

Vertrag zur Auftragsverarbeitung gem. Art. 28 DS-GVO

Diese Vereinbarung wird getroffen

zwischen dem Verantwortlichen

Firma:

Straße:

PLZ Ort:

Gesetzlich vertreten durch:

Name, abweichende Anschrift des Datenschutzbeauftragten:

oder

(wenn zutreffend, bitte ankreuzen) Unser Unternehmen ist nach EU-DSGVO nicht verpflichtet einen Datenschutzbeauftragten zu bestellen

- nachstehend „**Auftraggeber**“ genannt -

und dem Auftragsverarbeiter

cobra GmbH – Line-Eid-Str. 1 - 78467 Konstanz

Gesetzlich vertreten durch die Geschäftsführer: Benjamin Bruno, Philipp Kreis

- nachstehend „**Auftragnehmer**“ genannt -

- nachstehend zusammen die **Vertragspartner** –

§ 1 Begriffsbestimmungen (Art. 4 DS-GVO)

- (1) „Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.
- (2) „Verarbeitung“ meint 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.
- (3) „Verantwortlicher“ ist diejenige 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.
- (4) „Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

§ 2 Inhalt der Vereinbarung (Art. 28 Abs. 3 DS-GVO)

- (1) Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragspartner, welche sich aus dem bestehenden Vertragsverhältnis und den jeweils erteilten Einzelaufträgen und den darin festgelegten Pflichten ergeben. Sie findet Anwendung auf alle Tätigkeiten, die hiermit in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.
- (2) In dieser Vereinbarung werden Gegenstand und Dauer der Verarbeitung (Ziffer 3), Art und Zweck der Verarbeitung (Ziffer 4), die Art der personenbezogenen Daten (Ziffer 5), die Kategorien betroffener Personen (Ziffer 6) und die Pflichten und Rechte der Vertragspartner (Ziffer 7 bis 17) beschrieben.

§ 3 Gegenstand und Dauer der Verarbeitung

- (1.) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die durch das bestehende Vertragsverhältnis sowie durch die erteilten Einzelaufträge konkretisiert werden.
- (2.) Ergänzend hierzu gilt je nach Einzelauftrag folgende Beschreibung des Gegenstands der Verarbeitung:
 - Nutzung der Softwareanwendungen und deren Funktionen (z.B. Auslesen von Visitenkartendaten etc.)
 - Hosting und / oder Bereitstellung von Softwareanwendungen in einem Rechenzentrum
 - Supportleistungen im Rahmen der Nutzung der Softwareanwendungen (z.B. Fernwartung, Datensicherung etc.)
 - Consultingdienstleistungen als Vorbereitung für die Einführung neuer Software/Erweiterung der bestehenden Software
 - Sonstige IT-Dienstleistungen

Der Auftraggeber ist für die Vollständigkeit der Angaben verantwortlich.

- (3.) Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des bestehenden Vertragsverhältnisses und der erteilten Einzelaufträge und tritt mit Unterzeichnung durch beide Vertragspartner in Kraft.
- (4.) Die Verarbeitung der personenbezogenen 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 Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

§ 4 Art und Zweck der Verarbeitung

- (1.) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus dem bestehenden Vertragsverhältnis und aus dem erteilten Einzelauftrag.
 - (2.) Ergänzend hierzu gilt folgende Beschreibung von Art und Zweck der Verarbeitung:
 - Einsichtnahme zum Zwecke der Erbringung von Supportleistungen
 - Einsichtnahme, Veränderung, Vervielfältigung und Auswertung im Rahmen der Fernwartung
 - Vervielfältigung zum Zwecke der Durchführung von Datensicherungen und Backups
 - Speicherung zum Zwecke des Hostings von Softwareanwendungen
 - Importieren, Exportieren, Erfassen, Auslesen und Speichern von Daten z.B. im Rahmen des Visitenkartenscans
- Der Auftraggeber ist für die Vollständigkeit der Angaben verantwortlich.

§ 5 Art der personenbezogenen Daten

- (1.) Die Art der verarbeiteten personenbezogenen Daten ergibt sich aus dem bestehenden Vertragsverhältnis und aus dem erteilten Einzelauftrag.
- (2.) Ergänzend hierzu gilt folgende Beschreibung der Art der verarbeiteten personenbezogenen Daten:

Der Auftraggeber ist für die Vollständigkeit der Angaben verantwortlich.

§ 6 Kategorien betroffener Personen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieser Vereinbarung Betroffenen umfasst:

Der Auftraggeber ist für die Vollständigkeit der Angaben verantwortlich.

§ 7 Dokumentierte Weisung (Art. 28 Abs. 3 a))

- (1.) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages, d.h. im Rahmen der sich aus dem bestehenden Vertragsverhältnis und den erteilten Einzelaufträgen ergebenden Bestimmungen und Weisungen des Auftraggebers verarbeiten.
- (2.) Der Auftraggeber ist als Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit und nach Beendigung dieser Vereinbarung Weisungen an den Auftragnehmer erteilen.
- (3.) Jede Weisung des Auftraggebers bedarf der Schrift- oder Textform (z.B. Brief, Fax, E-Mail) und muss nachvollziehbar dokumentiert werden. Es muss stets nachvollzogen werden können, wann von wem eine Weisung an den Auftragnehmer erteilt wurde. Der Auftragnehmer hat nur Weisungen in Schrift- oder Textform zu befolgen.
- (4.) Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DS-GVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

§ 8 Vertraulichkeit (Art. 28 Abs. 3 b))

- (1.) Der Auftragnehmer gewährleistet und versichert, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
- (2.) Der Auftragnehmer erbringt auf Anfrage den Nachweis über die Verpflichtung auf Vertraulichkeit.

§ 9 Technisch-organisatorische Maßnahmen des Auftragnehmers (Art. 28 Abs. 3 c))

- (1.) Der Verantwortliche arbeitet nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.
- (2.) Unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen hat der Auftragnehmer geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:
 - a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
 - b. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
 - c. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
 - d. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
- (3.) Bei der Beurteilung des angemessenen Schutzniveaus hat der Auftragnehmer die Risiken berücksichtigt, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
- (4.) Der Auftragnehmer unternimmt Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.
- (5.) Zur Gewährleistung der Sicherheit und Vertraulichkeit der Daten hat der Auftragnehmer die in seinem Datenschutz- und Datensicherheitskonzept aufgeführten technisch-organisatorischen Maßnahmen getroffen. Das Datenschutz- und Datensicherheitskonzept des Auftragnehmers wird als verbindlich festgelegt. Die Beschreibung der technischen und organisatorischen Datensicherungsmaßnahmen nach Art. 32 DS-GVO ist in **Anlage AV 1** und **Anlage AV 2** aufgeführt.

§ 10 Einschaltung von weiteren Auftragsverarbeitern (Art. 28 Abs. 3 d))

- (1.) Der Auftragnehmer nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch.

- (2.) Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragnehmer den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.
- (3.) Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine Pflichten aus dieser Vereinbarung dem weiteren Auftragsverarbeiter zu übertragen. Dies gilt insbesondere für die zwischen den Vertragspartnern festgelegten Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit.
- (4.) Für den Fall, dass der Auftraggeber ein cobra cloud-Produkt (siehe **Anlage AV 3** Übersicht der cobra cloud-Produkte in der jeweils aktuellen Fassung) beim Auftragnehmer bestellt, erteilt der Auftraggeber bereits hiermit sein ausdrückliches Einverständnis dazu, dass der Auftragnehmer zur Begründung eines Unterauftragsverhältnisses nach Maßgabe der hier vereinbarten Regelungen mit der Buhl Data Service GmbH, Am Siebertsweiher 3/5, 57290 Neunkirchen, berechtigt ist.
- (5.) Der Auftraggeber erteilt hiermit sein ausdrückliches Einverständnis, dass der Auftragnehmer zur Begründung eines Unterauftragsverhältnisses nach Maßgabe der hier vereinbarten Regelung mit den in **Anlage AV 4** genannten Unterauftragsverarbeitern berechtigt ist.

§ 11 Rechte der Betroffenen (Art. 28 Abs. 3 e))

- (1.) Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Verarbeitung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen.
- (2.) Der Auftragnehmer trifft insbesondere geeignete technische und organisatorische Maßnahmen, um dem Auftraggeber die Erfüllung seiner Pflichten gegenüber den Betroffenen zu ermöglichen.

§ 12 Unterstützung des Auftraggebers (Art. 28 Abs. 3 f))

- (1.) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit der Verarbeitung personenbezogener Daten sowie zu etwa bestehenden Melde- und Benachrichtigungspflichten, durchzuführenden Datenschutz-Folgeabschätzungen und notwendigen vorherigen Konsultationen der Aufsichtsbehörde.
- (2.) Der Auftragnehmer stellt ein angemessenes Schutzniveau durch technische und organisatorische Maßnahmen sicher, welche die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.
- (3.) Der Auftragnehmer ist verpflichtet, eine Verletzung des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden. Der Auftragnehmer unterstützt den Auftraggeber bei dessen Meldeverpflichtung aus Art. 33 DS-GVO und stellt ihm die etwa benötigten Informationen unverzüglich zur Verfügung.
- (4.) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen aus Art. 34 DS-GVO und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.
- (5.) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen etwa durchzuführender Datenschutz-Folgeabschätzungen gem. Art. 35 DS-GVO.
- (6.) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen etwa notwendiger vorheriger Konsultationen der Aufsichtsbehörde.

§ 13 Abschluss der Erbringung der Verarbeitungsleistungen (Art. 28 Abs. 3 g))

- (1.) Nach Beendigung des bestehenden Vertragsverhältnisses und des jeweiligen Einzelauftrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen (mit Ausnahme von routinemäßig gesicherten Back-ups).
- (2.) Die Datenträger des Auftragnehmers sind danach physisch zu löschen (mit Ausnahme von routinemäßigen Back-ups). Die Löschung ist – auf Verlangen des Auftraggebers – in geeigneter Weise zu dokumentieren.

§ 14 Kontrollrechte des Auftraggebers (Art. 28 Abs. 3 h))

- (1.) Der Auftraggeber hat das Recht, sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers zu überzeugen. Hierfür kann er insbesondere Selbstauskünfte des Auftragnehmers einholen und sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufes persönlich überzeugen oder einen Dritten hiermit beauftragen.
- (2.) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind. Der Auftragnehmer ist insbesondere verpflichtet, die Umsetzung von angemessenen technischen und organisatorischen Maßnahmen nachzuweisen. Der Nachweis über solche Maßnahmen, die nicht nur den konkreten Einzelauftrag betreffen, kann erfolgen durch:
 - a. die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DS-GVO;
 - b. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DS-GVO;
 - c. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
 - d. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

§ 15 Berichtigung, Einschränkung und Löschung von Daten

- (1.) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, einschränken oder löschen. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- (2.) Falls vereinbart, sind das Vorhandensein eines datenschutzkonformen Löschkonzeptes, die Datenportabilität sowie die Umsetzung der Rechte auf Berichtigung und Löschung („Recht auf Vergessenwerden“) vom Auftragnehmer sicherzustellen.
- (3.) Der Auftragnehmer bietet dem Auftraggeber die Möglichkeit, Daten der Cloud-Anwendung zu exportieren. Diese exportierbaren Daten können zum Wechsel zu Diensten von Drittanbietern oder zu einer Infrastruktur in den eigenen Räumlichkeiten des Auftraggebers verwendet werden. Der Auftraggeber hat den Wechsel 2 Monate vorher in Textform anzukündigen. Die Datenübertragung erfolgt spätestens nach Ablauf einer Übergangsfrist von höchstens 30 Kalendertagen ab Ablauf der zweimonatigen Ankündigungsfrist. Der Auftragnehmer behält sich das Recht vor, den Export von Daten zu beschränken, die die Sicherheit der Dienste oder das geistige Eigentum des Auftragnehmers gefährden könnten. Der Auftragnehmer leistet angemessene Unterstützung beim Export der Daten. Der Vertrag gilt als beendet, wenn der Wechsel erfolgreich vollzogen ist oder die Daten nach Ablauf der zweimonatigen Ankündigungsfrist auf Verlangen des Auftraggebers gelöscht wurden. Sollte der Wechsel des Auftraggebers zu einer vorzeitigen Vertragsbeendigung führen, hat der Auftraggeber die bis zum regulär nächstmöglichen Vertragsende vereinbarten Kosten zu tragen.

§ 16 Datenschutzbeauftragter und IT-Sicherheitsbeauftragter

- (1.) Der Auftragnehmer ist gesetzlich zur Bestellung eines Datenschutzbeauftragten verpflichtet. Dieser Verpflichtung ist er nachgekommen. Der Datenschutzbeauftragte des Auftragnehmers übt seine Tätigkeit gem. Art. 38 und 39 DS-GVO aus. Die Kontaktdaten sind:
MORGENSTERN consecom GmbH, Herr Jan Morgenstern, Große Himmelsgasse 1, 67346 Speyer,
Tel.: 06232/100119-44, E-Mail: datenschutz@cobra.de.
- (2.) Der Auftragnehmer hat einen IT-Sicherheitsbeauftragten bestellt. Die Kontaktdaten sind:
Emre Gürkan, Tel. 07531/8101-183, E-Mail: ITSicherheit@cobra.de.

§ 17 Dokumentationspflichten des Auftragnehmers

- (1.) Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag für den Auftraggeber durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:
 - a. den Namen und die Kontaktdaten des Auftragnehmers oder der Auftragnehmer und jedes Verantwortlichen, in dessen Auftrag der Auftragnehmer tätig ist, sowie gegebenenfalls des Vertreters des Auftraggebers oder des Auftragnehmers und eines etwaigen Datenschutzbeauftragten;

- b. die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
 - c. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 Unterabs. 2 DS-GVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
 - d. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO.
- (2.) Das Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.
- (3.) Der Auftraggeber oder der Auftragnehmer sowie gegebenenfalls der Vertreter des Auftraggebers oder des Auftragnehmers stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

§ 18 Informationspflichten, Schriftformklausel, Rechtswahl

- (1.) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.
- (2.) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, mindestens in Textform, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (3.) Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftraggebers.
- (4.) Diese Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO ersetzt alle vorhergehenden Vereinbarungen zur Auftragsverarbeitung der beiden Parteien mit cobra als Auftragsverarbeiter.

Konstanz, den

Ort,

den

cobra GmbH

Unterschrift Kunde

Anlagen:

- Anlage AV 1:** Beschreibung der technischen und organisatorischen Datensicherungsmaßnahmen nach Art. 32 DS-GVO der cobra GmbH
- Anlage AV 2:** Beschreibung der technischen und organisatorischen Datensicherungsmaßnahmen nach Art. 32 DS-GVO der Buhl Data Service GmbH für cobra cloud-Produkte
- Anlage AV 3:** Übersicht der cobra cloud-Produkte
- Anlage AV 4:** Übersicht der Unterauftragnehmer

Stand: Januar 2026

Anlage AV 1

Beschreibung der technischen und organisatorischen Datensicherungsmaßnahmen nach Art. 32 DS-GVO der cobra GmbH

Der Verantwortliche hat unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für Rechte und Freiheiten natürlicher Personen die im Folgenden aufgeführten geeigneten technischen und organisatorischen Maßnahmen umgesetzt, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der geltenden DS-GVO erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

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

1.1 Zutrittskontrolle

- Alarmsystem zur Überwachung aller Eingangstüren
- Fensterloser, innenliegender Serverraum im 4. Obergeschoss
- Empfang während der Geschäftszeiten stets besetzt
- Besucher werden persönlich am Empfang abgeholt
- Keine Besucher auf Etage, in der IT-Infrastruktur steht
- Kein Zutritt für Unbefugte zu den Datenverarbeitungsanlagen des Rechenzentrums
- Manuelles Schließsystem an der Eingangstür
- Schließanlage mit Codesperre am Serverraum (zusätzlich ist die Zutrittsberechtigung zum Serverraum auf ein Mindestmaß reduziert)
- Schlüsselausgabekonzept
- Kameraüberwachung (Bewegungserkennung) der Eingangsbereiche während der Nicht-Bürozeiten
- Sorgfältige Auswahl von Reinigungspersonal

1.2 Zugangskontrolle

- Verwendung fortlaufend aktualisierter Virenschutzsoftware
- Schutz des E-Mail-Verkehrs vor Viren und Spam
- Redundante Firewallsysteme
- Automatisierte Einspielung von Sicherheits-Patches
- Planbasierter Einsatz von Sicherheits-Patches beim Server
- Zentrales Rechtemanagement für Arbeitsplatz-PCs
- Regelung und Kontrolle von externer Wartung und Fernwartung
- Getrennte Administration der Firewall und Serversysteme durch unterschiedliche Personen/Teams

1.3 Zugriffskontrolle

- Zugriff auf Systeme nur mit individuellen Benutzernamen und Kennwörtern
- Rollenbasiertes Berechtigungskonzept
- Freigabe der Berechtigungen nach dem Mehr-Augen-Prinzip
- Rollenbasierte Administrationsrechte
- Personenbezogene gespeicherte Daten können nur im Rahmen des Berechtigungskonzepts gelesen, kopiert, verändert oder entfernt werden

- Verwendung fortlaufend aktualisierter Virenschutzsoftware
- Schutz des E-Mail-Verkehrs vor Viren und Spam
- Redundante Firewallsysteme
- Protokollierung von Zugriffen
- Automatisierte Einspielung von Sicherheits-Patches
- Planbasierter Einsatz von Sicherheits-Patches beim Server
- Sicherstellung einer hohen Widerstandsfähigkeit der DV-Systeme bei starkem Zugriff bzw. starker Belastung, etwa durch Angriffe von außen, u.a. durch den Einsatz einer entsprechenden XDR-Lösung
- Regelmäßige Pentests
- Verwendung ausgetesteter Software
- Einsatz von Intrusion-Detection-System
- Netzwerksegmentierung durch VLAN, Einsatz von Reverse Proxy
- Hohe Passwortsicherheit, regelmäßiger Wechsel
- Verschlüsselung von Passwörtern
- Zwei-Faktor-Authentifizierung bei Outlook
- Externer Zugriff nur über gesicherte VPN-Verbindung (MFA-geschützt)
- Automatische Bildschirmsperre bei Nichtbenutzung
- Zugriffsschutz auf Basis SQL-Server und Active Directory
- Zentrales Rechtemanagement für Arbeitsplatz-PCs
- Regelung und Kontrolle von externer Wartung und Fernwartung
- Segmentierung des Netzwerks (VLAN)
- Wöchentlicher Security Scan auf unsere externen Systeme
- Festplattenverschlüsselung bei Notebooks
- Sichere Löschung von Datenträgern durch mehrfaches Überschreiben

1.4 Trennungskontrolle

- Trennung der Produktiv- von der Test- und Entwicklungsumgebung
- Berechtigungskonzept / Datentrennung nach Abteilung bzw. Funktion

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

2.1 Weitergabekontrolle

- Einrichtung von VPN-Verbindungen
- VPN-Verbindungen mit Zwei-Faktor-Authentifizierung
- Überprüfung der Empfänger von Dateien vor Versand
- Sichere Löschung von Datenträgern durch mehrfaches Überschreiben
- Sicherer physischer Transport (alle Medien, die zum Transport freigegeben sind, werden verschlüsselt, z. B. Verschlüsselung von USB-Sticks per Bitlocker)
- Allgemeine Verschlüsselung von Speichermedien per Bitlocker

- Protokollierung der Weitergabe von Speichermedien (Herausgabe von Speichermedium muss per IT-Support-Ticket beantragt werden inkl. Protokollierung)
 - Sichere Löschung von Datenträgern durch mehrfaches Überschreiben
 - DIN-Shredder auf jedem Stockwerk
- 2.2 Eingabekontrolle
- Protokollierung (Logging)
- (3) Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 b) DS-GVO)**
- 3.1 Verfügbarkeitskontrolle
- Service-Level-Agreement mit Dienstleistern
 - Netzwerkplan
 - IT-Asset-Management
 - Mehrstufige, externe Datensicherung
 - Regelmäßige Wiederherstellungstests
 - Klimaanlage in Serverräumen
 - Raumtemperaturüberwachung von Serverräumen inklusive Alarmierung
 - Load-Balancing
 - Alert-Meldung bei hoher Belastung
 - Virtualisierung/Dynamische Zuteilung
 - Brandschutzvorrichtungen
 - Rauchmelder mit Alarm in Serverräumen
 - Doppelt- oder Mehrfachvorhaltung aller Komponenten bei der Datenverarbeitung (z. B. Datensicherung und Spiegelung von Hardwarekomponenten)
 - Datensicherungs- und Recoverykonzept
 - Personenbezogene Daten sind verfügbar und geschützt gegen zufällige Zerstörung oder Verlust durch tägliche Backups
 - Aufbewahrung von Backup-Kopien in einem anderen Brandabschnitt
 - Sicherheitskopien
 - Sicherstellung einer hohen Widerstandsfähigkeit der DV-Systeme bei starkem Zugriff bzw. starker Belastung, etwa durch Angriffe von außen, u.a. durch den Einsatz einer entsprechenden XDR-Lösung
 - Regelmäßige Pentests
 - Einsatz von Intrusion-Detection-System
 - Unterbrechungsfreie Stromversorgung
 - Redundante Stromzuführungen
 - Überwachungs- und Meldesysteme
 - Regelmäßige Durchführung von Reviews durch externe Dienstleister zur Verbesserung der Systeme (auch bezüglich externer Verbindungen)
 - Anpassung der Systeme nach Durchführung von Reviews
- 3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 c) DS-GVO)
- Datensicherungs- und Recoverykonzept
- Zugriffsschutz für Datensicherungen durch sichere Aufbewahrung im Banktresor
 - Schutz der Datensicherungen z. B. durch Verschlüsselungsverfahren
 - Personenbezogene Daten sind ständig verfügbar und geschützt gegen zufällige Zerstörung oder Verlust durch tägliche Backups
 - Sicherheitskopien
 - Unterbrechungsfreie Stromversorgung
- (4) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 d) DS-GVO; Art. 25 Abs. 1 DS-GVO)**
- 4.1 Auftragskontrolle
- Eindeutige Vertragsgestaltung
 - Formalisiertes Auftragsmanagement
 - Auswahl von Auftragnehmern unter Sorgfalts Gesichtspunkten (insbesondere hinsichtlich Datensicherheit)
 - Sicherstellung der Vernichtung / Rückgabe / Löschung von Daten nach Beendigung des Auftrags
 - Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation
 - Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
 - Bestellung eines Datenschutzbeauftragten
- 4.2 Datenschutzmanagement
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
 - Bestellung eines Datenschutzbeauftragten
 - Vertragspartner mit Zutritt zum Serverraum werden auf die Vertraulichkeit verpflichtet
 - Regelungen zur Beschaffung von Hard- und Software
 - Regelmäßige Prüfung, ob / in welchem Umfang Zugangsrechte noch erforderlich sind
 - Durchführung von Mitarbeiterschulungen
 - Datenschutzrichtlinien (Datenschutzverletzungen, Betroffenenanfragen)
 - Freiwillige jährliche IT-Sicherheitsaudits
- 4.3 Incident-Response-Management
- Incident-Response-Management
 - Einsatz einer XDR-Lösung
 - Notfallplan
 - Dokumentation von Vorfällen
- 4.4 Datenschutzfreundliche Voreinstellungen
- Die standardisierten Voreinstellungen wurden im datenschutzfreundlichen Sinne getroffen
 - Festlegung von Löschrufen

Stand: Januar 2026

Anlage AV 2

Beschreibung der technischen und organisatorischen Datensicherungsmaßnahmen nach Art. 32 DS-GVO der Buhl Data Service GmbH für cobra cloud-Produkte

- 1) **Pseudonymisierung und Verschlüsselung personenbezogener Daten**
 - HTTPS-Verschlüsselung in der Webkommunikation (Data-at-Transport)
 - obligatorische Verschlüsselung aller administrativen Zugriffe
 - obligatorische Verschlüsselung aller ausgehenden E-Mails
 - Verwendung einer speziellen Hardware-Verschlüsselung für besonders kritische Daten (HSM)
 - Verschlüsselung aller Datensicherungsbänder

- (2) **Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen**
 - Zugang zu Systemen nur mit individuellen Benutzernamen und Kennwörtern
 - obligatorische Mehr-Faktor-Authentifizierung für Fernzugriffe
 - Zentraler selbst-gehosteter individueller Passwort-Safe für alle Beschäftigte
 - Berechtigte können nur auf für sie berechtigte Daten zugreifen
 - personenbezogene gespeicherte Daten können nur im Rahmen der Berechtigungsstufen gelesen, kopiert, verändert oder entfernt werden
 - Einsatz eines Firewall- und Web-Application-Firewallsystems
 - Ausschließliche Verwendung der vom Hersteller der Hardware und Virtualisierungssoftware freigegebenen Software
 - Verpflichtung der Mitarbeiter auf das Datengeheimnis
 - Redundante Klimaanlage, redundante USVs in Serverräumen
 - Alert-Meldung bei Ausfällen der Serversysteme
 - Virtualisierung/Dynamische Zuteilung der Anwendung auf getrennte Serverräume
 - Kein Zugang für Unbefugte zu den Datenverarbeitungsanlagen des Rechenzentrums
 - Besucher der Rechenzentren (z. B. für Wartungszwecke) werden zwingend begleitet
 - Festlegung der berechtigten Personen für die sensiblen Bereiche der Rechenzentren
 - Einbruchschutzmaßnahmen, Alarmanlage mit Aufschaltung auf Wachdienst
 - Besonderer Perimeterschutz für RZ-Bereiche
 - Protokollierung des Zutritts zu den Rechenzentren über entsprechende Transponder
 - Sichere Löschung von Datenträgern
 - Videoüberwachung (Empfang und RZs)
 - Regelungen zur Kontrolle von externer Wartung und Fernwartung

- Brandfrüherkennung und Gas-Löschanlage in besonderen RZ-Bereichen
- Brandmeldeanlage mit Aufschaltung auf Feuerwehroleitstelle
- Redundante Internetanbindung mit erdkabelfreier Breitband-Fallback-Anbindung
- Schutz vor Netz-Überlastungsangriffen (DDoS) auf Tier 1-Ebene

 - (3) **Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen**
 - Doppelt- oder Mehrfachvorhaltung aller Komponenten bei der Datenverarbeitung (z. B. Datensicherung und Spiegelung von Hardwarekomponenten);
 - Datensicherungs- und Recoverykonzept
 - Auslagerung von Backups zu einem entfernten, eigenen Disaster-Recovery Standort umgehend nach Erstellung
 - besonders geschützte Rechenzentrumsabschnitte in getrennten Brandabschnitten und Gebäuden
 - unterbrechungsfreie Stromversorgung
 - Überwachungs- und Meldesysteme
 - Netzersatzanlage (NEA)

 - (4) **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Verarbeitung**
 - Regelmäßige Prüfung, ob/in welchem Umfang Zugangsrechte noch erforderlich sind
 - Regelmäßige Prüfung, ob/in welchem Umfang Zugriffsrechte noch erforderlich sind
 - Incident-Response-Management
 - Auftragskontrolle bei Auftragsverarbeitung
 - Regelmäßige Ausfalltests der Infrastrukturkomponenten

Stand: November 2025

Anlage AV 3

Übersicht der cobra cloud-Produkte

cobra Private Cloud
cobra WEB PRO
cobra CXM WEB CONNECT
cobra Add-in für Microsoft Office

Stand: November 2025

Anlage AV 4

Übersicht der Unterauftragnehmer

Unterauftragnehmer	Anschrift	Leistung bzw. Modul
Accantum GmbH	Äußere Oberastr. 36/4, 83026 Rosenheim	(Weiter-) Entwicklung der Schnittstelle accantum
astendo GmbH	Büropark Top Tegel Haus C, Wittestraße 30 C, 13509 Berlin-Reinickendorf	Support-Leistungen/Installation von astendo Zusatzprodukten für cobra CRM
Brehmer Software GmbH	Benzstraße 7A 14482 Potsdam-Babelsberg	Installation, (Weiter-) Entwicklung, Pflege und Support der DocuWare Schnittstelle
Buhl Data Service GmbH	Am Siebertsweiher 3/5, 57290 Neunkirchen	Hosting der cobra cloud-Produkte
compuart.com GmbH	Ravensburger Straße 71, 88239 Wangen im Allgäu	Installation, Support und Pflege der cobra Hosting-Produkte
efense GmbH	Am Königsweg 9b, 48599 Gronau-Epe	(Weiter-) Entwicklung, Pflege und Support D.velop Schnittstelle
vectano GmbH	Am Sudheimer Weg 3, 33034 Brakel	(Weiter-) Entwicklung der Schnittstelle cobra-Microtech
Fisel GmbH	Gellertstraße 83, 74074 Heilbronn	(Weiter-) Entwicklung der cobra Schnittstelle zu lobodms
Fluctus IT GmbH	Tempowerkring 1, 21079 Hamburg	Projektbezogene (Weiter-) Entwicklung und Installation der mesonic-Schnittstelle nach Kundenauftrag
Fynn GmbH	Barthelstr. 4, 50823 Köln	Abo- und Kundenverwaltung für die Abrechnung
HPH Software GmbH	Eickener Straße 83, 41061 Mönchengladbach	(Weiter-) Entwicklung der sage50- Schnittstelle
id-netsolutions GmbH	Segeberger Str. 9, 23863 Kayhude	(Weiter-) Entwicklung der docufied ELO Schnittstelle
Intelligent Webworks GmbH	Darmstädter Str. 66, 64354 Reinheim	(Weiter-) Entwicklung, Installation Support und Pflege der cobra Hosting-Produkte u. CXM Portal
IONOS SE	Elgendorfer Str. 57, 56410 Montabaur	Hosting
LANOS Computer GmbH & Cie KG	Görlitzer Straße 6, 33758 Schloß Holte-Stukenbrock	(Weiter-) Entwicklung der LANOS Kanzlei Lösung
Microtech GmbH	Arthur-Rauner-Straße 5, 55595 Hargesheim	(Weiter-) Entwicklung der Schnittstelle cobra-Microtech
P17 GmbH	Kircheninsel 3, 48599 Gronau	(Weiter-) Entwicklung der cobra Schnittstelle zu d.velop, (Weiter-) Entwicklung, Pflege und Support-Leistungen für das Produkt MAP+PLUS
PerlSystem® it solutions	Bismarckstrasse 29 06749 Bitterfeld-Wolfen OT Bitterfeld	(Weiter-) Entwicklung, Pflege und Support der Schnittstelle ELO for cobra u. CXM Portal
PROCLANE Commerce GmbH	Willy-Brandt-Straße 57, 20457 Hamburg	Weiter-) Entwicklung, Installation und Support der SAP-Schnittstelle
Rautenberg Druck GmbH	Blinke 8, 26789 Leer	Druck und Versand von Infopost, Postern, Flyern und Broschüren
RS Gesellschaft für Informationstechnik mbH	Auf dem Knapp 35, 42855 Remscheid	(Weiter-) Entwicklung der SAGE New- Classic-Schnittstelle

Ruthardt Softwaretechnik GmbH	Friedrich-List-Straße 34, 70771 Leinfelden-Echterdingen	(Weiter-)Entwicklung, Pflege und Support der PLUS-Tools der Ruthardt Softwaretechnik GmbH
SelectLine Software GmbH	Otto-von-Guericke-Straße 67, 39104 Magdeburg	(Weiter-) Entwicklung der SelectLine Schnittstelle
SKIT Dynamics GmbH	Am Frauwald 12, 65510 Idstein	(Weiter-) Entwicklung der Schnittstelle cobra-EVALANCHE
Vanquish GmbH	Steinkamp 20, 26125 Oldenburg	(Weiter-) Entwicklung der Alludo/Parallels Softwareprodukte
VTE Teichmann GmbH	Schardthof 10, 84051 Essenbach	(Weiter-) Entwicklung der DATEV-Schnittstelle
WesCon GmbH	Bergiusstraße 1, 28816 Stuhr	(Weiter-) Entwicklung der NAV2cobra-Schnittstelle
windream GmbH	Wasserstraße 219, 44799 Bochum	(Weiter-) Entwicklung der windream-Schnittstelle

Stand: Dezember 2025