

# Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für Expensya

Vertragspartner sind die Telekom Deutschland GmbH (im Folgenden Telekom genannt), Landgrabenweg 151, 53227 Bonn, und der Kunde.

## 1. Allgemeines

Gegenstand der Vereinbarung ist die Regelung der Rechte und Pflichten des Verantwortlichen (Kunde) und des Auftragsverarbeiters (Telekom), sofern im Rahmen der Leistungserbringung (nach AGB und mitgeltenden Dokumenten) eine Verarbeitung personenbezogener Daten durch die Telekom für den Kunden im Sinne des anwendbaren Datenschutzrechts erfolgt. Die Vereinbarung gilt entsprechend für die (Fern-)Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Aus den AGB und den mitgeltenden Dokumenten, diesen „Ergänzenden Bedingungen Auftragsverarbeitung“ sowie der „Anlage zu den Ergänzenden Bedingungen Auftragsverarbeitung“ (Anlage) - zusammen „ErgB-AV“ - ergeben sich Rechtsgrundlage, Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie die Kategorien der betroffenen Personen.

### Definitionen

Im Sinne dieser „ErgB-AV“ bezeichnet der Ausdruck

- a) „**Auftragsverarbeiter**“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet; „Auftragsverarbeiter“ ist die Telekom;
- b) „**Dritter**“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und die Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;
- c) „**AGB und mitgeltenden Dokumenten**“ die, die Leistungserbringung regelnden Dokumente;
- d) „**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 ist die als „Kunde“ bezeichnete Vertragspartei, die hier in diesen ErgB-AV allein über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;
- e) „**Verarbeitung**“ 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 oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die

Einschränkung, das Löschen oder die Vernichtung;

f) „**personenbezogene Daten**“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

g) „**weiterer Auftragsverarbeiter oder Unterauftragsverarbeiter**“ den Vertragspartner der Telekom, der von dieser mit der Durchführung bestimmter Verarbeitungsaktivitäten für den Verantwortlichen beauftragt wird;

h) „**Sub-Unterauftragsverarbeiter**“ den Vereinbarungspartner des Weiteren Auftragsverarbeiters oder Unterauftragsverarbeiters, der von Letzterem mit der Durchführung bestimmter Verarbeitungsaktivitäten im Regelungsbereich diesen ErgB-AV beauftragt wird.

## 2. Rechte und Pflichten des Kunden

2.1 **[Zulässigkeit der Datenverarbeitung]** Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Kunde verantwortlich. Der Kunde wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z.B. durch Einholung von Einwilligungserklärungen) geschaffen werden, damit die Telekom die vereinbarten Leistungen auch insoweit rechtsverletzungsfrei erbringen kann.

2.2 **[Weisungen]** Die Telekom wird personenbezogene Daten nur auf dokumentierte Weisung des Kunden – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeiten, sofern sie nicht durch das Recht der Union oder der Mitgliedstaaten, dem die Telekom unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt die Telekom dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Als Weisungen sind die AGB und mitgeltenden Dokumente sowie die ErgB-AV zu verstehen. Im Rahmen der produktspezifischen Parameter bestimmt der Kunde Art und Umfang der Datenverarbeitung durch die Art der Nutzung des Produktes, durch Auswahl der dort ggf. ermöglichten Varianten

z.B. hinsichtlich des Umfangs und der Art der zu verarbeitenden Daten oder des Ortes der Datenverarbeitung.

Alle zusätzlichen Weisungen werden schriftlich oder per E-Mail erteilt. Die Telekom informiert den Kunden unverzüglich, falls sie der Auffassung ist, dass eine Weisung gegen die geltenden rechtlichen Bestimmungen verstößt. Die Telekom ist berechtigt, die Durchführung einer solchen Weisung solange auszusetzen, bis diese durch den Kunden bestätigt oder geändert wird.

**2.3 [Ausgleich Mehrleistung]** Soweit in den AGB und den mitgeltenden Dokumenten Vereinbarungen zu Leistungsänderungen getroffen wurden, gehen diese den Regelungen in diesem Absatz vor. Soweit keine Vereinbarung zu Leistungsänderungen in den AGB und den mitgeltenden Dokumenten getroffen wurden, werden zusätzliche Weisungen und Maßnahmen, die eine Abweichung zu den in dieser ErgB-AV oder in den AGB und den mitgeltenden Dokumenten festgelegten Leistungen darstellen, als Antrag auf Leistungsänderung behandelt. Zusätzliche Weisungen und Maßnahmen, die über die vertraglich vereinbarten Leistungen hinausgehen, sind - soweit nicht ausdrücklich anders vereinbart - bei Mehraufwand für die Telekom gesondert zu vergüten. Die Vertragsparteien werden sich in diesem Fall über eine angemessene Vergütung gesondert verständigen. Bei begründeten Weisungen, deren Umsetzung für die Telekom nicht oder nur mit unverhältnismäßig hohem Mehraufwand möglich ist, und deshalb von der Telekom nicht umgesetzt werden, kann der Kunde den Vertrag fristlos kündigen.

Soweit nicht ausdrücklich anders vereinbart, werden Unterstützungsleistungen der Telekom nach Ziffer 2.5 und Ziffer 3.4, 3.5, 3.7, 3.8, (dort Satz 2), 3.9 und 3.10 dieser Vereinbarung gesondert vergütet.

**2.4 [Nachweis durch die Telekom]** Der Telekom steht es frei, die hinreichende Umsetzung ihrer gesetzlichen Pflichten sowie der Pflichten aus diesen ErgB-AV, insbesondere der technisch-organisatorischen Maßnahmen (Ziffer 4) und Maßnahmen, die nicht nur den konkreten Auftrag betreffen, durch die in der Anlage bezeichneten Nachweise zu belegen.

**2.5 [Überprüfungen, Inspektionen]** Der Kunde kann auf eigene Kosten die Einhaltung der Vorschriften über den Datenschutz und der in diesen ErgB-AV niedergelegten Pflichten durch die Einholung von Auskünften und Abfrage der nach Ziffer 2.4 angeführten Nachweise bei der Telekom in Hinblick auf die sie betreffende Verarbeitung kontrollieren. Der Kunde wird vorrangig prüfen, ob die in Satz 1 dieses Absatzes eingeräumte Möglichkeit der Überprüfung ausreicht. Der Kunde kann darüber hinaus in besonders zu begründenden Ausnahmefällen auf eigene Kosten die Einhaltung der Vorschriften über den Datenschutz vor Ort 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 betraute Personen oder Dritte sind mit Beauftragung nachweislich zur Wahrung der Vertraulichkeit zu verpflichten. Die vom Kunden mit der Kontrolle betrauten Personen oder Dritte werden der Telekom in angemessener Form vorangekündigt und in die Lage versetzt, ihre Legitimation zur Durchführung der Kontrollen nachzuweisen. Dritte im Sinne dieses Absatzes dürfen keine Vertreter von Wettbewerbern der

Telekom oder ihrer Konzernunternehmen sein. Der Kunde wird Kontrollen mit einer angemessenen Frist ankündigen und bei deren Durchführung auf Geschäftsbetrieb und Betriebsablauf Rücksicht nehmen. Die der Telekom entstehenden Kosten für eine vor Ort Kontrolle sind vom Kunden zu tragen.

**2.6 [Unterstützung durch den Kunden]** Der Kunde wird in Hinblick auf die ihn betreffende Verarbeitung die Telekom bei Verdacht auf Datenschutzverletzungen und/oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten unverzüglich und vollständig informieren. Der Kunde wird in Hinblick auf die ihn betreffende Verarbeitung die Telekom bei der Prüfung möglicher Verstöße und bei der Abwehr von Ansprüchen Betroffener oder Dritten sowie bei der Abwehr von Sanktionen durch Aufsichtsbehörden zeitnah und umfänglich unterstützen.

### 3. Rechte und Pflichten der Telekom

**3.1 [Datenverarbeitung]** Die Telekom verarbeitet die personenbezogenen Daten ausschließlich im Rahmen des getroffenen Vertrags und nach Weisung des Kunden entsprechend der Regelung der Ziffer 2.2. Die Telekom verwendet die personenbezogenen Daten für keine anderen Zwecke und wird die ihr überlassenen personenbezogenen Daten nicht an unberechtigte Dritte weitergeben. Kopien und Duplikate werden ohne vorherige Einwilligung des Kunden nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung.

Die Telekom gewährleistet, dass die mit der Verarbeitung der personenbezogenen Daten des Kunden befassten Mitarbeiter und andere für die Telekom tätigen Personen diese personenbezogenen Daten nur auf Grundlage der Weisung des Kunden verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

**3.2 [Datenschutzbeauftragter]** Die Telekom wird einen unabhängigen, fachkundigen und zuverlässigen Datenschutzbeauftragten bestellen, sofern dies von dem anwendbaren Recht der Europäischen Union oder des Mitgliedsstaates, dem die Telekom unterliegt, gefordert wird.

**3.3 [Räumliche Beschränkungen; Vollmacht]** Die Telekom wird die vertraglichen Leistungen in Deutschland bzw. von den mit dem Kunden in den AGB und mitgeltenden Dokumente sowie der ErgB-AV vereinbarten Leistungsstandorten aus erbringen. Änderungen des Ortes der Datenverarbeitung werden die Parteien bei Bedarf unter Beachtung der in dieser Vereinbarung festgelegten Form nach Maßgabe der Ziffer 6.2 bis Ziffer 6.6 entsprechend vereinbaren.

Eine Datenverarbeitung in sogenannten Drittländern (d. h. Ländern, die keine Mitgliedstaaten der Europäischen Union sind und über kein angemessenes Datenschutzniveau verfügen), wird unter Berücksichtigung der einschlägigen geltenden rechtlichen Bestimmungen der Europäischen Union auf der in der Anlage dargestellten Grundlage vorgenommen.

Soweit hierzu die EU-Standardvertragsklauseln verwendet werden, wird Telekom diese im Namen und im Auftrag des Kunden abschließen bzw. wird ihren Subunternehmer ermächtigen die EU Standardvertragsklausel in Namen und im Auftrag des Kunden mit seinen Subauftragsverarbeitern

abzuschließen. Die Vertretungsvollmacht hierfür wird hiermit durch den Kunden erteilt.

**3.4 [Unterstützung bei Pflichten des Verantwortlichen]** Die Telekom wird – im vertraglich vereinbarten Umfang unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen - den Kunden bei der Einhaltung seiner ihm nach den geltenden rechtlichen Bestimmungen obliegenden Pflichten unterstützen.

**3.5 [Unterstützung bei Überprüfung und Auskunftsbegehren]** Ist der Kunde gegenüber einer staatlichen Stelle oder einer betroffenen Person (Betroffener) verpflichtet, Auskünfte über die Verarbeitung von personenbezogenen Daten zu geben, so wird die Telekom den Kunden darin unterstützen, diese Auskünfte zu erteilen, sofern diese Auskünfte die vertragliche Datenverarbeitung betreffen und soweit der Kunde dem Auskunftsbegehren nicht selbst oder bereits durch entsprechende Auswahl bestimmter Produktparameter nachkommen kann.

Abhängig von der Art der Verarbeitung wird die Telekom den Kunden bei dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen unterstützen. Soweit sich ein Betroffener zwecks Geltendmachung eines Betroffenenrechts unmittelbar an die Telekom wendet, leitet die Telekom die Anfragen des Betroffenen zeitnah an den Kunden weiter.

Die Telekom wird den Kunden – soweit rechtlich zulässig - über an sie als Auftragsverarbeiter gerichtete Mitteilungen der Aufsichtsbehörden (z. B. Anfragen, Benachrichtigung über Maßnahmen oder Auflagen) in Verbindung mit der Verarbeitung von personenbezogenen Daten nach diesen ErgB-AV informieren. Soweit rechtlich zulässig wird die Telekom Auskünfte an Dritte, auch an Aufsichtsbehörden, nur nach schriftlicher Zustimmung durch und in Abstimmung mit dem Kunden erteilen.

**3.6 [Meldung von Zwischenfällen]** Die Telekom informiert den Kunden ohne schuldhaftes Zögern über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen und/oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten.

**3.7 [Nachweis und Dokumentation]** Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung.

**3.8 [Verzeichnis von im Auftrag durchgeführten Tätigkeiten der Verarbeitung]** Die Telekom führt nach Maßgabe der einschlägigen geltenden rechtlichen Bestimmungen, denen sie unterliegt, ein Verzeichnis zu allen Kategorien von im Auftrag des Kunden durchgeführten Tätigkeiten der Verarbeitung personenbezogener Daten. Die Telekom unterstützt den Kunden auf Anfrage und stellt dem Kunden die für die Führung seines Verzeichnisses von Verarbeitungstätigkeiten notwendigen Angaben zur Verfügung, soweit diese Angaben im vertraglich umschriebenen Verantwortungs- und Leistungsbereich der Telekom als Auftragsverarbeiter liegen und der Kunde keinen anderen Zugang zu diesen Informationen hat.

**3.9 [Datenschutz-Folgenabschätzung]** Falls der Kunde eine Datenschutzfolgenabschätzung durchführt und/oder eine Konsultation der Aufsichtsbehörde nach einer Datenschutzfolgenabschätzung beabsichtigt, werden sich die Vertragsparteien bei Bedarf und auf Anfrage des Kunden über Inhalt und Umfang etwaiger Unterstützungsleistungen der Telekom abstimmen.

**3.10 [Abschluss der vertraglichen Arbeiten, Rückgabe oder Löschung]** Nicht mehr benötigte personenbezogene Daten, mit Ausnahme der aufgrund gesetzlicher Verpflichtung der Telekom weiter vorzuhaltenden personenbezogenen Daten, werden, soweit nicht in den AGB und den mitgeltenden Dokumenten bereits geregelt und soweit nicht anders vereinbart, an den Kunden zurückgegeben oder auf Kosten des Kunden vernichtet bzw. gelöscht. Gleiches gilt für Test- und Ausschussmaterial. Soweit nicht bereits durch entsprechende Auswahl bestimmter Produktparameter durch den Kunden möglich, kann der Kunde während des Bestehens des Vertragsverhältnisses oder mit Vertragsende schriftlich die personenbezogenen Daten, die nicht gemäß Satz 1 vernichtet bzw. gelöscht sind, auf seine Kosten und in einem vorher abgestimmten Format heraus verlangen und der Telekom einen Zeitpunkt (längstens bis Vertragsende) für die Herausgabe nennen. Das Herausgabeverlangen muss der Telekom einen Monat vor dem vom Kunden benannten Zeitpunkt bzw. ein Monat vor Vertragsende zugegangen sein.

## 4. Technische und organisatorische Sicherheitsmaßnahmen

**4.1 [Technisch organisatorische Maßnahmen]** Der Kunde und die Telekom werden geeignete technische und organisatorische Maßnahmen treffen, um ein, dem Risiko angemessenes Schutzniveau zu gewährleisten.

Die derzeit als geeignet angesehenen Maßnahmen der Telekom sind in der Anlage beschrieben. Der Kunde hat die technischen und organisatorischen Maßnahmen vor dem Hintergrund seiner konkreten Datenverarbeitung in Hinblick auf ein angemessenes Schutzniveau bewertet und als angemessen akzeptiert. Etwaige Weiterentwicklungen erfolgen nach Maßgabe von Ziffer 4. 2.

**4.2 [Weiterentwicklung]** Die technischen und organisatorischen Maßnahmen können im Laufe des Vertragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Dabei darf das Schutzniveau das vereinbarte Schutzniveau nicht unterschreiten. Die Sicherheit der Verarbeitung und die Angemessenheit des Schutzniveaus wird der Kunde regelmäßig prüfen und der Telekom unverzüglich mitteilen, sollten die technischen und organisatorischen Maßnahmen seinen Anforderungen nicht mehr genügen. Der Kunde wird der Telekom hierzu alle erforderlichen Informationen zur Verfügung stellen. Die Telekom ihrerseits kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in ihrem Verantwortungsbereich im Einklang mit den Anforderungen der EU-DSGVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird. Zusätzliche technische und organisatorische Maßnahmen, die über die vertraglich

vereinbarten Maßnahmen hinausgehen, sind - soweit nicht ausdrücklich anders vereinbart - bei Mehraufwand für die Telekom gesondert zu vergüten. Die Vertragsparteien werden sich in diesem Fall über eine angemessene Vergütung gesondert verständigen. Bei Maßnahmen, deren Umsetzung für die Telekom nicht oder nur mit unverhältnismäßig hohem Mehraufwand möglich ist, kann die Telekom den Vertrag kündigen.

**4.3 [Überprüfung und Nachweis]** Für die Überprüfungs- und Nachweismöglichkeiten gelten Ziffer 2.4 und 2.5.

## 5. Vertraulichkeit

**5.1 [Vertraulichkeit]** Die Telekom wird im Zusammenhang mit der hier vereinbarten Verarbeitung personenbezogener Daten die Vertraulichkeit wahren. Sie wird die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichten, soweit diese nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Vereinbarungen in den AGB und den mitgeltenden Dokumenten zur Wahrung der Vertraulichkeit und zum Schutz von nicht personenbezogenen Daten bleiben unberührt. Soweit in den AGB und den mitgeltenden Dokumenten hierzu keine Vereinbarung getroffen wurden, verpflichten sich beide Parteien, alle nicht allgemein offenkundigen Informationen aus dem Bereich der anderen Partei, die ihnen durch die Geschäftsbeziehung bekannt werden, geheim zu halten und nicht für eigene Zwecke außerhalb dieses Vertrages oder Zwecke Dritter zu verwenden.

**5.2 [Pflichten beteiligter Personen]** Die Telekom wird Personen, die Zugang zu personenbezogenen Daten haben, mit den für sie maßgeblichen Datenschutzvorgaben und Weisungen dieser Vereinbarung im Voraus vertraut machen.

## 6. Unterauftragsverarbeiter

**6.1 [Befugnis]** Die Telekom darf zur Erfüllung der in diesem Vertrag beschriebenen Aufgaben weitere Auftragsverarbeiter (Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter) einsetzen.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Aufträge zu verstehen, die die Telekom bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung erteilt und die keine Auftragsverarbeitungsleistung personenbezogener Daten für den Kunden beinhalten.

**6.2 [Gesonderte Genehmigung]** Für die in der Anlage aufgeführten Unterauftragsverarbeiter sowie Sub-Unterauftragsverarbeiter und die dort genannten Aufgabenbereiche gilt die Genehmigung des Kunden als erteilt.

**6.3 [Allgemeine schriftliche Genehmigung]** Der Kunde erteilt hiermit der Telekom die allgemeine Genehmigung für den künftigen Einsatz weiterer Auftragsverarbeiter (Unterauftrags- und Sub-Unterauftragsverarbeiter).

**6.4 [Information bei Änderungen]** Die Telekom informiert den Kunden über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung weiterer oder die Ersetzung bestehender Unterauftragsverarbeiter und/oder Sub-Unterauftragsverarbeiter, Telekom Deutschland GmbH

wodurch der Kunde die Möglichkeit erhält, gegen derartige Änderungen binnen 14 Tagen nach Zugang der Information beim Kunden Einspruch zu erheben. Der Kunde wird die Genehmigung derartiger Änderungen nicht ohne wichtigen Grund verweigern. Sofern der Kunde von seinem Einspruchsrecht Gebrauch macht und die Telekom den Unterauftragsverarbeiter und/oder Sub-Unterauftragsverarbeiter trotzdem einsetzt, kann der Kunde den Vertrag fristlos kündigen.

**6.5 [Auswahl]** Die Telekom wird Unterauftragsverarbeiter auswählen, die hinreichende Garantien dafür bieten, dass die vereinbarten geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der einschlägigen geltenden rechtlichen Bestimmungen erfolgt. Die Telekom wird mit Unterauftragsverarbeitern vertragliche Vereinbarungen treffen, die den vertraglichen Regelungen dieser ErgB-AV inhaltlich entsprechen. Die Telekom wird mit dem Unterauftragsverarbeiter die technischen und organisatorischen Maßnahmen festlegen und sich die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen von diesem regelmäßig bestätigen lassen.

**6.6 [Sub-Unterauftragsverarbeiter]** Die Beauftragung von Sub-Unterauftragsverarbeitern ist nach Maßgabe der Ziffer 6.1 bis Ziffer 6.5 entsprechend zulässig.

## 7. Vertragsdauer; Kündigung

Diese Vereinbarung gilt für die Dauer der tatsächlichen Leistungserbringung durch die Telekom. Dies gilt unabhängig von der Laufzeit etwaiger anderer Verträge (insbesondere der AGB und den mitgeltenden Dokumenten), die die Parteien ebenfalls bzgl. der Erbringung der vereinbarten Leistungen abgeschlossen haben.

## 8. Haftung und Freistellung

**8.1 [Verantwortungsbereich des Kunden]** Der Kunde gewährleistet in seinem Verantwortungsbereich die Umsetzung der sich aus den einschlägigen geltenden rechtlichen Bestimmungen ergebenden Pflichten bei der Verarbeitung personenbezogener Daten.

**8.2 [Haftung]** Die Haftungsregelung aus den AGB und den mitgeltenden Dokumenten gilt für diese ErgB-AV, soweit nicht eine Haftungsbeschränkung nach Maßgabe der jeweils einschlägigen geltenden rechtlichen Bestimmungen zugunsten der Telekom greift.

## 9. Sonstiges

**9.1 [Gültigkeit des Vertrags]** Von der Ungültigkeit einer Bestimmung dieser ErgB-AV bleibt die Gültigkeit der übrigen Bestimmungen unberührt. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Parteien diese durch eine neue ersetzen, die dem von den Parteien Gewollten am nächsten kommt.

**9.2 [Änderungen des Vertrags]** Sämtliche Änderungen dieser ErgB-AV sowie Nebenabreden bedürfen der Textform

(einschließlich der elektronischen Form). Dies gilt auch für das Abbedingen dieser Schriftformklausel selbst.

**9.3 [Geschäftsbedingungen]** Es besteht zwischen den Parteien Einigkeit darüber, dass die „Allgemeinen Geschäftsbedingungen“ des Kunden auf diese ErgB-AV keine Anwendung finden.

**9.4 [Gerichtsstand]** Der alleinige Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesen ErgB-AV ist Bonn. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes.

**9.5 [Rechtsgrundlage]** Dieser ErgB-AV liegen die Bestimmungen der EU-Datenschutzgrundverordnung (EU DSGVO) zugrunde. Gegebenenfalls ergänzende landesspezifische Regelungen sind in der Anlage aufgeführt.

**9.6 [Vorrangregelung]** Bei Widersprüchen zwischen den Bestimmungen dieser ErgB-AV und Bestimmungen sonstiger Vereinbarungen, insbesondere der AGB und den mitgeltenden Dokumenten, sind die Bestimmungen dieser ErgB-AV maßgebend. Im Übrigen bleiben die Bestimmungen der AGB und den mitgeltenden Dokumenten unberührt und gelten für diese ErgB-AV entsprechend.

# Anlage zu ergänzende Bedingungen Auftragsverarbeitung personenbezogener Daten für Expensya

## 1. Einzelheiten der Datenverarbeitung

### a. Angaben zu „Kategorien von Verarbeitungen“:

- SaaS (Software as a Service)

### b. Kategorien betroffener Personen:

- Mitarbeiter des Verantwortlichen

### c. Betroffene personenbezogene Daten:

- Stammdaten der Mitarbeiter des Verantwortlichen  
 Kontaktdaten der Mitarbeiter des Verantwortlichen  
 Alle anderen personenbezogenen Daten, die in Art. 4 Nr. 1 der DSGVO definiert sind, die vom Kunden im Zuge des Produktes übermittelt oder gespeichert werden.

### d. Besondere Kategorien von personenbezogenen Daten: (z.B. Art. 9 DSGVO)

Keine.

## 2. Zugriff auf personenbezogene Daten

Der Kunde stellt der Telekom die personenbezogenen Daten bereit, ermöglicht ihm Zugriff auf die personenbezogenen Daten oder erlaubt ihm, die personenbezogenen Daten zu erheben und zwar wie nachfolgend beschrieben:

Die Datenzugriffe werden in der Leistungsbeschreibung zu dem Produkt Expensya beschrieben. Es gelten dazu die SaaS Software AGBs zu finden auf dem Telekom AGB Server.

## 3. Leistungen; Vertragszweck:

Die Leistungen werden detailliert in der Leistungsbeschreibung zu dem Produkt Expensya beschrieben. Es gelten dazu die SaaS Software AGBs zu finden auf dem Telekom AGB Server.

## 4. Verarbeitungsort:

Deutschland, Irland, Niederlande, Frankreich, Tunesien

## 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, 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, Sandboxing;
- **Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)**  
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

### 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), elektronische Signatur;
- **Eingabekontrolle**  
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 die Telekom**

Der Telekom steht es frei, die hinreichende Umsetzung der Pflichten aus diesen ErgB-AV, insbesondere der technisch-organisatorischen Maßnahmen (Ziffer 5) und Maßnahmen, die nicht nur den konkreten Auftrag betreffen, durch einen der folgenden Nachweise zu belegen:

- die Einhaltung genehmigter Verhaltensregeln;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren;
- 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**

Angaben zu Unterauftragsverarbeitern / Leistungen / Verarbeitungsorte

Gesonderte Genehmigung:  
Telekom beabsichtigt, die folgenden Unterauftragsverarbeiter für die folgenden Leistungen an den folgenden Verarbeitungsorten einzusetzen:

Unterauftragsverarbeiter:

Expensya Paris  
Sales Marketing in Paris  
Expensya SAS,  
91 boulevard Sebastopol, 75002, Paris (France)

Deutsche Telekom AG  
Friedrich-Ebert-Allee 140, 53113 Bonn  
Leistung: Plattformbetreiber TelekomCLOUD (technisch)

Strato AG, Berlin  
Pascalstraße 10, 10587 Berlin  
Leistung: Service Desk, 1st Level Support

Die Telekom beabsichtigt weitere Unterauftragsverarbeiter zu beauftragen. Welche dies konkret sind, ist abrufbar bzw. über [GDPR@telekom.de](mailto:GDPR@telekom.de) zu erfragen.

**8. Genehmigte Sub-Unterauftragsverarbeiter**

Die Telekom beabsichtigt Sub-Unterauftragsverarbeiter zu beauftragen. Welche dies konkret sind, ist abrufbar bzw. über [GDPR@telekom.de](mailto:GDPR@telekom.de) zu erfragen.

**9. Anforderungen an die Auftragsverarbeitung in Drittländer**

ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (z.B. Art. 45 Abs. 3 DSGVO);

wird ebenso hergestellt durch verbindliche interne Datenschutzvorschriften (z.B. Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO);

wird hergestellt durch Standarddatenschutzklauseln (z.B. Art. 46 Abs. 2 lit. c und d DSGVO);