeitern.

7.4 Der Auftragsverarbeiter wird den Kunden über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung eines Unter-/Sub-Unterauftragsverarbeiters in Textform (z.B. per E-Mail) unter konkreter Benennung des Unter- und/oder Sub-Unterauftragsverarbeiters mit Firmierung und Anschrift sowie Art und Umfang der Datenverarbeitung informieren. Der Kunde hat die Möglichkeit, gegen die angekündigte Änderung innerhalb von vier Wochen nach Zugang der Information schriftlich (Textform) Einspruch zu erheben. Sofern der Kunde von seinem Einspruchsrecht Gebrauch macht und der Auftragsverarbeiter den Unter- und/oder Sub-Unterauftragsverarbeiter trotzdem einsetzt, steht dem Kunden ein Sonderkündigungsrecht zu. Macht der Kunde hingegen von seinem Einspruchsrecht keinen Gebrauch, gilt die Zustimmung des Kunden zum Einsatz des Unter-/Sub-Unterauftragsverarbeiters als erteilt.

7.5 Eine Verlagerung des Ortes der Verarbeitung in einen Drittstaat wird ebenfalls nur in der von den Parteien festgelegten Form nach Maßgabe der Ziffern 7.2 - Ziffer 7.4 und zudem nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff DSGVO (z.B. Angemessenheitsbeschluss der Kommission, Standard-datenschutzklauseln) erfüllt sind.

7.6 Erteilt der Auftragsverarbeiter Aufträge an Unterauftragsverarbeiter, obliegt es ihm, seine datenschutzrechtlichen Pflichten aus dieser AVV dem Unterauftragsverarbeiter zu übertragen und die Einhaltung der vertraglichen datenschutzrechtlichen Verpflichtungen des Unterauftragsverarbeiters zu überprüfen und im Falle von Verstößen Abhilfe zu schaffen. Er wird mit dem Unterauftragsverarbeiter insbesondere Vereinbarungen treffen, die ein angemessenes Datenschutz- und Informationssicherheits-Niveau gewährleisten. Durchgeführte Kontrollen werden dokumentiert und dem Kunden auf Anforderung zur Verfügung gestellt.

7.7 Nicht als Unterauftragsverhältnisse im Sinne von Ziffer 7. gelten Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu den Leistungen, die der Auftragsverarbeiter für den Kunde erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Die Wartung von Systemen und/oder Applikationen stellt ein Unterauftragsverhältnis dar, wenn die Wartung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung der Leistungen für den Kunde genutzt werden und bei denen auf die Auftraggeber-Daten zugegriffen werden kann. Der Auftragsverarbeiter wird auch bei ausgelagerten Nebenleistungen angemessene vertragliche Vereinbarungen treffen sowie Kontrollmaßnahmen ergreifen.

8. Meldepflichten gegenüber dem Kunden

8.1 Der Auftragsverarbeiter wird den Kunden ohne schuldhaftes Zögern über eingetretene oder begründete Verdachtsfälle auf Datenschutzverletzungen und/oder Verstöße gegen diese AVV (z.B. Verstoß gegen Weisung) informieren, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

8.2 Der Auftragsverarbeiter wird den Kunden unverzüglich über Kontrollen oder Maßnahmen, insbesondere Ermittlungsmaßnahmen nach Art. 58 DSGVO informieren, die bei ihm von Aufsichtsbehörden oder anderen Dritten durchgeführt werden, soweit diese Bezüge zur Auftragsverarbeitung und den Auftraggeber-Daten aufweisen.

9. Datengeheimnis und Wahrung der Vertraulichkeit

9.1 Der Auftragsverarbeiter wird bei der Verarbeitung der Auftraggeber-Daten das Datengeheimnis wahren und die gleichen Geheimnisschutzregeln beachten, wie sie dem Kunden als Verantwortlichem obliegen.

9.2 Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der Auftraggeber-Daten befugten Personen gemäß Art. 28 Abs. 3 lit. b) DSGVO zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verpflichtung unterliegen. Der Auftragsverarbeiter weist dem Kunden die wirksame Verpflichtung auf das Datengeheimnis auf Verlangen nach.

9.3 Die Bestimmungen zum Datenschutz und zur Vertraulichkeitsverpflichtung in den AGB bleiben unberührt.

10. Vergütung

10.1 Die Vergütung des Auftragsverarbeiters ist in dem der AVV zugrundeliegenden Vertragsverhältnis vereinbart, in deren Rahmen die Datenverarbeitung erfolgt. Eine gesonderte Vergütung für die Auftragsverarbeitung ist mit Ausnahme einer Vergütung nach Ziffer 10.2 nicht zu entrichten.

10.2 Etwaige Mehraufwände, die durch über das zugrundeliegende Vertragsverhältnis hinausgehende Weisungen des Kunden entstehen, werden als Antrag auf Leistungsänderung behandelt und sind bei einem Mehraufwand für den Auftragsverarbeiter vom Kunden zu vergüten. Die Vertragspartner werden sich über eine angemessene Vergütung gesondert verständigen. Der Auftragsverarbeiter ist nicht verpflichtet, den Leistungsumfang zu erweitern.

11. Vertragsdauer

Die Vertragsdauer dieser AVV entspricht der Vertragsdauer des (Rahmen)Dienstleistungsvertrages.

12. Löschung und Rückgabe

12.1 Der Auftragsverarbeiter wird - soweit aufgrund des Wahlrechts des Kunden nicht abweichend vereinbart - spätestens einen (1) Monat nach Beendigung des jeweiligen Einzelleistungsvertrages sämtliche in seinen Besitz gelangten Daten, Unterlagen und erstellte Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen und die nicht einer gesetzlichen oder vertraglichen Aufbewahrungsfrist unterliegen, datenschutz-gerecht löschen bzw. vernichten/ vernichten lassen. Test- und Ausschussmaterial wird unverzüglich vernichtet oder physisch gelöscht. Die datenschutzgerechte Löschung/Vernichtung wird dem Kunden auf Verlangen bestätigt. Dies betrifft auch etwaige Datensicherungen beim Auftragsverarbeiter.

12.2 Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für ein volles Kalenderjahr nach Beendigung des jeweiligen Einzelleistungsvertrages aufzubewahren.

12.3 Der Kunde hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragsverarbeiter zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragsverarbeiters erfolgen. Die Vor-Ort-Kontrolle muss mit angemessener Frist durch den Kunden angekündigt werden.

13. Haftung

13.1 Der Kunde gewährleistet in seinem Verantwortungsbereich die Umsetzung der sich aus den einschlägigen geltenden rechtlichen Bestimmungen ergebenden Pflichten als Verantwortlicher für die Verarbeitung personenbezogener Daten.

13.2 Für die Haftung des Auftragsverarbeiters nach dieser AVV gelten die Haftungsregelungen in den

Allgemeinen und Besonderen Geschäftsbedingungen des Auftragsverarbeiters.

14. Schlussbestimmungen

14.1 Die **Anlagen 1, 2 und 3** sind integraler Bestandteil dieser AVV.

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

14.3 Änderungen und Ergänzungen dieser AVV müssen schriftlich vereinbart werden und bedürfen des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser AVV handelt.

14.4 Sollten einzelne Teile dieser AVV unwirksam sein, so berührt dies die Wirksamkeit der AVV im Übrigen nicht. Bei etwaigen Widersprüchen der Bestimmungen dieser AVV mit den AGB, BGB und mitgeltenden Vertragsdokumenten im Hinblick auf die im Auftrag verarbeiteten Auftraggeber-Daten gehen die Bedingungen dieser AVV den Regelungen des zugrundeliegenden Vertragsverhältnisses vor.

14.5 Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

14.6 Allgemeiner Gerichtsstand für Streitigkeiten aus und im Zusammenhang mit dieser AVV ist Köln.

Anlage 1 zu den Ergänzenden Bedingungen Auftragsverarbeitung

Die Inhalte dieser Anlage finden Anwendung auf alle vom Kunden während des Bestehens des Rahmendienstleistungsvertrages beauftragten Leistungen bei telegra, bei denen eine Verarbeitung personenbezogener Daten durch telegra im Auftrag des Kunden erfolgt.

1. telegra ACD

1.1 Gegenstand und Zweck der Verarbeitung

- Optimierung der Anruf-Auslastung von Contact Centern über eine webbasiert nutzbare Konfigurationsoberfläche zur automatisierten Anrufverteilung im In- und Outbound.
- telegra stellt dem Kunden die im Einzelleistungsvertrag telegra ACD definierten Leistungen als SaaS zur Verfügung.

1.2 Verarbeitungsort

- Deutschland

1.3 Kategorien betroffener Personen

- Mitarbeiter des Kunden
- Anrufer (Inbound) des Kunden
- Angerufene (In- und Outbound) des Kunden

1.4 Betroffene personenbezogene Daten

- Personenbeziehbare oder personenbezogene Protokolldaten (z.B. IP-Adresse, Logdateien), Konfigurations- und Anmeldedaten (z.B. Benutzername, Passwort, Rufnummer, E-Mail) von Mitarbeitern und ACD-Nutzern des Kunden
- Personenbezogenen Daten, die vom Kunden in eigenem Ermessen im Rahmen der Produktnutzung in die Netz-ACD übermittelt und/oder dort von ihm gespeichert werden
- Anrufdaten (z.B. A-Rufnummer, Zielrufnummer, Datum, Uhrzeit), die dem Kunden zur Auswertung und zur Erstellung von Statistiken zur Verfügung gestellt werden
- Aufzeichnungen von Telefonaten

1.5 Besondere Kategorien personenbezogene Daten (Art. 9 DSGVO)

- Keine

1.6 Erhebung/Zugriff auf personenbezogene Daten

- Der Kunde stellt telegra die personenbezogenen Daten, soweit diese nicht in eigener Verantwortung erhoben werden (z.B. Anrufdaten), zur Verfügung oder erlaubt ihr diese zu erheben.

1.7 Löschung der Auftraggeber-Daten durch telegra

- Die Löschung der Auftraggeber-Daten erfolgt, soweit diese nicht einer gesetzlichen oder vertraglichen Aufbewahrungsfrist unterliegen und keine abweichende Vereinbarung getroffen wurde, spätestens einen (1) Monat nach Vertragsende. Ferner wie nachfolgend beschrieben:
  - Statistikdateien: 180 Tage nach Bereitstellung
  - Aufzeichnungsdateien von Telefonaten: 30 Tage nach Bereitstellung

2. telegra ACD mit AgentAssist

2.1 Gegenstand und Zweck der Verarbeitung

- AgentAssist dient der weiteren Optimierung und Qualitäts-verbesserung von Contact Center-Leistungen durch KI-Funktionen.
- Die Funktionalitäten unterstützen Agenten des Contact Centers mittels KI-Funktionen bei der Beantwortung und Bearbeitung von Anrufer/Angerufenen-Anliegen.
- telegra stellt dem Kunden AgentAssist im Rahmen des SaaS-Einzelleistungsvertrages telegra ACD als optionale zusätzliche Funktionalität zur Verfügung.

2.2 Verarbeitungsort

- Deutschland mit Ausnahme Transkription (vgl. Anlage 3)

2.3 Kategorien betroffene Personen

- Mitarbeiter des Kunden
- Anrufer (Inbound) des Kunden
- Angerufene (In- und Outbound) des Kunden
- Sonstige Personen, zu denen der Kunde personenbezogene Daten zur Verarbeitung an telegra übermittelt

2.4 Betroffene personenbezogene Daten

- Ggfs. Vor- und Nachname des Anrufers/des Angerufenen und des Agenten
- Ob und welche personenbezogenen Daten ferner verarbeitet werden, hängt maßgeblich von der Art der kundenspe-zifischen Anwendungsfälle und der Gestaltung des Telefonats durch den Kunden ab und liegt in dessen Verantwortung.

2.5 Besondere Kategorien personenbezogene Daten (Art. 9 DSGVO)

- Ob und welche besonderen personenbezogenen Daten verarbeitet werden, liegt in der Verantwortung des Kunden.

2.6 Erhebung/Zugriff auf personenbezogene Daten

- Der Kunde stellt telegra alle personenbezogenen Daten, die mit AgentAssist KI-basiert im Auftrag

verarbeitet werden, zur Verfügung und erlaubt ihr, diese zu erheben.

2.7 Löschung der Auftraggeber-Daten durch telegra

- Die Löschung der Auftraggeber-Daten durch telegra erfolgt spätestens einen (1) Monat nach Vertragsende.

3. telegra Contact Center (TCC)

3.1 Gegenstand und Zweck der Verarbeitung

- Kommunikationskanalübergreifende Bearbeitung von Anfragen über eine webbasiert nutzbare Konfigurationsoberfläche zur Optimierung von Contact Centern durch automatisierte Anrufverteilung im In- und Outbound, E-Mail- und Webchat-Kommunikation.
- telegra stellt dem Kunden die im Einzelleistungsvertrag telegra TCC definierten Leistungen als SaaS zur Verfügung.

3.2 Verarbeitungsort

- Deutschland

3.3 Kategorien betroffener Personen

- Mitarbeiter des Kunden
- Anrufer (Inbound) des Kunden
- Angerufene (In- und Outbound) des Kunden
- Absender und Empfänger von E-Mail-Kommunikation des Kunden
- Webchat-Nutzer des Kunden

3.4 Betroffene personenbezogene Daten

- Personenbeziehbare oder personenbezogene Protokolldaten (z.B. IP-Adresse, Logdateien), Konfigurations- und Anmeldedaten (z.B. Benutzername, Passwort, Rufnummer, E-Mail) von Mitarbeitern und TCC-Nutzern des Kunden
- Kontakt- und sonstige personenbezogene Daten, die vom Kunden in eigenem Ermessen ins integrierte telegra CRM-System übermittelt und/oder dort von ihm gespeichert werden (z.B. E-Mails und Webchats)
- Anrufdaten (z.B. A-Rufnummer, Zielrufnummer, Datum, Uhrzeit, E-Mail-Kommunikation), die dem Kunden zur Auswertung und zur Erstellung von Statistiken zur Verfügung gestellt werden
- Aufzeichnungen von Telefonaten und Webchats

3.5 Besondere Kategorien personenbezogene Daten

- Keine

3.6 Erhebung/Zugriff auf personenbezogene Daten

- Der Kunde stellt telegra die personenbezogenen Daten, soweit diese nicht in eigener Verantwortung erhoben werden (z.B. Anrufdaten) zur Verfügung oder erlaubt ihr diese zu verarbeiten.

3.7 Löschung der Auftraggeber-Daten durch telegra

- Die Löschung der Auftraggeber-Daten erfolgt, soweit diese nicht einer gesetzlichen oder vertraglichen Aufbewahrungsfrist unterliegen und keine abweichende Vereinbarung getroffen wurde, spätestens einen (1) Monat nach Vertragsende. Ferner wie nachfolgend beschrieben:
  - Aufzeichnungsdateien von Telefonaten: 30 Tage nach Bereitstellung
  - Statistikdateien: 180 Tage nach Bereitstellung
  - Webchat-Verläufe: mit Löschung des vom Kunden hinterlegten Kontakts
  - E-Mails: spätestens 30 Tage nach Eingang

4. telegra CloudCall - Virtuelle TK-Anlage

4.1 Gegenstand und Zweck der Verarbeitung

- Bereitstellung einer virtuellen TK-Anlage im Netz zur webbasierten Nutzung durch den Kunden über eine Konfigurationsoberfläche.
- telegra stellt dem Kunden die im Einzelleistungsvertrag telegra CloudCall definierten Leistungen als SaaS in zur Verfügung.

4.2 Verarbeitungsort

- Deutschland

4.3 Kategorien betroffener Personen

- Mitarbeiter des Kunden
- Anrufer und Angerufene des Kunden

4.4 Betroffene personenbezogene Daten

- Personenbeziehbare oder personenbezogene Protokolldaten (z.B. IP-Adresse, Logdateien), Konfigurations- und Anmeldedaten (z.B. Benutzername, Passwort, Rufnummer) von Mitarbeitern und CloudCall Nutzern des Kunden
- Personenbezogenen Daten, die vom Kunden in eigenem Ermessen im Rahmen der Produktnutzung übermittelt und/oder dort von ihm gespeichert werden (z.B. Adressbücher)
- Anrufdaten (z.B. A-Rufnummer, Zielrufnummer, Datum, Uhrzeit), die dem Kunden zur Auswertung und zur Erstellung von Statistiken zur Verfügung gestellt werden

4.5 Besondere Kategorien personenbezogene Daten

- Keine

4.6 Erhebung/Zugriff auf personenbezogene Daten

- Der Kunde stellt telegra die personenbezogenen Daten, soweit diese von telegra nicht in eigener Verantwortung erhoben werden (z.B. Anrufdaten) zur Verfügung.

4.7 Löschung der Auftraggeber-Daten durch telegra

- Die Löschung der Auftraggeber-Daten erfolgt, soweit diese nicht einer gesetzlichen oder vertraglichen Aufbewahrungsfrist unterliegen und keine abweichende Vereinbarung getroffen wurde, spätestens einen (1) Monat nach Vertragsende.

5. telegra KIT - Voicebot

5.1 Gegenstand und Zweck der Verarbeitung

- Automatisierung einzelner Abläufe mittels Künstlicher Intelligenz (KI) -Mechanismen nach Vorgabe des Kunden. Zweck der Verarbeitung ist die semantische Analyse des Anliegens des Anrufers und die Konfiguration einer aufgrund des Analyseergebnisses automatisierten Aktion (z.B. automatisierte Antwort oder ein Routing des Anrufs auf eine bestimmte Rufnummer).
- telegra stellt dem Kunden ein nach Vorgaben und auf Datenbasis des Kunden lernendes Cloud-System („Bot“) als SaaS zur Verfügung
- Transkription des gesprochenen Anrufer-Anliegens in Text (Speech to Text) zur automatisierten Erkennung des Anliegens
- Synthese von Text in Sprache (Text to Speech) zur automatisierten Beantwortung von Anliegen.

5.2 Verarbeitungsort

- Deutschland mit Ausnahme Transkription/Synthese (vgl. Anlage 3)

5.3 Kategorien betroffener Personen

- Mitarbeiter des Kunden
- Anrufer des Kunden

5.4 Betroffene personenbezogene Daten

- Vom Kunden beim Anrufer abgefragtes telefonisches Anliegen
- Time Stamp des Anrufs

5.5 Besondere Kategorien personenbezogene Daten

- Keine

5.6 Erhebung/Zugriff auf personenbezogene Daten

- Der Kunde stellt telegra die personenbezogenen Daten, soweit diese nicht in eigener Verantwortung erhoben werden (z.B. Anrufdaten) zur Verfügung oder erlaubt ihr diese zu erheben.

5.7 Löschung der Auftraggeber-Daten durch telegra

- Voicebot-Trainingsdaten: Manuell durch den Kunden, spätestens einen (1) Monat nach Vertragsende durch telegra, soweit keine abweichende Vereinbarung getroffen wurde.

6. telegra Insight

6.1 Gegenstand und Zweck der Verarbeitung

- Transkription von Sprachdateien in maschinenlesbare Form zur Auswertung der Inhalte der Transkripte (z.B. zur Qualitätskontrolle).
- telegra stellt dem Kunden ein Cloud-System zur Verfügung, auf das der Kunde aus telegra-internen und externen (Dritt)-Systemen stammende Sprachdateien zur Transkription und zur kundenindividuellen Auswertung der Transkripte übertragen kann.

6.2 Verarbeitungsort

- Deutschland

6.3 Kategorien betroffener Personen

- Mitarbeiter des Kunden
- Anrufer des Kunden

6.4 Betroffene personenbezogene Daten

- Konfigurations- und Anmeldedaten (Anmeldename, Gruppe, Call-Classifikation(en) von Mitarbeitern und Insight-Nutzern des Kunden
- Vom Kunden an die Plattform telegra Insight übermittelte Sprachdateien mit Metadaten (Zeitpunkt, Call-ID, Hotline, Agent, ggf. Rufnummer des Anrufers)
- Automatisch erstellte Transkripte der Sprachdateien, kombiniert mit Metadaten (s. o.)

6.5 Besondere Kategorien personenbezogene Daten

- Keine

6.6 Erhebung/Zugriff auf personenbezogene Daten

- Der Kunde stellt telegra die personenbezogenen Daten zur Verfügung und erlaubt telegra, diese zu verarbeiten. Dies gilt ausdrücklich auch für die Sprachdateien.

6.7 Löschung der Auftraggeber-Daten durch telegra

- Die Löschung der Auftraggeber-Daten erfolgt, soweit keine abweichende Vereinbarung getroffen wurde, spätestens einen (1) Monat nach Vertragsende. Ferner wie nachfolgend beschrieben:
- Sprachdateien: 30 Tage nach Eingang auf der Cloud-Plattform

7. telegra Control

7.1 Zweck der Verarbeitung

- Kundenportal zur webbasierten Konfiguration von Diensten, Rufnummern etc. mit weiteren Funktionen
- telegra stellt dem Kunden die telegra Control Leistungen als SaaS zur Verfügung.

7.2 Verarbeitungsort

- Deutschland

7.3 Kategorien betroffener Personen

- Mitarbeiter des Kunden

7.4 Betroffene personenbezogene Daten

- Personenbeziehbare oder personenbezogene Protokolldaten (z.B. IP-Adresse, Logdateien), Konfigurations- und Anmeldedaten (z.B. Benutzername, Passwort, Rufnummer) von Mitarbeitern des Kunden
- Personenbezogenen Daten, die vom Kunden in eigenem Ermessen übermittelt und im Kundenportal gespeichert werden (z.B. Listenroutings)
- Anrufdaten (z.B. A-Rufnummer, Zielrufnummer, Datum, Uhrzeit), die dem Kunden zur Auswertung und zur Erstellung von Statistiken zur Verfügung gestellt werden.

7.5 Weitere betroffene personenbezogene Daten bei Nutzung besonderer Control-Funktionalitäten

- Fax2Mail: Faxinhalt und Empfänger-Mail-Adresse

  Auf zuvor festgelegten Rufnummern des Auftraggebers eingehende Faxe werden "zwischengespeichert" und als PDF-Anhang per E-Mail an vom Auftraggeber vorgegebene E-Mail-Adressen gesendet.
- Mail2Fax: Fax-Absender

  Dokumente, die als Mail-Anhang auf vom Kunden zuvor festgelegten Mail-Adressen eingehen, werden als Fax-Dokumente an vom Kunden zuvor bestimmte (Fax)Nummern gesendet. Hierfür werden die Mail-Anhänge für den Versand "zwischengespeichert".

7.6 Besondere Kategorien personenbezogene Daten

- Keine

7.7 Erhebung/Zugriff auf personenbezogene Daten

- Der Kunde stellt telegra die personenbezogenen Daten, soweit diese nicht in eigener Verantwortung erhoben werden (z.B. Anrufdaten) zur Verfügung oder erlaubt ihr diese zu erheben.

7.8 Löschung der Auftraggeber-Daten durch telegra

- Die Löschung der Auftraggeber-Daten erfolgt, soweit diese nicht einer gesetzlichen oder vertraglichen Aufbewahrungs-frist unterliegen und keine abweichende Vereinbarung getroffen wurde, spätestens einen (1) Monat nach Vertragsende. Ferner wie nachfolgend beschrieben:
  - Statistikdateien: 180 Tage nach Bereitstellung
  - Mail2Fax:

    Mail-Anhang: 30 Tage nach Versand

    Empfänger-Faxnummer: Mit Beendigung der Mail2Fax-Konfiguration durch den Kunden, spätestens einen (1) Monat nach Vertragsende.
  - Fax2Mail:

    Fax-Dokument: 30 Tage nach Versand
    Empfänger-Mail-Adressen: Mit Beendigung der Fax2Mail-Konfiguration durch den Kunden, spätestens einen (1) Monat nach Vertragsende.

8. telegra Digitale Rufnummer

8.1 Gegenstand und Zweck der Verarbeitung

- Herstellung von WebRTC-Anrufen über einen QR-Code/Link u.a. mit der Möglichkeit für den Kunden, in eigenem Ermessen Daten vom Web-User zur schnelleren Bearbeitung zu erheben.
- Kundenportal zur webbasierten Konfiguration des Dienstes, Rufnummern etc. mit weiteren Funktionen

8.2 Verarbeitungsort

- Deutschland

8.3 Kategorien betroffener Personen

- Web-User/Anrufer des Kunden,
- Mitarbeiter des Kunden

8.4 Betroffene personenbezogene Daten

- Personenbeziehbare oder personenbezogene Protokolldaten (z.B. IP-Adresse, Logdateien), Konfigurations- und Anmelde-daten (z.B. Benutzername, Passwort, Rufnummer, E-Mail) von Mitarbeitern des Kunden.
- Personenbezogenen Daten, die vom Kunden in eigenem Ermessen im Rahmen der Produktnutzung vom Web-User/ Anrufer erhoben und an telegra zur Verarbeitung übermittelt werden.
- Anrufdaten (z.B. Zielrufnummer, Datum, Uhrzeit), die dem Kunden zur Auswertung und zur Erstellung von Statistiken zur Verfügung gestellt werden
- Aufzeichnungen von WebRTC-Anrufen

8.5 Besondere Kategorien personenbezogene Daten (Art. 9 DSGVO)

- Keine

8.6 Erhebung/Zugriff auf personenbezogene Daten

- Der Kunde stellt telegra die personenbezogenen Daten, soweit diese nicht in eigener Verantwortung von telegra erhoben werden (WebRTC-Anrufdaten), zur Verfügung oder erlaubt ihr diese zu verarbeiten.

8.7 Löschung der Auftraggeber-Daten durch telegra

- Die Löschung der Auftraggeber-Daten erfolgt, soweit diese nicht einer gesetzlichen oder vertraglichen Aufbewahrungsfrist unterliegen und keine

abweichende Vereinbarung getroffen wurde, spätestens einen (1) Monat nach Vertrags-ende. Ferner wie nachfolgend beschrieben:

- Erhobene Daten des Web-Users: 180 Tage nach Bereitstellung
- Statistikdateien: 180 Tage nach Bereitstellung
- Aufzeichnungsdateien WebRTC-Anrufe: 30 Tage nach Anrufdatum

Anlage 2 zu den Ergänzenden Bedingungen Auftragsverarbeitung

Technisch organisatorische Maßnahmen

Für die beauftragte Erhebung und/oder Verarbeitung von personenbezogenen Daten werden folgende am jeweiligen Schutzziel orientierte Maßnahmen zwischen telegra und dem Kunden vereinbart:

I. Das Schutzziel der Vertraulichkeit der Daten

Die Verpflichtung zur Wahrung der Vertraulichkeit ergibt sich u.a. aus Art. 5 Abs. 1, Art. 32 Abs. 1b) sowie Art. 38 Abs. 5 DSGVO bzw. Art. 28 Abs. 3 b) DSGVO. Sie soll den Schutz vor unbefugter und unrechtmäßiger Verarbeitung gewährleisten. Die Vertraulichkeit wird bereichs- und systembezogen über verschiedenen Maßnahmen sichergestellt:

Zutrittskontrolle

Die Verhinderung eines unbefugten (räumlichen) Zutritts zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, wird durch verschiedene Maßnahmen gewährleistet:

- Einteilung des Gebäudes in Sicherheitsbereiche
- Türsicherung (elektrische Türöffner)
- Zutrittskontrollsystem durch personalisierten Token, teilweise mit zusätzlicher PIN
- Schlüssel / Schlüsselvergabe an berechtigte Personen
- Sicherung der Racks durch Schlösser
- Verzicht auf Ausschilderung des Rechenzentrums
- Überwachungseinrichtungen (Zutritt, Videoüberwachung)
- Verhaltensregeln für Firmenfremde
- Dokumentation der Anwesenheit von Besuchern (Besucherausweis)

Zugangskontrolle/Verschlüsselung

Das Eindringen Unbefugter in die Datenverarbeitungssysteme wird durch folgende technische und organisatorische Maßnahmen verhindert:

- Festlegung von Zugangsberechtigungen
- Zugangssicherung (Verschlüsselung, VPN)
- Automatisierte Kontrolle durch Protokollierung des Zugangs
- Anwesenheitsaufzeichnungen in bestimmten Sicherheits-bereichen
- Einrichtung eines Benutzerstammsatzes pro User
- Zugang zu EDV-Systemen nur mit Benutzerkennung und individuellem Passwort
- Bildschirmsperre an Arbeitsstationen, automatische Sperrung bei längerer Abwesenheit
- Zugänge zu IT-Systemen werden bei wiederholt erfolglosen Anmeldeversuchen automatisch gesperrt

Zugriffs- und Speicherkontrolle

Zur Verhinderung unerlaubter Tätigkeiten der Berechtigten (unbefugte Kenntnisnahme, Veränderung und Löschung) in Datenverarbeitungssystemen sowie der unbefugten Kenntnisnahme erfolgt eine am Schutzbedarf orientierte Ausgestaltung der Berechtigungen und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- Datenspeicherung in eigenen Datacentern in Deutschland
- Festlegung der Zugriffs- und Benutzerberechtigungen nach dem „Need to know Prinzip“
- Legitimation der Zugriffs- und Benutzerberechtigungen
- Differenzierte Berechtigungen (Rollen)
- Überwachung administrativer Fernzugriffe
- Automatisierte oder manuelle Auswertung von Protokollen
- Regelmäßige Überprüfung der Berechtigungen; Entzug nicht mehr erforderlicher Berechtigungen (u.a. Ein- und Austritt, Abteilungswechsel)

Trennungskontrolle / Zweckbindungskontrolle

Die Verpflichtung, Daten ausschließlich für den Zweck zu verarbeiten, zu dem sie erhoben wurden, wird gewährleistet durch:

- "Interne Mandantenfähigkeit", Zweckbindung, getrennte Verarbeitung
- Trennung: Produktion / Test
- Vorhandensein von Richtlinien
- Vorhandensein von Stellenbeschreibungen
- Vorhandensein von Programmierrichtlinien
- Überwachung der Einhaltung der Regelungen
- Umsetzung einer Funktionstrennung, z.B. durch Vier-Augen-Prinzip

II. Das Schutzziel der Integrität der Daten

Das Gewährleistungsziel der Integrität, das in Art. 5 Abs. 1 f) DSGVO als Grundsatz für die Verarbeitung von Daten und in Art. 32 Abs. 1 b) DSGVO als Voraussetzung für die Sicherheit einer Datenverarbeitung genannt wird und ein unbefugtes Ändern und Entfernen von Daten ausschließen soll, wird durch folgende Maßnahmen sichergestellt:

Eingabekontrolle

Die Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind, erfolgt durch:

- Dokumentation der Eingabeverfahren
- Automatisierte Protokollierung der Dateneingabe, Änderung, Löschung
- Protokollierung gescheiterter Zugriffsversuche

- Protokollierung der Historie des Systemverwalters und sämtlicher Benutzer
- Sicherung der Protokolldaten gegen Verlust und Veränderung durch Verschlüsselung

Transport- bzw. Weitergabekontrolle

Die Transport- bzw. Weitergabekontrolle wird durch Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während des 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 durch Einrichtungen zur Datenübertragung vorgesehen ist, wie folgt umgesetzt:

- Übermittlungen von personenbezogenen Daten sind im Template zur Erfassung von Verarbeitungstätigkeiten (Grundlage für Verarbeitungsverzeichnis) dokumentiert
- Festlegung der Stellen, an die Daten übermittelt werden dürfen
- Lagerung von Datenträgern in bestimmten Bereichen
- Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)
- Protokollierung über Logfiles und Datenbankeinträge
- Kontrollierte Vernichtung von Datenträgern
- Vorhandensein einer Regelung zur Klassifizierung von Dokumenten und Dateien
- Vorhandensein und Durchführung einer Regelung zur Weitergabe klassifizierter Daten
- Verwenden privater Datenträger ist untersagt
- Besucher haben keinen Zugriff auf betriebliches LAN/WLAN (gesondertes Gast-WLAN)
- Vernichtung von Datenträgern durch zertifizierten Entsorger

III. Das Schutzziel der Verfügbarkeit der Daten

Der Grundsatz der Verfügbarkeit hat an mehreren Stellen Einklang in der DSGVO gefunden. Er soll die Verfügbarkeit der Daten zu dem jeweiligen Zweck, solange dieser noch besteht, gewährleisten und wird durch folgende Maßnahmen umgesetzt:

Verfügbarkeitskontrolle

Zur Verhinderung einer zufälligen Zerstörung oder dem Verlust von Daten werden verschiedene Maßnahmen zur Datensicherung (physikalisch / logisch) realisiert. Die Angaben beziehen sich auf eigene IT-Systeme:

- Erstellung eines Datensicherheitskonzepts
- Vorhandensein und Umsetzung eines Konzepts zur redundanten Datenhaltung (Backup-Richtlinie)
- Spiegeln von Festplatten, z.B. RAID-Verfahren
- Vorhandensein und Prüfung von Notstromaggregaten und Überspannungsschutzeinrichtungen
- Schadsoftwareschutz Virenschutz / Firewall
- Sicherheitsrelevante Updates und Patches werden regelmäßig zeitnah eingespielt
- Gesicherte Lagerung von Datenträgern

IV. Das Schutzziel der Belastbarkeit der Systeme

Wiederherstellbarkeit

Die Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können, erfolgt durch:

- Erstellung eines Notfallhandbuches
- Erstellung von Wiederanlaufplänen
- Regelmäßige Backup-Läufe aller Systeme
- Image-Generierung von Laufzeitsystemen
- Regelprozess zur Einrichtung von Backup-Mechanismen bei Servern
- Regelmäßige Überprüfung der Backup-Mechanismen, z.B. durch Log-Dateien
- Geographisch getrennte Lagerung von Backup-Medien

Zuverlässigkeit

Die Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können, erfolgt durch:

- Technische Überwachungs- und Monitoringsysteme mit Alarmierungsfunktion
- Log-Dateien
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regeln und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarung, Verpflichtung auf die Vertraulichkeit)
- Rechtevergabe nach dem Erforderlichkeitsprinzip
- Implementierung eines Authentisierungsverfahrens

V. Das Schutzziel der Pseudonymisierung

Art. 32 Abs. 1 lit.a) und Art. 25 Abs. 1 DSGVO fordern Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen durch Datenminimierung und Pseudonymisierung zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung.

Pseudonymisierung

Die Gewährleistung, dass personenbezogene Daten in einer Weise verarbeitet werden, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen, soll durch folgende Maßnahmen Rechnung getragen werden:

- Prüfung und Erfassung der Verarbeitungsprozesse vor deren Einführung unter Berücksichtigung einer Pseudonymisierung von Daten im Verarbeitungsverzeichnis

VI. Das Schutzziel der Sicherheit der Verarbeitung bei einer Auftragsverarbeitung

Auftragskontrolle

Zur Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Kunden verarbeitet werden können, erfolgt eine Abgrenzung der Kompetenzen zwischen Kunde und Auftragsverarbeiter und eine Dokumentation der Weisungen des Kunden

- Sorgfältige Auswahl von Unterauftragsverarbeitern
- Dokumentation der Kriterien zur Auswahl von Unterauftragsverarbeitern
- Festlegung eindeutiger Vertragsbestimmungen
- Eindeutige Vertragsgestaltung (entsprechend der geltenden Vorschriften)
- Formalisierte Auftragserteilung
- Kontrolle der Vertragsausführung
- Verarbeitung aufgrund schriftlicher (auch elektronischer) Weisungen

VII. Verfahren zur Wiederherstellung und Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Nutzung eines Notfallhandbuchs. Das Notfallhandbuch definiert den Notfall, legt die Verantwortlichkeiten fest und beschreibt das Vorgehen, d.h. die Reihenfolge, in der vom Notfall betroffene Systeme wiederhergestellt werden, die Kommunikation mit Betroffenen, Kunden und Behörden, auch im Blickwinkel mit personenbezogenen Daten.

„Einfache“ technische oder physische Störungen an Einzelsystemen, die zu einem Verlust personenbezogener Daten führen oder führen können, werden wir folgt behandelt:

- Bei Server-Ausfall Wiederherstellung der Systeme aus Images der Laufzeitsysteme
- Bei Datenverlust Wiederherstellung der Daten aus dem Backup-System
- Inbetriebnahme der betroffenen Systeme gemäß der Wiederanlaufpläne
- Überprüfung der wiederhergestellten Systeme
- Freigabe für den Betrieb
- Ggf. Information der Aufsichtsbehörde und/oder der Betroffenen gemäß Meldeverfahren

VIII. Verfahren Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

telegra ist gemeinsam mit der IN-telegence GmbH, dem technischen Dienstleister und Plattformbetreiber von telegra im sog. Multi Site Verfahren gemäß ISO27001 zertifiziert und besitzt zudem eine Konformitätsbescheinigung gemäß DIN EN ISO/IEC 27701:2021 über die wirksame Anwendung der DIN EN ISO/IEC 27701:2021 Sicherheitstechniken - Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz erhalten.
telegra nutzt das Informationssicherheits- und Datenschutz-Management-System auch zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen. Ermittelte Risiken und deren Behandlung werden dokumentiert (Risikobehandlungsplan). Der Fortschritt der Maßnahmenumsetzung und die Wirksamkeit der Maßnahmen werden regelmäßig überprüft und ebenfalls dokumentiert.