

## Besondere Bestimmungen zur Auftragsverarbeitung nach Art. 28 DS-GVO

### 1. Vertragspartner

Vertragspartner sind die ETK networks solution GmbH (im Folgenden „ETK networks“ genannt) und der Kunde, der nicht Verantwortlicher i.S.v. Art. 4 Ziff. 7 DSGVO ist.

### 2. Geltungsbereich und Vertragsgegenstand

**2.1** Diese Besonderen Bestimmungen zur Auftragsverarbeitung und ihre Anlage finden Anwendung und werden Bestandteil der Verträge zwischen ETK networks und dem Kunden, wenn und soweit ETK networks im Rahmen der Erbringung von Leistungen personenbezogene Daten des Kunden verarbeitet (z.B. bei Leistungen des myApps Cloud-Service oder Wartungs- und/oder Supportleistungen sowie Leistungen im Zusammenhang mit Schulungen und Online-Trainings) und die DS-GVO und ggf. weitere Datenschutzgesetze hierauf Anwendung finden.

**2.2** Gegenstand der Vereinbarung ist die Regelung der Rechte und Pflichten des Verantwortlichen (nachfolgend „Kunde“ genannt) und des Auftragsverarbeiters (nachfolgend „ETK networks“ genannt), sofern im Rahmen der Leistungserbringung auf der Grundlage eines Vertrages und den jeweils geltenden Allgemeinen Geschäftsbedingungen (AGB), z.B. für den myApps Cloud-Service, eine Verarbeitung personenbezogener Daten durch ETK networks für den Kunden im Sinne des anwendbaren Datenschutzrechtes stattfindet. Die Verarbeitung gilt entsprechend für die Fern-Prüfung (z.B. Remote-Zugriff) und/oder Wartung im Rahmen der Leistungserbringung, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

**2.3** Aus dem jeweiligen Vertrag nebst den AGB (z.B. Besondere Bestimmungen über den myApps Cloud-Service) sowie diesen ergänzenden Besonderen Bestimmungen für Auftragsverarbeitung sowie der Anlage zu diesen Besonderen Bestimmungen ergeben sich Rechtsgrundlage, Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie die Kategorien der betroffenen Personen.

**2.4** Allgemeine Geschäftsbedingungen des Kunden werden grundsätzlich nicht Bestandteil der vertraglichen Vereinbarung zwischen den Parteien. Etwas anderes gilt nur, wenn sie von ETK networks schriftlich bestätigt wurden.

**2.5** Der Vertrag zur Auftragsverarbeitung wird erst durch schriftliche Bestätigung von ETK networks verbindlich. Erfolgt der Vertragsschluss im elektronischen Rechtsverkehr, gibt der Kunde durch das Anklicken des Bestätigungsbuttons auf elektronischem Wege ein Angebot auf Abschluss eines Vertrages (rechtsgeschäftliche Erklärung) ab und akzeptiert darüber hinaus diese Besonderen Bestimmungen zur Auftragsverarbeitung.

### 3. Vertragsdauer/Laufzeit des Auftragsverarbeitungsvertrages

Die Laufzeit des Auftragsverarbeitungsvertrages richtet sich nach der Dauer des Vertrages (z.B. über den myApps Cloud-Service) und endet spätestens mit Einstellung der tatsächlichen Erbringung der Leistungen durch ETK networks.

### 4. Rechte und Pflichten des Kunden/Verantwortlichen

**4.1** Der Kunde ist als Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe sowie für die Rechtmäßigkeit der Datenverarbeitung, allein verantwortlich. Ihm obliegt insb. die Beurteilung der Zuverlässigkeit des Auftragsverarbeiters und die Prüfung der Rechtmäßigkeit der Datenverarbeitung sowie die Wahrung der Rechte der Betroffenen. Der Kunde wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen geschaffen werden, damit ETK networks die vereinbarten Leistungen auch insoweit rechtsverletzungsfrei erbringen kann.

**4.2** Darüber hinaus hat der Kunde ETK networks unverzüglich zu informieren, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Verarbeitungstätigkeit durch ETK networks feststellt.

### 5. Pflichten von ETK networks als Auftragsverarbeiter

**5.1** ETK networks darf personenbezogene Daten nur auf dokumentierte Weisung des Kunden verarbeiten, außer es liegt ein Ausnahmefall gem. Art. 28 Abs. 3 a) DS-GVO vor. ETK networks informiert den Kunden unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. ETK networks darf die Umsetzung der Weisung solange aussetzen, bis sie vom Kunden bestätigt oder abgeändert wurde.

**5.2** ETK networks wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Kunden treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. ETK networks 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.

**5.3** Die derzeit als geeignet angesehenen Maßnahmen („TOM“) sind in der Anlage zu diesen Allgemeinen Geschäftsbedingungen für Auftragsverarbeitung beschrieben. Der Kunde hat die technischen und organisatorischen Maßnahmen von ETK networks vor dem Hintergrund der konkreten Datenverarbeitung im Hinblick auf ein angemessenes Schutzniveau bewertet und als angemessen akzeptiert. Eine Änderung der getroffenen IT-Sicherheitsmaßnahmen bleibt ETK networks vorbehalten, wobei jedoch sichergestellt sein muss, dass das zum Zeitpunkt des Vertragsabschlusses angemessene Schutzniveau nicht unterschritten wird. ETK networks gewährleistet, ihren Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

**5.4** ETK networks unterstützt den Kunden im Rahmen ihrer Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

**5.5** ETK networks gewährleistet, dass es den mit der Verarbeitung der Daten des Kunden befassten Mitarbeitern und andere für sie tätigen Personen untersagt ist, die Daten außerhalb der Weisung des Kunden zu verarbeiten. Ferner gewährleistet ETK networks, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder in einem angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages bzw. nach Beendigung der Leistungserbringung fort.

**5.6** Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Kunden und darf nur erfolgen, wenn die besonderen Voraussetzungen des Art. 44 ff. DSGVO erfüllt sind.

**5.7** ETK networks wird einen Datenschutzbeauftragten benennen, sofern dies von dem anwendbaren Recht der EU oder dem anwendbaren Recht des Mitgliedstaates, dem ETK networks unterliegt, gefordert wird. Die Kontaktdaten des Datenschutzbeauftragten sind auf der Webseite von ETK networks in der Datenschutzzinformatoren (Art. 13, 14 DS-GVO) einsehbar.

**5.8** Im Falle einer Inanspruchnahme des Kunden durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich ETK networks den Kunden bei der Abwehr des Anspruches im Rahmen ihrer Möglichkeiten zu unterstützen.

### 6. Löschung und Rückgabe von Daten

**6.1** ETK networks berichtigt oder löscht nicht mehr benötigte personenbezogene Daten, wenn der Kunde dies anweist und dies vom Weisungsrahmen umfasst ist.

**6.2** Personenbezogene Daten werden spätestens nach Auftragsende gelöscht. Der Kunde ist dafür verantwortlich sicherzustellen, dass die notwendigen Datensicherungen (z.B. Backups) vorgenommen werden. Darüber hinaus hat er rechtzeitig Daten zu exportieren, insbesondere sofern gesetzliche Aufbewahrungsfristen und/oder Speicherpflichten bestehen.

### 7. Anfragen Betroffener

Wendet sich eine betroffene Person mit Forderungen bzw. Anträgen zur Berichtigung, Löschung oder Auskunft an ETK networks, wird ETK networks diese an den Kunden verweisen. ETK networks leitet die Anträge des Betroffenen unverzüglich an den Kunden weiter und unterstützt den Kunden im Rahmen ihrer Möglichkeiten bei der Erfüllung der Anträge gem. Kapitel III der DS-GVO (Rechte der Betroffenen).

### 8. Nachweis- und Kontrollrechte

**8.1** ETK networks stellt dem Kunden auf dessen Aufforderung hin alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO genannten Pflichten zur Verfügung und ermöglicht Überprüfungen – einschließlich Inspektionen –, die vom Kunden oder einem von ihm beauftragten Prüfer durchgeführt werden, bzw. unterstützt diese.

**8.2** ETK networks informiert den Kunden unverzüglich, wenn ihr Verletzung des Schutzes personenbezogener Daten des Kunden bekannt werden oder sie der Auffassung ist, dass eine Weisung des Kunden gegen die DS-GVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. ETK networks stellt die zur Sicherung der Daten und Minderung möglicher nachteiliger Folgen betroffener Personen erforderlichen Mittel bereit und spricht sich hierzu unverzüglich mit dem Kunden ab.

**8.3** Sollten im Einzelfall Inspektionen durch den Kunden 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. ETK networks darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitsklärung hinsichtlich der

unternehmensinternen Daten abhängig machen. Sollte der durch den Kunden beauftragte Prüfer in einem Wettbewerbsverhältnis zu ETK networks oder dem Hersteller innovaphone stehen, hat ETK networks gegen dessen Beauftragung ein Einspruchsrecht.

#### **9. Unterbeauftragte/Subunternehmer**

**9.1** Beim Einsatz von Subunternehmern als Unterauftragsverarbeiter gelten die Vorschriften des § 28 Abs. 4 S.1 DS-GVO, d.h. diesen werden durch einen Vertrag oder ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht des Mitgliedstaates dieselben Datenschutzpflichten nach dem Vertrag über Auftragsverarbeitung und diesen Besonderen Bestimmungen für Auftragsverarbeitung auferlegt.

**9.2** Die Liste der von ETK networks eingesetzten Unterauftragsverarbeiter ergibt sich aus der Anlage zu diesen Besonderen Bestimmungen für Auftragsverarbeitung.

**9.3** Der Kunde erteilt ETK networks die allgemeine Genehmigung zum Einsatz weiterer Unterauftragsverarbeiter. ETK networks wird den Kunden über das Ersetzen und/oder den Einsatz neuer Unterauftragsverarbeiter informieren. Der Kunde hat die Möglichkeit, binnen 14 Tagen nach der Mitteilung Einspruch zu erheben. Erfolgt kein Einspruch, so gilt der (neue) Subunternehmer als genehmigt (Fiktion).

#### **10. Haftung/Haftungsfreistellung**

**10.1** Der Kunde gewährleistet in seinem Verantwortungsbereich die Umsetzung der sich aus den einschlägigen geltenden rechtlichen Bestimmungen ergebenden Pflichten hinsichtlich der Verarbeitung personenbezogener Daten.

**10.2** Sofern Dritte Ansprüche gegen ETK networks wegen der Verletzung datenschutzrechtlicher Bestimmungen geltend machen, die auf einem Verstoß des Kunden gegen datenschutzrechtliche Bestimmungen und/oder gegen die Bestimmungen dieser Vereinbarung beruhen, trägt der Kunde sämtliche Kosten, einschließlich der Rechtsverfolgungskosten, d.h. der Verteidigung in einem außergerichtlichen Verfahren, einem Rechtsstreit und/oder verwaltungsgerichtlichen Verfahren und stellt ETK networks von sämtlichen Ansprüchen auf erstes Anfordern frei. Vertragliche Haftungsbeschränkungen zu Gunsten von ETK networks (z.B. gemäß den Allgemeinen Geschäftsbedingungen) bleiben im Übrigen unberührt.

#### **11. Geltendes Recht, Gerichtsstand**

**11.1** Auf diese Besonderen Bestimmungen für Auftragsverarbeitung und den jeweils zugrundeliegenden Vertrag über Auftragsverarbeitung findet deutsches Recht unter Ausschluss des UN-Kaufrechts Anwendung.

**11.2** Die Beseitigung von Erfüllungsort für Lieferungen und Leistungen sowie der Ort der Nacherfüllung ist München.

**11.3** Nebenabreden, Änderungen oder Ergänzungen dieser Besonderen Bestimmungen für die Auftragsverarbeitung bedürfen zu ihrer Wirksamkeit der Unterzeichnung beider Vertragsparteien oder deren bevollmächtigten Vertretern. Dies gilt auch für die Abänderung dieses Schriftformerfordernisses.

**11.4** Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit der Auftragsverarbeitung ist München. Ein etwaiger ausschließlicher Gerichtsstand ist vorrangig.

#### **12. Teilunwirksamkeit/Salvatorische Klausel**

Sollten einzelne Bestimmungen dieser Besonderen Bestimmungen für Auftragsverarbeitung unwirksam, nichtig oder undurchführbar sein oder werden, wird die Wirksamkeit der übrigen Bestimmungen der Besonderen Bestimmungen für Auftragsverarbeitung im Übrigen davon nicht berührt. Es besteht Einigkeit, dass in einem solchen Fall diejenige Regelung gilt, die dem angestrebten wirtschaftlichen Zweck der unwirksamen, nichtigen oder undurchführbaren Bestimmung im Rahmen einer an Sinn und Zweck orientierten Auslegung am nächsten kommt. Die vorstehende Regelung gilt entsprechend, sollte sich eine Regelungslücke der Besonderen Bestimmungen für Auftragsverarbeitung herausstellen.

## Anlage zu den Allgemeinen Geschäftsbedingungen zur Auftragsverarbeitung (Art. 28 DS-GVO)

### 1. Einzelheiten der Datenverarbeitung

#### a) Angaben zu den „Kategorien von Verarbeitungen“:

- Leistungen im Rahmen des myApps Cloud Service bzw. Betrieb der PBX (Telefonanlage) und Kommunikationsplattform in der Cloud
- Supportleistungen im Zusammenhang mit der PBX (Telefonanlage) / und myApps Cloud-Kommunikationsplattform des Kunden (remote oder On-Premises)
- Wartungsleistung bei Hardwarewartung/RMA
- Leistungen im Rahmen der Zertifizierung und Qualifizierung von Partnern oder Endkunden (über Plattformen)

#### b) Kategorien betroffener Personen:

- Teilnehmer in der Telefonanlage/Kommunikationsplattform des Verantwortlichen
- Externe Dritte als Systemverantwortliche der PBX (Telefonanlage) des Verantwortlichen
- Externe Dritte als Leistungsempfänger (RMA, Hardwarewartung und Support)
- Externe Dritte als Leistungsempfänger von Schulungen/Trainings

#### c) Betroffene personenbezogene Daten:

- Kontakt- und Präsenzdaten der Teilnehmer der Telefonanlage/Kommunikationsplattform und externen Dritten (Systemverantwortliche) des Verantwortlichen
- Personenbezogene Protokolldaten (z.B. Benutzernamen/-kennung, IP-Adresse)
- Inhaltsdaten von aufgezeichneten Nachrichten/Gesprächen (z.B. Voice-/Mailbox) oder Sprachnachrichten (z.B. Chatnachrichten)
- Kontaktdaten von Leistungsempfängern (z.B. Telefonnummer, Name, email, etc.)
- Qualifizierungsdaten von Schulungsteilnehmern

#### d) Besondere Kategorien von personenbezogenen Daten:

Keine

### 2. Zugriff auf personenbezogene Daten

ETK networks ermöglicht dem Kunden die Nutzung der PBX (Telefonanlage) und Kommunikationsplattform in der Cloud, bzw. die Nutzung von Plattformen (z.B. für Schulungen). Dadurch werden kundenseitige, personenbezogene Daten durch ETK networks und durch den Hersteller innovaphone als (Hosting-)Provider verarbeitet sowie darüber hinaus auf Basis gesonderter Verträge Leistungen im Bereich des Supports, der Wartung / Fernwartung / IT-Fehleranalyse im Störfall und ggf. eine Hardware-Diagnose per Fernzugriff für Hardwareprodukt(e) (wie z.B. Endgeräte, Router, Gateways) sowie Schulungsleistungen erbracht.

Es werden folgende ergänzende Vereinbarungen getroffen:

- Prüfungs- und Support- sowie Wartungsarbeiten an ETK networks Komponenten des Kunden werden nach Aufforderung und Freigabe durch den jeweiligen Berechtigten des Kunden durchgeführt.
- Vor Beginn der Prüfungs- und Wartungsarbeiten erfolgt eine Ankündigung durch ETK networks an den Verantwortlichen.
- Auf Anforderung des Verantwortlichen informiert ETK networks den Verantwortlichen, welche Arbeiten wann und von welchen Mitarbeitern durchgeführt werden und wie diese Personen sich dem Verantwortlichen gegenüber identifizieren und authentifizieren werden.
- ETK networks wird von den ihr eingeräumten Zugriffsrechten – auch in zeitlicher Hinsicht – so Gebrauch machen, als dies für die ordnungsgemäße Durchführung der beauftragten Wartungs-, Support- und Prüfungsarbeiten notwendig ist.

### 3. Leistungen/Vertragszweck

Bereitstellung einer PBX (Telefonanlage) und Kommunikationsplattform in der Cloud gem. Vertrag und AGB z.B. myApps Cloud-Service sowie Leistungen auf der Grundlage von Verträgen im Bereich der Wartung/Fernwartung/IT-Fehleranalyse & Support und Schulungs- und Trainingsleistungen.

### 4. Verarbeitungsort

Deutschland und Standorte in der EU/EWR (keine Drittstaaten)

### 5. Technische und organisatorische Sicherheitsmaßnahmen

Für die beauftragte Erhebung und/oder Verarbeitung von personenbezogenen Daten werden folgende Maßnahmen vereinbart:

#### a) Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen
- Zugangskontrolle: Keine unbefugte Systembenutzung, z.B. (sichere) Kennwörter, automatische Sperrmechanismen, ggf. Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern
- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen
- Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit
- Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO, Art. 25 Abs. 1 DS-GVO), soweit dies aufgrund der Risiken für ein angemessenes Schutzniveau erforderlich ist.

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

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN); Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement

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

- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

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

- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle: Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

### 6. Nachweis durch ETK networks

ETK networks steht es frei, die hinreichende Umsetzung der Pflichten aus Vertragsbedingungen, insbesondere der technisch-organisatorischen Maßnahmen (Ziff. 5) und Maßnahmen, die nicht nur den konkreten Auftrag betreffen, durch einen der folgenden Nachweise zu belegen:

- Die Einhaltung genehmigter Verhaltensregeln
- Aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision)
- Eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit; Eigenerklärung des Auftragsverarbeiters.

### 7. Genehmigte Unterauftragsverarbeiter

ETK networks ist berechtigt, Unterauftragsverarbeiter für die von ihr erbrachten Leistungen einzusetzen. Liste der Unterauftragsverarbeiter:

- innovaphone AG - <https://www.innovaphone.com/>