cobra®
CRM

Vereinbarung zur Auftragsbearbeitung gem. Art. 9 DSG-neu

Diese Vereinbarung wird getroffen

zwischen dem Verantwortlichen

Firma, Strasse, Postleitzahl, Ort

Gesetzlich vertreten durch: _____

- nachstehend „**Auftraggeber**“ genannt -

und dem Auftragsbearbeiter

cobra computer's brainware AG – Bahnstr. 1 - 8274 Tägerwilen
Gesetzlich vertreten durch den Geschäftsführer: Jürgen Litz

- nachstehend „**Auftragnehmer**“ genannt -
- nachstehend zusammen die **Vertragspartner** –

§ 1 Begriffsbestimmungen (Art. 5 DSG-neu)

(1.) „Personendaten“ sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

(2.) „Bearbeiten“ meint jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.

(3.) „Verantwortlicher“ ist diejenige private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet.

(4.) „Auftragsbearbeiter“ ist diejenige private Person oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.

§ 2 Inhalt der Vereinbarung (Art. 9 DSG-neu)

(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 Personendaten des Auftraggebers in Berührung kommen können.

(5.) In dieser Vereinbarung werden Gegenstand und Dauer der Bearbeitung (Ziffer 3), Art und Zweck der Bearbeitung (Ziffer 4), die Art der Personendaten (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 Bearbeitung

(1.) Der Auftragnehmer bearbeitet Personendaten 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 Bearbeitung:

- 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.) Es findet ausschließlich eine Bearbeitung von Personendaten von Bürgern der Schweizerischen Eidgenossenschaft (nachfolgend „Schweiz“) statt. Sollte eine Bearbeitung von Personendaten von Bürgern eines Mitgliedstaates der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stattfinden, hat die Bearbeitung für diese Personen in Form eines Auftragsverarbeitungsvertrages gem. Art. 28 DS-GVO stattzufinden, welcher dann stets vorrangig ist. Gleichfalls verhält es sich, wenn der Auftraggeber seinen Hauptsitz oder eine Niederlassung innerhalb der eines Mitgliedstaates der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum hat und dort im Rahmen seiner Tätigkeiten die Daten verarbeitet. Der Auftragsverarbeiter gem. Art. 28 DS-GVO wird auch insoweit die Weisungen des Verantwortlichen ausführen.

§ 4 Art und Zweck der Bearbeitung

(1.) Art und Zweck der Bearbeitung der Personendaten 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 Bearbeitung:

- 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 Personendaten

(1.) Die Art der bearbeiteten Personendaten ergibt sich aus dem bestehenden Vertragsverhältnis und aus dem erteilten Einzelauftrag.

(2.) Ergänzend hierzu gilt folgende Beschreibung der Art der bearbeiteten Personendaten:

- _____
- _____
- _____
- _____

Der Auftraggeber ist für die Vollständigkeit der Angaben verantwortlich.

§ 6 Kategorien betroffener Personen

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

- _____
- _____
- _____
- _____

Der Auftraggeber ist für die Vollständigkeit der Angaben verantwortlich.

§ 7 Dokumentierte Weisung

(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. 7 Abs. 1 DSG-neu 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 Datenbearbeitung 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 das DSG-neu oder gegen andere Datenschutzbestimmungen der Schweiz verstößt.

§ 8 Vertraulichkeit

(1.) Der Auftragnehmer gewährleistet und versichert, dass sich die zur Bearbeitung der Personendaten 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. 7, 8 DSG-neu)

(1.) Der Verantwortliche arbeitet nur mit Auftragsbearbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Bearbeitung im Einklang mit den Anforderungen des DSG-neu erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2.) Unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfanges, der Umstände und der Zwecke der Bearbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen hat der Auftragsbearbeiter 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 der Personendaten;
b. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Bearbeitung auf Dauer sicherzustellen;
c. die Fähigkeit, die Verfügbarkeit der Personendaten 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 Bearbeitung.

(3.) Bei der Beurteilung des angemessenen Schutzniveaus hat der Auftragsbearbeiter die Risiken berücksichtigt, die mit der Bearbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu Personendaten, die übermittelt, gespeichert oder auf andere Weise bearbeitet wurden – verbunden sind.

(4.) Der Auftragnehmer unternimmt Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu Personendaten haben, diese nur auf Anweisung des Auftraggebers bearbeiten, es sei denn, sie sind nach dem Recht der Schweiz zur Bearbeitung verpflichtet.

(5.) Zur Gewährleistung der Sicherheit und Vertraulichkeit der Daten hat der Auftragsbearbeiter die in seinem Datenschutz- und Datensicherheitskonzept aufgeführten technisch-organisatorischen Maßnahmen getroffen. Das Datenschutz- und Datensicherheitskonzept des Auftragsbearbeiters wird als verbindlich festgelegt. Die Beschreibung der technischen und organisatorischen Datensicherungsmaßnahmen nach Art. 7, 8 DSG-neu ist in **Beilage AV 1** und **Beilage AV 2** aufgeführt.

§ 10 Einschaltung von weiteren Auftragsbearbeitern (Art. 9 Abs. 3 DSG-neu)

(1.) Der Auftragnehmer nimmt keinen weiteren Auftragsbearbeiter ohne vorherige gesonderte schriftliche Genehmigung des Auftraggebers in Anspruch.

(2.) Erteilt der Auftragnehmer nach vorgängiger Genehmigung Aufträge an weitere Auftragsbearbeiter, so obliegt es dem Auftragnehmer, seine Pflichten aus dieser Vereinbarung dem weiteren Auftragsbearbeiter zu

übertragen. Dies gilt insbesondere für die zwischen den Vertragspartnern festgelegten Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit.

(3.) Für den Fall, dass der Auftraggeber ein cobra cloud-Produkt (siehe **BeilageAV 3** Übersicht der cobra cloud-Produkte in der jeweils aktuellen Fassung) beim Auftragnehmer bestellt, erteilt der Auftraggeber bereits hiermit seine ausdrückliche vorgängige Genehmigung 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.

(4.) Der Auftragnehmer ist berechtigt Unterauftragsverhältnisse nach vorgängiger Genehmigung durch den Auftraggeber zu begründen. Diese vorgängigen Genehmigungen werden als Anlage AV4 zum Vertrag genommen. Der Auftraggeber erteilt in der **Beilage AV 4** konkret bezogen auf den jeweiligen Unterauftragsbearbeiter seine vorgängige Genehmigung zur Begründung des Unterauftragsverhältnisses nach Maßgabe der hier vereinbarten Regelung.

§ 11 Rechte der Betroffenen (Art. 25 DSG-neu)

(1.) Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Bearbeitung 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

(1.) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Bearbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 7 bis 29 DSG-neu genannten Pflichten zur Sicherheit der Bearbeitung von Personendaten 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 Bearbeitung 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 der Personendaten unverzüglich an den Auftraggeber zu melden. Der Auftragnehmer unterstützt den Auftraggeber bei dessen Meldeverpflichtung aus Art. 24 DSG-neu 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. 24 Abs. 4 DSG-neu 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. 22 DSG-neu.

(6.) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen etwa notwendiger vorheriger Konsultationen der Aufsichtsbehörde.

§ 13 Abschluss der Erbringung der Bearbeitungsleistungen

(1.) Nach Beendigung des bestehenden Vertragsverhältnisses und des jeweiligen Einzelauftrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Bearbeitungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen.

(2.) Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Die Löschung ist – auf Verlangen des Auftraggebers – in geeigneter Weise zu dokumentieren.

§ 14 Kontrollrechte des Auftraggebers (Art. 9 Abs. 2 DSG-neu)

(1.) Der Auftraggeber hat das Recht, sich vor der Aufnahme der Datenbearbeitung 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. 11 DSG-neu;
b. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 13 DSG-neu;
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.

§ 15 Berichtigung, Einschränkung und Löschung von Daten

(1.) Der Auftragnehmer darf die Daten, die im Auftrag bearbeitet 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.

§ 16 Datenschutzberater und IT-Sicherheitsberater

(1.) Der Auftragnehmer ist nicht gesetzlich zur Bestellung eines Datenschutzberaters verpflichtet. Gleichwohl hat er diesen ernannt. Der Datenschutzberater des Auftragnehmers übt seine Tätigkeit gem. Art. 10 DSG-neu aus. Die Kontaktdaten sind:

MORGENSTERN consecom GmbH, Herr Jan Morgenstern, Große Himmelsgasse 1, 67346 Speyer,
Tel: 0049 6232/100119-44, E-Mail: privacy@morgenstern-privacy.com

(2.) Der Auftragnehmer hat einen IT-Sicherheitsberater bestellt. Die Kontaktdaten sind:

Arthur Frey, a.frey@cobraag.ch, Tel: 071/6668040, a.frey@cobraag.ch

§ 17 Dokumentationspflichten des Auftragnehmers (Art. 12 DSG-neu)

(1.) Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag für den Auftraggeber durchgeführten Tätigkeiten der Bearbeitung, 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 Datenschutzberaters;
b. die Kategorien von Bearbeitungen, die im Auftrag jedes Auftraggebers durchgeführt werden;
c. gegebenenfalls Übermittlungen von Personendaten ins Ausland, einschließlich der Angabe des betreffenden Staates, sowie bei den in Art. 16 Abs. 2 DSG-neu genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
d. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 8 DSG-neu.

(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 Schweizer Recht. Gerichtsstand ist der Sitz des Auftraggebers.

(4.) Diese Vereinbarung zur Auftragsbearbeitung gem. Art. 9 DSG-neu ersetzt alle vorhergehenden Vereinbarungen zur Auftragsbearbeitung der beiden Parteien mit cobra als Auftragsbearbeiter.

Tägerwilen, den _____ «Ort», den _____

_____ _____

cobra computer's brainware AG «Firma» «Firma2»

Beilagen:

Beilage AV 1: Beschreibung der technischen und organisatorischen Datensicherungsmaßnahmen nach Art. 7, 8 DSG-neu der cobra computer's brainware AG

Beilage AV 2: Beschreibung der technischen und organisatorischen Datensicherungsmaßnahmen nach Art. 7, 8 DSG-neu der Buhl Data Service GmbH für cobra cloud-Produkte

Beilage AV 3: Übersicht der cobra cloud-Produkte

Beilage AV 4: Verzeichnis der Unterauftragsbearbeiter mit vorgängiger Genehmigung gemäß Art. 9 Abs. 3 DSG-neu

cobra® CRM

Beilage AV 1

Beschreibung der technischen und organisatorischen Datensicherungsmassnahmen nach Art. 7, 8 DSG-neu der cobra computer's brainware AG

Kontrollziele	**Beschreibung der technischen und/oder organisatorischen Sicherungsmassnahmen**
Pseudonymisierung und Verschlüsselung personenbezogener Daten	• HTTPS-Verschlüsselung in der Webkommunikation (Data-at-Transport) • RDP-Verschlüsselung der Remotedesktopkommunikation (Data-at-Transport)
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, • 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 Firewallsystems, • Ausschliessliche Verwendung der vom Hersteller der Hardware und Virtualisierungssoftware freigegebenen Software, • Verpflichtung der Mitarbeiter auf das Datengeheimnis • Klimaanlagen, USV in Serverräumen • Virtualisierung/Dynamische Zuteilung der Anwendung auf getrennte Serverräumen • 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, • Protokollierung des Zutritts über Schließanlage • Sichere Löschung von Datenträgern • Regelungen zur Kontrolle von externer Wartung und Fernwartung • Brandmeldeanlage
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 • besonders geschützte Rechenzentrumsabschnitte, • unterbrechungsfreie Stromversorgung, • Überwachungs- und Meldesysteme,
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

Stand: Dezember 2023

cobra®
CRM

Beilage AV 2

Beschreibung der technischen und organisatorischen Datensicherungsmassnahmen nach Art. 7, 8 DSG-neu 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 Klimaanlagen, 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 Feuerwehrleitstelle
- 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: Januar 2022

Beilage AV 3

Übersicht der cobra cloud-Produkte

cobra Private Cloud
cobra WEB PRO

Stand: Januar 2022

Beilage AV4

Verzeichnis der Unterauftragsbearbeiter mit vorgängiger Genehmigung gemäß Art. 9 Abs. 3 DSG-neu

Der Auftraggeber genehmigt, dass der Auftragnehmer folgende Unterauftragsbearbeiter beauftragen darf:

Unterauftragnehmer	**Anschrift**	**Leistung bzw. Modul**
astendo GmbH	Wittestraße 30c, D-13509 Berlin	Bereitstellung der astendo-Softwareprodukte
BUHL-DATA-SERVICE GmbH	Am Siebertsweiher 3/5, D-57290 Neunkirchen	Hosting
cobra – computer's brainware GmbH	Weberinnenstr. 7, D-78467 Konstanz	Bereitstellung der cobra-Softwareprodukte
Ruthardt Softwaretechnik GmbH	Friedrich-List-Straße 34, D-70771 Leinfelden-Echterdingen	Bereitstellung der Ruthardt-Softwareprodukte

Tägerwilen, den _____

«Ort», den _____

_____
cobra computer's brainware AG

_____
«Firma» «Firma2»

Stand: Januar 2022