

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag gemäß § 11 BDSG

(Auftragsdatenverarbeitung - ADV)

„Legitimationsrichtlinie Prepaid“ – ADV Vertriebspartner

Zwischen

Demcom GmbH
Mergenthaler Allee 79-81
65760 Eschborn

- im Folgenden „Auftraggeber“ genannt -

und

[Name, vollständige Firmierung und Adresse des Vertriebspartners]

[bitte ausfüllen]

- im Folgenden „Auftragnehmer“ genannt -

- Auftraggeber und Auftragnehmer einzeln oder gemeinsam im Folgenden: „der Vertragspartner“ oder „die Vertragspartner“ genannt -

Präambel

Dieser Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragspartner. Der Vertrag findet Anwendung auf die Überprüfung der Identität (Legitimation) von Kunden gemäß „Legitimationsrichtlinie Prepaid“ und die dazu erhobenen, verarbeiteten und/oder genutzten Daten („**Auftraggeber-Daten**“).

Sollte bereits ein ADV-Vertrag zwischen dem Auftraggeber und dem Auftragnehmer bestehen, geltenden die folgenden Regelungen als Ergänzung des bereits bestehenden ADV-Vertrages. Bei Widerspruch der Regelungen gehen die Regelungen dieses ADV-Vertrages für den in der Anlage 1 Ziffer 1.1. benannten Auftragsgegenstand vor.

§ 1 Vertragsgegenstand, Zweck der Datenerhebung, -verarbeitung und -nutzung, Verantwortlichkeit

(1) Zweck, Art und Umfang der Erhebung, Verarbeitung und Nutzung von Auftraggeber-Daten im Sinne dieses Vertrags sowie die Art der Daten und der Kreis der Betroffenen ergibt sich aus **Anlage 1**.

(2) Der Auftraggeber bleibt im Rahmen dieses Vertrages verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG.

(3) Die Inhalte dieses Vertrags gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann.

§ 2 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Auftraggeber-Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen (§ 4).

(2) Der Auftragnehmer sichert zu, sämtliche Auftraggeber-Daten unverzüglich unwiederbringlich zu löschen, sobald diese nicht mehr für Zwecke dieses Vertrages benötigt werden, soweit nicht in einer Einzelweisung des Auftraggebers etwas anderes bestimmt wurde; dies beinhaltet insbesondere auch Daten auf Backup-Speichermedien und Datenträgern. Der Auftragnehmer sichert weiter zu, Auftraggeber-Daten entsprechend den Weisungen des Auftraggebers zu berichtigen, wenn diese unrichtig sind, und Auftraggeber-Daten entsprechend den gesetzlichen oder vertraglichen Regelungen zu sperren.

(3) Der Auftragnehmer garantiert in seinem Verantwortungsbereich die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird in seinem Verantwortungsbereich technische und organisatorische Maßnahmen entsprechend § 9 Bundesdatenschutzgesetz umsetzen und einhalten. Eine Auflistung dieser technischen und organisatorischen Maßnahmen erfolgt in **Anlage 2** zu diesem Vertrag.

(4) Soweit erforderlich, stellt der Auftragnehmer dem Auftraggeber die für die Übersicht nach § 4g Abs. 2 S. 1 BDSG notwendigen Angaben zur Verfügung. Falls ein betrieblicher Datenschutzbeauftragter bestellt wurde, teilt der Auftragnehmer dem Auftraggeber die Kontaktdaten seines betrieblichen Datenschutzbeauftragten mit.

(5) Der Auftragnehmer verpflichtet sich zur Einhaltung des Datengeheimnisses. Er stellt sicher, dass die mit der Verarbeitung der Auftraggeber-Daten befassten Mitarbeiter gemäß § 5 Bundesdatenschutzgesetz (Datengeheimnis) in Schriftform verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes und des Telekommunikationsgesetzes eingewiesen und über ein datenschutzkonformes Verhalten aufgeklärt worden sind. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

(6) Der Auftragnehmer ist dazu verpflichtet, sowohl seinen Datenschutzbeauftragten als auch den Auftraggeber bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Verletzungen des Schutzes personenbezogener Daten (§ 109a TKG, § 15a TMG, § 42a BDSG), bei Verstößen gegen die im Auftrag getroffenen Festlegungen oder Weisungen des Auftraggebers und/ oder Unregelmäßigkeiten bei der Verarbeitung der Auftraggeber-Daten unverzüglich zu informieren. Regelmäßig hat der Auftragnehmer den Auftraggeber über Vorfälle, die zwischen 8:00 und 16:00 Uhr eintreten, binnen 2 Stunden nach Bekanntwerden zu informieren. Tritt der Vorfall zwischen 16:00 und 8:00 Uhr ein, so hat der Auftragnehmer den Auftraggeber hierüber ebenfalls innerhalb von 2 Stunden zu informieren, spätestens jedoch bis 10 Uhr.

Der Auftragnehmer ist verpflichtet, die weitere Verarbeitung und Nutzung von Auftraggeber-Daten mit dem Auftraggeber unverzüglich abzustimmen. Der Auftragnehmer ist weiter verpflichtet, unverzüglich alle erforderlichen Maßnahmen einzuleiten, um entstandene oder drohende Gefährdungen für die Integrität, Authentizität, Vertraulichkeit und/oder Verfügbarkeit der Auftraggeber-Daten zu beseitigen bzw. auszuschließen.

(7) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen, z.B. auf CD-ROM, DVD-ROM, DVD-RAM, Blu-ray und ähnlichen WORM-type Einwegdatenträgern, verbleiben im Eigentum des Auftraggebers. Dies gilt nicht für Datenträger, die in der IT-Infrastruktur des Auftragnehmers installiert sind, einschließlich – aber nicht beschränkt auf – Festplatten, Storage-Area-Networks, Network-Attached-Storage und Backup-Speichermedien. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Unbefugten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf Anforderung jederzeit Auskünfte zu den Auftraggeber-Daten und Unterlagen zu erteilen.

(8) Der Auftragnehmer sichert zu, dass er die Daten des Auftraggebers ausschließlich innerhalb des Europäischen Wirtschaftsraums (EWR) verarbeitet und nutzt oder durch Subunternehmer, soweit nach § 6 (Subunternehmer) zulässig, verarbeiten und nutzen lässt.

(9) Der Auftragnehmer erwirbt an den Auftraggeber-Daten keine Rechte und ist auf Verlangen des Auftraggebers jederzeit zur Herausgabe der Auftraggeber-Daten verpflichtet. Zurückbehaltungsrechte in Bezug auf Auftraggeber-Daten sind ausgeschlossen. Dem Auftragnehmer ist es insbesondere nicht gestattet, für eigene Zwecke Tests durchzuführen, Analysen, interne Reportings bzw. Profile mit bzw. auf Grundlage der Auftraggeber-Daten zu erstellen. Ausnahmen muss der Auftraggeber in Textform gesondert zustimmen.

(10) Der Auftragnehmer führt angemessene Kontrollen der Einhaltung der Vorgaben aus diesem Vertrag und der Weisungen des Auftraggebers, insbesondere bezüglich der Umsetzung und Wirksamkeit der technischen und organisatorischen Maßnahmen durch, die er zum Schutz der Auftraggeber-Daten getroffen hat, mindestens einmal pro Kalenderjahr. Insbesondere prüft er die Maßnahmen und Prozesse zur Realisierung einer wirksamen Zutritts-, Zugriffs- und Zugangskontrolle.

Die Durchführung und die Ergebnisse der Selbstkontrolle sind zu dokumentieren und für die gesamte Vertragslaufzeit, mindestens jedoch für 24 Monate, zu archivieren und auf Anforderung des Auftraggebers binnen einem Werktag in Textform zur Verfügung zu stellen. Stellt der Auftragnehmer Abweichungen oder Lücken zu den vertraglichen Vorgaben fest oder ist die Wirksamkeit einer Maßnahme nicht vorhanden, ist der Auftraggeber unverzüglich über die Art der Abweichung sowie die geplante Maßnahme zur Behebung der Abweichung und den geplanten Umsetzungszeitpunkt zu unterrichten.

Der Auftraggeber behält sich das Recht vor, dem Auftragnehmer Vorgaben in Form von Prüflisten zur Durchführung der Selbstkontrolle zu geben. Diese sind durch den Auftragnehmer bei der nächsten, turnusgemäßen Selbstkontrolle anzuwenden.

Sofern der Auftragnehmer für wesentliche Teile des Auftrages (Hauptleistungspflichten) einen oder mehrere Subunternehmer verpflichtet, ist der jeweilige Subunternehmer ebenfalls zur Durchführung dieser Selbstkontrollen zu verpflichten. Über festgestellte Abweichungen im Rahmen der Unterbeauftragung ist der Auftraggeber ebenfalls zu unterrichten. § 6 (Subunternehmer) sowie die gesetzlichen Pflichten des Auftragnehmers zur Durchführung von Kontrollen bei den Subdienstleistern bleiben unberührt.

§ 3 Anfragen an den Auftraggeber

(1) Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen, vorausgesetzt der Auftraggeber hat den Auftragnehmer hierzu in Textform aufgefordert.

(2) Soweit sich ein Betroffener unmittelbar an den Auftragnehmer zwecks Berichtigung, Sperrung oder Löschung seiner Daten oder wegen einer Auskunft wenden sollte, wird der Auftragnehmer entsprechende Anfragen unverzüglich an den Auftraggeber weiterleiten. Gleiches gilt, wenn sich Behörden mit Anfragen an den Auftragnehmer richten.

(3) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über behördliche Anfragen gemäß § 113 TKG und informiert die anfragende Behörde, dass der Auftragnehmer zur Auskunftserteilung weder in der Lage noch berechtigt ist.

§ 4 Weisungen

(1) Der Umgang mit den Auftraggeber-Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. § 11 Abs. 3 Satz 1 BDSG). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.

(2) Der Auftragnehmer verwendet die Auftraggeber-Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an andere als vom Auftraggeber definierte Dritte weiterzugeben. § 6 (Subunternehmer) bleibt unberührt. Duplikate und Kopien (auch Sicherheitskopien, die zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind) werden ohne Zustimmung des

Auftraggebers, die in Textform erteilt werden muss, nicht erstellt. Sollte die Zustimmung erteilt werden, unterliegen die Datenverarbeitungen den Vereinbarungen dieses Vertrags.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen gesetzliche Vorschriften verstößt, so ist der Auftragnehmer verpflichtet, den Auftraggeber hierauf unverzüglich hinzuweisen, sowie berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung in Textform durch den Auftraggeber auszusetzen.

§ 5 Kontrollrecht

(1) Der Auftraggeber kann sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers überzeugen. Hierfür kann er insbesondere nach seiner Wahl Selbstauskünfte des Auftragnehmers einholen (vgl. § 2 Abs. 10), sich ein Testat eines Sachverständigen vorlegen lassen oder sich gemäß nachfolgendem Absatz 2 persönlich überzeugen.

(2) Der Auftraggeber, sein (Konzern-)Datenschutzbeauftragter, die für den Auftraggeber zuständige Aufsichtsbehörde sowie vom Auftraggeber beauftragte Dritte haben das Recht, nach vorheriger Ankündigung von zehn (10) Werktagen (in dringenden Fällen auch ohne Vorankündigung) die Geschäftsräume des Auftragnehmers zu den üblichen Geschäftszeiten zu betreten, um sich zeitlich und räumlich uneingeschränkt von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Maßnahmen zur Datensicherheit sowie von der Einhaltung der einschlägigen Datenschutzbestimmungen und der Einhaltung der vertraglichen Regelungen zum Datenschutz und zur Datensicherheit, einschließlich der auftragsgemäßen Erhebung, Verarbeitung und Nutzung der Auftraggeber-Daten, zu überzeugen. Der Auftragnehmer gewährt dem Auftraggeber, dem Datenschutzbeauftragten des Auftraggebers und/oder vom Auftraggeber beauftragten Dritten die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte. Entsprechende Mitwirkungspflichten obliegen dem Auftragnehmer auch gegenüber der für den Auftraggeber zuständigen Aufsichtsbehörde(n).

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung in Textform innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer umfassenden Auftragskontrolle erforderlich sind.

§ 6 Subunternehmer

(1) Die Beauftragung von Subunternehmern mit der Erbringung von Haupt- oder Nebenleistungen durch den Auftragnehmer darf nur mit vorheriger Zustimmung des Auftraggebers und unter Beachtung der in § 6 Abs. 2 niedergelegten Bedingungen erfolgen. Eine Unterbeauftragung liegt vor, wenn bei der Erhebung, Verarbeitung oder Nutzung der Auftraggeber-Daten oder bei der Prüfung, dem Support oder der Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch den Auftragnehmer Subunternehmer einbezogen werden und die Möglichkeit des Zugriffs auf die Auftraggeber-Daten nicht ausgeschlossen ist (§ 11 Abs. 1 und 5 BDSG). Als Subunternehmen gelten auch Konzern- und/ oder Tochtergesellschaften des Auftragnehmers. Nicht Subunternehmer im Sinne dieses Vertrags sind die mit dem Auftragnehmer vertraglich verbundenen Mitarbeiter, die unter Beachtung von § 2 Abs. 5 dieser Vereinbarung nachweislich auf das Datengeheimnis verpflichtet wurden.

(2) Werden Subunternehmer durch den Auftragnehmer eingeschaltet, so werden die vertraglichen Vereinbarungen zwischen Auftragnehmer und Subunternehmer so gestaltet, dass sie den Anforderungen zu Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages entsprechen. Dem Auftraggeber und der für den Auftraggeber zuständigen Aufsichtsbehörde sind Kontroll- und Überprüfungsrechte beim Subunternehmer entsprechend § 5 dieser Vereinbarung einzuräumen. Insbesondere hat der Auftragnehmer die Einhaltung der gesetzlichen Vorgaben gem. § 11 BDSG sicherzustellen und sich vor Beginn der unterbeauftragten Verarbeitung von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen. Die Form und das Ergebnis dieser Überprüfung ist dem Auftraggeber vor Beginn der unterbeauftragten Verarbeitung mitzuteilen.

Auf Verlangen des Auftraggebers hat der Auftragnehmer die von ihm für die Beauftragung von Subunternehmern (konzernintern oder extern) verwendeten Vertragsformulare sowie eine Kopie der jeweils mit den beauftragten Subunternehmern geschlossenen Datenschutzverträge zur Verfügung zu stellen. Der kommerzielle Teil dieser Verträge ist nicht vorzulegen, soweit dieser keine Relevanz für die Verarbeitung von Auftraggeber-Daten hat.

Der Auftragnehmer hat die von ihm eingesetzten Subunternehmen zu benennen. Der Auftragnehmer hat die Informationen zu Subunternehmen, die für die Auftragsdatenverarbeitung eingesetzt werden sollen, in einer Liste (**Anlage 3**) aufzuführen und nach Unterzeichnung dieses ADV-Vertrages – jedoch noch vor Durchführung der Auftragsdatenverarbeitung – dem Auftraggeber auszuhändigen. Der Einsatz der in der Liste aufgeführten Subunternehmen gilt als genehmigt, wenn der Auftraggeber vier Wochen nach Zugang der Liste keinen Widerspruch äußert. Sollte der Auftragnehmer nach Beginn der Auftragsdatenverarbeitung neue Subunternehmen einsetzen wollen, hat er die Anlage hinsichtlich der neuen Subunternehmen auszufüllen. Der Einsatz der neuen

Subunternehmen gilt ebenfalls vier Wochen nach Zugang der Liste ohne Widerspruch des Auftraggebers als genehmigt. Sollte ein Subunternehmen nicht mehr eingesetzt werden, so ist der Auftraggeber ebenfalls anhand der Liste zu informieren.

(3) Sofern eine Weitergabe der Auftraggeber-Daten innerhalb des Konzerns/ Unternehmensverbunds des Auftragnehmers für die Datenverarbeitung im Rahmen dieses Vertrages erforderlich sein sollte, so hat der Auftragnehmer dem Auftraggeber ein Konzept zum konzerninternen Datentransfer vorzulegen. Diesem Konzept muss der Auftraggeber schriftlich oder in Textform zustimmen, bevor Auftraggeber-Daten von einem anderen Unternehmen innerhalb des Konzerns/ Unternehmensverbund des Auftragnehmers verarbeitet werden oder dieses Zugriff auf Auftraggeber-Daten erhält.

(4) Eine Beauftragung von Subdienstleistern, die ihren Sitz außerhalb der EU/des EWR haben oder die aus Ländern außerhalb der EU/des EWR auf Auftraggeber-Daten zugreifen können, ist untersagt (§ 2 Abs. 8 dieses Vertrags), es sei denn, der Auftraggeber hat dem ausdrücklich und schriftlich zugestimmt. Der Auftragnehmer verpflichtet sich in diesem Fall, den Abschluss aller datenschutzrechtlich erforderlichen Verträge herbeizuführen, insbesondere erforderlichenfalls unmittelbar zwischen dem Auftraggeber und dem Subdienstleister abzuschließende Vereinbarungen. Die Zustimmung kann – auch in diesem Fall – ohne Angabe von Gründen durch den Auftraggeber eingeschränkt oder verweigert werden.

Der Abschluss erforderlicher Verträge zwischen Auftraggeber und Subunternehmern entbindet den Auftragnehmer nicht von seiner Verpflichtung zur Kontrolle seiner Subunternehmer. Zudem hat der Auftragnehmer den Auftraggeber in angemessener Weise bei der Kontrolle der Subunternehmer durch den Auftraggeber oder bei dem Ergreifen anderer erforderlicher und im Rahmen des Vertrages zwischen Auftraggeber und Subunternehmer zulässiger Maßnahmen zu unterstützen.

Sollte aufgrund (künftiger) behördlicher, gerichtlicher oder gesetzlicher Anforderungen der Beitritt des Auftragnehmers zu dem EU-Standardvertrag zwischen Auftraggeber und Subunternehmer erforderlich sein, hat der Auftragnehmer die Vereinbarung zwischen Auftraggeber und Subunternehmer unverzüglich mit zu unterzeichnen. Der Auftragnehmer hat sicherzustellen, dass der Subunternehmer rechtzeitig seine Zustimmung zu dem Vertragsbeitritt des Auftragnehmers gibt, zudem ist der Auftragnehmer dafür verantwortlich, dass der Subunternehmer die in dem Vertrag mit dem Auftraggeber übernommenen Verpflichtungen erfüllt.

Wird die Übermittlung von Daten des Auftraggebers, einzelner Datenkategorien oder spezieller Verarbeitungen in Drittstaaten unzulässig (z.B. aufgrund von gesetzlichen, gerichtlichen und/ oder behördlichen Verpflichtungen/ Untersagungen), so hat der Auftragnehmer die Übermittlung auf Anforderung des Auftraggebers unverzüglich einzustellen.

§ 7 Vertragsdauer

(1) Dieser Vertrag wird auf unbestimmte Zeit geschlossen. Die Kündigungsfrist beträgt 3 Monate. Einvernehmlich kann der Vertrag von beiden Seiten mit sofortiger Wirkung aufgehoben werden.

(2) Mit Beendigung dieses Vertrags ist die Auftragsdatenverarbeitung durch den Auftragnehmer einzustellen. Der Auftragnehmer hat die Auftraggeber-Daten nach Wahl und Vorgabe des Auftraggebers vollständig datenschutzgerecht zu löschen oder an den Auftraggeber herauszugeben (einschließlich etwaiger verfahrens- oder sicherheitstechnisch notwendiger Kopien).

(3) Der Auftragnehmer hat auf Anforderung des Auftraggebers eine Dokumentation und Bestätigung der vollständigen Löschung oder Herausgabe zu erteilen.

(4) Auch über den Zeitpunkt der Vertragsbeendigung hinaus, bleiben die Verpflichtungen aus §§ 2, 3, 5 und 7 Abs. 3 dieses Vertrages bestehen.

§ 8 Freistellung

Der Auftragnehmer stellt den Auftraggeber von jeglichen Ansprüchen Dritter, die auf der Verletzung von Pflichten des Auftragnehmers aus diesem Vertrag beruhen, frei.

§ 9 Sonstiges, Allgemeines

(1) Die **Anlagen** sind verpflichtender Bestandteil dieses Vertrages.

(2) Sollten Auftraggeber-Daten beim Auftragnehmer durch Pfändung, Durchsuchung 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 an den Auftraggeber-Daten beim Auftraggeber liegt. Dies gilt ebenso, wenn Auftraggeber-Daten auf Datenträgern des Auftragnehmers gespeichert werden, die von einer Maßnahme nach Satz 1 betroffen sind.

(3) Änderungen und Ergänzungen dieses Vertrags und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses Vertrags handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(4) Soweit im Hauptvertrag nichts Abweichendes bestimmt ist, gilt deutsches Recht und der Gerichtsstand München.

(5) Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden, oder eine an sich notwendige Regelung nicht enthalten sein, so wird dadurch die Wirksamkeit der übrigen Bestimmungen dieses Vertrages nicht berührt. Anstelle der unwirksamen Bestimmung oder zur Ausfüllung der Regelungslücke gilt eine rechtlich zulässige Regelung, die so weit wie möglich dem entspricht, was die Parteien gewollt haben oder nach Sinn und Zweck dieses Vertrages gewollt hätten, wenn sie die Regelungslücke erkannt hätten.

Anlagen:

- **Anlage 1:** Allgemeine Angaben zum Auftrag
- **Anlage 2:** Darstellung der technischen und organisatorischen Maßnahmen des Auftragnehmers

Auftraggeber:

(Ort, Datum)

(Name des Unterzeichnenden)

(Unterschrift und Stempel)

(Ort, Datum)

(Name des Unterzeichnenden)

(Unterschrift und Stempel)

Auftragnehmer:

(Ort, Datum)

(Name des Unterzeichnenden)

(Unterschrift und Stempel)

(Ort, Datum)

(Name des Unterzeichnenden)

(Unterschrift und Stempel)

Anlage 1: Angaben zum Auftrag

1.1.	Gegenstand, Art und Umfang der Datenverarbeitung	Identitätsüberprüfung gemäß § 111 TKG und der Vorgaben aus der „Legitimationsrichtlinie Prepaid“ bei Kunden, die einen Prepaid-Vertrag abschließen möchten (Erhebung von Kundendaten, Überprüfung der Identität des Kunden anhand des vorgelegten Legitimationspapiers, Überprüfung des vorgelegten Legitimationspapiers auf Echtheit, Gültigkeit und Zulässigkeit, Weitergabe der Daten an Auftraggeber mittels Telefónica ID Scan APP und EPOS)
1.2.	Gegenüber dem Auftragnehmer weisungsbefugte Abteilung des Auftraggebers	
1.3.	Dauer des Auftrags	Beginn: 01.07.2017 Ende: unbefristet
1.4.	Zweck der Verarbeitung und Nutzung	Begründung eines Vertragsverhältnisses mit Teilnehmern (Erhebung und Validierung der Kundendaten)
1.5.	Vom Auftragnehmer verarbeitete Datenkategorien	personenbezogene Daten der Teilnehmer gemäß § 111 TKG (z.B. Rufnummer, Name, Adresse, Geburtsdatum, Legitimationspapiere) (siehe „Legitimationsrichtlinie Prepaid“)
1.6.	Betroffene Personengruppe	TK-Dienste-Teilnehmer

Anlage 2: Beschreibung der technischen und organisatorischen Maßnahmen, die der Auftragnehmer gemäß § 2 Abs. 3 dieses Vertrages eingeführt hat

Diese Maßnahmen sind neben der Einhaltung der Vorgaben der „Legitimationsrichtlinie Prepaid“ zum Umgang mit Daten und Dokumenten im Rahmen der Identitätsprüfungen nach § 111 TKG vom Auftragnehmer als Mindestmaßnahmen einzuhalten.

2.1.	Folgende Maßnahmen zur räumlichen Zutrittskontrolle sind ergriffen worden, die es Unbefugten verwehren, sich den Systemen, Datenverarbeitungsanlagen und Devices physisch zu nähern, mit denen der Vertriebspartner personenbezogene Daten im Rahmen der Identitätsprüfung nach § 111 TKG erhebt und verarbeitet.	<ul style="list-style-type: none"> • Schlüsselverwaltung / Dokumentation der Schlüsselvergabe • Abschließen der Geschäftsräume außerhalb der Öffnungszeiten • Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.) • Schutz vor Einsichtnahme und akustischer Wahrnehmung durch Dritte (z.B. gesonderter abgetrennter Bereich für Identitätsprüfung)
2.2.	Folgende Maßnahmen zur Zugangskontrolle sind ergriffen worden, die verhindern, dass ein Zugriff durch Unbefugte auf Datenverarbeitungssysteme beim Vertriebspartner erfolgt.	<ul style="list-style-type: none"> • Persönlicher und individueller User-Login bei Anmeldung am System, Device bzw. Unternehmensnetzwerk • Automatische Sperrung der Clients und sonstigen Devices nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung) • Sichere Verwahrung und Verwendung von Zugangsdaten, • Jederzeitiger Schutz der Zugangsdaten vor Zugriffen Unberechtigter
2.3.	Folgende Maßnahmen zur Zugriffskontrolle sind ergriffen worden, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Vertriebspartner ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Identitätsprüfung nach § 111 TKG nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	<ul style="list-style-type: none"> • Verwaltung und Dokumentation von Berechtigungen • Regelmäßige Prüfung der Aktualität von Zugriffsrechten • Passwort-Identifikation (individuell pro Mitarbeiter vergeben)

2.4.	Folgende Maßnahmen zur Weitergabekontrolle sind ergriffen worden, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder ihrer Speicherung auf Datenträgern 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.	<ul style="list-style-type: none"> • Gesichertes WLAN • ausschließliche Nutzung der Plattformlösung(en) und Apps des Auftraggebers für alle eingesetzten Systeme und Devices • Keine Weitergabe der im Rahmen der Prozesse nach § 111 TKG zu verwendenden Devices, Software und/oder Zugangs-/Zugriffspasswörter • Keine Nutzung von Devices mit ‚Jailbreak‘ • Nutzung aktuellster Versionen zu nutzender Software • Regelmäßige Sicherheitsüberprüfung der verwendeten Devices
2.5.	Folgende Maßnahmen zur Auftragskontrolle sind ergriffen worden, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	<ul style="list-style-type: none"> • Schulungen aller zugriffsberechtigten Mitarbeiter zu den datenschutz- und telekommunikationsrechtlichen Anforderungen sowie zur „Legitimationsrichtlinie Prepaid“ • Regelmäßige Nachschulungen • Regelmäßige Kontrollen
2.6.	Folgende Maßnahmen zur Verfügbarkeitskontrolle sind ergriffen worden, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	<ul style="list-style-type: none"> • Service Level Agreements (SLAs) mit Dienstleistern • Virenschutz / Firewall in aktuellster Version bzw. Konfigurierung
2.7.	Folgende Maßnahmen zur Einhaltung des Trennungsgebots sind ergriffen worden, die gewährleisten, dass Daten, die zu unterschiedlichen Zwecken erhoben werden, getrennt verarbeitet (z.B. gelöscht) werden können.	<ul style="list-style-type: none"> • Rechte- und Rollenkonzepte • Trennung durch Zugriffsregelungen

