Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO

zwischen
Auftraggeber (Verantwortlicher):

---

und
Auftragnehmer (Auftragsverarbeiter):

BRZ Deutschland GmbH

Präambel

Dieser Vertrag regelt abschließend die Verpflichtungen des Auftraggebers sowie dessen Tochtergesellschaften mit dem Auftragnehmer zum Datenschutz zur Erfüllung der Anforderungen an eine Auftragsverarbeitung gemäß Art. 28 DS-GVO und ergänzt den Service-/Wartungs- bzw. Mietvertrag („Hauptvertrag“). Er findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten („Daten“) des Auftraggebers in Berührung kommen können.

1. Gegenstand und Dauer des Vertrages

Gegenstand des Vertrages

Gegenstand dieses Vertrages ist die Schaffung der datenschutzrechtlichen Rahmenbedingungen für die vom Auftragnehmer durchgeführte Auftragsverarbeitung.

Bei den im Hauptvertrag zum Outsourcing Rechnungswesen zu erbringenden Leistungen und zu erfüllenden Aufgaben, verarbeitet der Auftragnehmer bzw. Mitarbeiter oder Subunternehmer des Auftragnehmers personenbezogenen Daten des Auftraggebers im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu 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 (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Vertrages

Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieses Vertrages nicht darüberhinausgehende Verpflichtungen ergeben.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.
Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind im Hauptvertrag bzw. in der Leistungsbeschreibung konkretisiert (siehe **Anlage 1**)

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO):

☒ Mitarbeiter-Stammdaten mit Adressdaten
☒ Kunden-Stammdaten
☒ Lieferanten-Stammdaten
☒ Bankverbindungen
☒ Eindeutige Kennzahlen zu Steuer-/Sozialabgaben
☒ ggfs. Lohn- und Gehaltsdaten

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):

☒ Beschäftigte
☒ Kunden
☒ Lieferanten

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten. Sofern sich die gegenständliche Datenverarbeitung in ein Drittland verlagern sollte, wird der Auftragnehmer den Auftraggeber unverzüglich über diesen Ortswechsel in Kenntnis setzen.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftragnehmer wird den Auftraggeber im Falle einer Konsultation der Aufsichtsbehörde nach Art. 36 DS-GVO im erforderlichen Umfang unterstützen.
Der Auftragnehmer führt ein Verzeichnis von Verarbeitungstätigkeiten, welches alle im Auftrag des Auftraggebers ausführten Verarbeitungstätigkeiten beinhaltet. Der Auftragnehmer berücksichtigt dabei die Mindestanforderungen aus Art. 30 Abs. 2 bis 5 DS-GVO.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 4 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen des getroffenen Vertrages und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO).

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom

Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. H DS-GVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Soweit die Daten in einer Privatwohnung verarbeitet werden (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers), sind vom Auftragnehmer die Maßnahmen nach Art. 32 DS-GVO auch in diesem Fall sicherzustellen.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb**.**

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Beim Auftragnehmer ist als Beauftragter für den Datenschutz

heyData GmbH
Schützenstr. 5
10117 Berlin
datenschutz@heydata.eu

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

5. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die

im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

6. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt, soweit er den Auftraggeber hiervon vorab durch Zusendung einer aktuellen Liste der Unterauftragnehmer in Kenntnis setzt. Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der „Information“ zu widersprechen.
Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung direkt gegenüber den Subunternehmern wahrnehmen kann.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die in **Anlage 2** mit Namen, Anschrift und Auftragsinhalt bezeichneten Unterauftragnehmer mit der Verarbeitung von personenbezogenen Daten beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in

Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

7. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird (siehe **Anlage 3**).

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO).

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

8. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

9. Haftung

Die Vertragsparteien haften entsprechend der in Art. 82 DS-GVO getroffenen Regelung. Im Innenverhältnis gilt Art. 28 Abs. 4 S. 2 DS-GVO.

10. Sonstiges

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Es gilt deutsches Recht. Gerichtsstand ist Nürnberg.

Anlage 1 Leistungsbeschreibung

Aufgabenbereiche, die beim Kunden bleiben bzw. die der Kunde direkt durchführt
• Führen von Grundaufzeichnungen wie z.B. Wareneingangsbuch, Kassenberichte • Prüfung der Belege, insbesondere auf materielle Richtigkeit und Vollständigkeit ab Eröffnung des Betriebes • Sämtliche nicht unter §6 Nr. 4 StBerG genannten speziellen Berufsgruppen vorbehaltenen Aufgabengebiete wie z.B. Einrichtung einer Buchhaltung, Erstellung der Jahresabschlüsse, der Einnahmen-Überschussrechnung.
Dienstleistung Finanzbuchhaltung
Einmalige Leistungen bei Übernahme
• Organisation und Schulung der Mitarbeiter, betriebswirtschaftliche Beratung • Installation und Inbetriebnahme eines Dokumentenscanners beim Kunden (soweit über BRZ bezogen) • Implementierung BRZ-Outsourcing Rechnungswesen Musterkontenrahmen • Einrichtung der Stammdaten, Übernahme der Bewegungsdaten
Belege, die nur nach schriftlicher Freigabe und Übermittlung durch den Kunden verbucht werden
• Kasse • Bank • Kreditoren • Debitoren • sonstige lfd. Geschäftsvorfälle (manuelle Erfassung in geringen Umfang soweit vertretbar)
Dienstleistungen, die nur nach schriftlicher Aufforderung durch den Kunden bzw. zum vereinbarten Termin von BRZ erbracht werden
• Übernahme von BRZ Baulohnverbuchung • Offene Posten Liste (mit wöchentlich abgestimmten Buchungsstand) • Maschineller Zahlungsverkehr mit Übersendung Zahlungsvorschlagsliste an Kunden zur Überprüfung und ggf. Nachbearbeitung. Sobald Rücklauf erfolgt die Weiterleitung der Daten an das Kreditinstitut des Kunden. Endgültige Freigabe erfolgt direkt vom Kunden an die ausführende Bank (1x/Woche). Einmalige Einrichtung erforderlich. • Bearbeitung einzelner eingehender Mahnungen (soweit nicht bei Kunden möglich) • Bearbeitung einzelner eingehender Saldenbestätigungen (soweit nicht bei Kunden möglich)
Dienstleistungen zum Monats-/Jahresabschluss
• Abstimmung der Sach-/Finanzkonten (soweit durch BRZ zu vertreten) • Abstimmung der Personenkonten einschließlich offener Posten (soweit durch BRZ zu vertreten) • Übernahme aus der BRZ-Anlagenbuchhaltung (soweit zutreffend)
Auswertungen zum Monats-/Jahresabschluss über Auswertungen online (SaS) durch Kunden
• Summen- und Saldenliste • Vorbereitung der Umsatzsteuervoranmeldung (mit Verprobung) • Betriebswirtschaftliche Auswertung • Liquiditätsübersicht
Dienstleistung Betriebsabrechnung
Belege, die nur nach schriftlicher Freigabe und Übermittlung durch den Kunden von BRZ verbucht bzw. automatisch übernommen werden
• Kosten, Rechnungsstellung, Zahlungseingang (aus Finanzbuchhaltung) • Plankosten nach Kostenarten • Leistungstand aus Rechnungsstellung • Leistungsmeldung nach Kostenstellen durch Kunden • Innerbetriebliche Verrechnungen (manuelle Erfassung in geringen Umfang soweit vertretbar) • Gemeinkostenumlagen (Stammdaten)
Dienstleistungen zum Monats-/Jahresabschluss
• Gemeinkostenrechnung • Kalkulatorische Zinsberechnung
Auswertungen zum Monats-/Jahresabschluss über Auswertungen online (SaS) durch Kunden
• Einzelkostenübersichten • Kostenstellenabrechnung • Chefliste mit kurzfristigem Betriebsergebnis • Graphische Auswertung für Betriebsergebnis, Liquidität, Verwaltung, Sozialkosten, Betriebsmittellohn, etc.
Dienstleistung Kommunikation / Systembetrieb / Archivierung
• Übermittlung von Belegen und Formularen über das von BRZ vorgegebene Scanningsystem (ausschließlich) • Zugriff auf alle archivierten Buchungsbelege über Web-Archiv • Telefonische Erreichbarkeit der Buchhalter während der BRZ-Outsourcing Bürozeiten

Anlage 2 Liste der Unterauftragnehmer

Firma/Unterauftragnehmer	Anschrift/Land	Leistung
ADN – Advanced Digital Network Distribution GmbH	Josef-Haumann-Straße 10 44866 Bochum	Softwarepartner
Allgeier SE	Wehrlestraße 12 81679 München	Softwarepartner
BroadSoft Germany GmbH c/o Cisco Systems GmbH	Lothringer Straße 56 50677 Köln	Softwarepartner, Telefonie
Check Point Software Technologies GmbH	Oskar-Messter-Straße 13 85737 Ismaning	Softwarepartner
Crossinx GmbH	Hanauer Landstr. 291a 60314 Frankfurt am Main	Softwarepartner, Support
Freshworks GmbH	Neue Grünstraße 17 10179 Berlin	Softwarepartner, Support
Hubspot Germany Gmbh	Am Postbahnhof 17 10243 Berlin	Softwarepartner, Marketing
Ing.-Büro f. Steuerung- und Messtechnik Minderlein	Am Leitenbrünnlein 25 91056 Erlangen	Systemprogrammierung
internex GmbH	Lagerstraße 15 A-3950 Gmünd	Softwarepartner, Shopsystem
Microsoft Deutschland GmbH	Walter-Gropius-Straße 5 80807 München	Softwarepartner
SAP Deutschland SE & Co. KG	Hasso-Plattner-Ring 7 69190 Walldorf	Softwarepartner, Dienstleistungspartner
Shopify International Limited	Victoria Buildings, 2. Etage 1-2 Haddington Road Dublin 4, D04 XN32, Irland	Softwarepartner, Shopsystem
Trend Micro Deutschland GmbH	Zeppelinstraße 1 85399 Hallbergmoos	Softwarepartner
Xentral Connect GmbH	Industriering 4 49393 Lohne	Softwarepartner, Shopsystem

Anlage 3 Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1.0 Vertraulichkeit

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

☒ Alarmanlage	☒ Schlüsselregelung / Liste
☒ Automatisches Zugangskontrollsystem	☒ Empfang / Rezeption / Pförtner
☒ Vereinzelungsanlage	☒ Besucherbuch / Protokoll der Besucher
☒ Chipkarten / Transpondersysteme	☒ Mitarbeiter- / Besucherausweise
☒ Manuelles Schließsystem	☒ Besucher in Begleitung durch Mitarbeiter
☒ Sicherheitsschlösser	☒ Sorgfalt bei Auswahl Reinigungsdienste
☒ Schließsystem mit Codesperre	☒ Sorgfalt bei Auswahl des Wachpersonals
☒ Absicherung der Gebäudeschächte	
☒ Türen mit Knauf Außenseite	
☒ Schleusensystem	
☒ Videoüberwachung der Eingänge	

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Anti-Viren-Software Server	☒ Erstellen von Benutzerprofilen
☒ Anti-Virus-Software Clients	☒ Richtlinie „Sicheres Passwort“
☒ Firewall	☒ Richtlinie „Löschen / Vernichten“
☒ Intrusion Detection Systeme	☒ Allg. Richtlinie Datenschutz und / oder Sicherheit
☒ Einsatz VPN bei Remote-Zugriffen	
☒ Verschlüsselung von Datenträgern	
☒ Verschlüsselung von Notebooks / Tablet	

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Aktenschredder (mind. Stufe 3, cross cut)	☒ Einsatz Berechtigungskonzepte
☒ Externer Aktenvernichter (DIN 66399)	☒ Datenschutztresor
☒ Vernichtung von Datenträgern	☒ Verwaltung Benutzerrechte durch Administratoren

1.4 Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Testumgebung	☒ Festlegung von Datenbankrechten
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	
☒ Mandantenfähigkeit relevanter Anwendungen	

1.5 Pseudonymisierung

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.

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

2.0 Integrität

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von VPN	
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	
☒ Nutzung von Signaturverfahren	

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☒ Manuelle oder automatisierte Kontrolle der Protokolle	

3.0 Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert)
☒ Feuerlöscher Serverraum	☒ Kontrolle des Sicherungsvorgangs
☒ Serverraumüberwachung Temperatur und Feuchtigkeit	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ Serverraum klimatisiert	☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☒ USV	☒ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
☒ Schutzsteckdosenleisten Serverraum	☒ Getrennte Partitionen für Betriebssysteme und Daten
☒ RAID System / Festplattenspiegelung	☒ Regelmäßige Wartung technischer Anlagen
☒ Videoüberwachung Serverraum	☒ Spam- und Virenschutzkonzept
☒ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

4.0 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Maßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Anderweitiges dokumentiertes Sicherheitskonzept	☒ Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten
	☒ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
	☒ Interner / externer Informationssicherheitsbeauftragter Name / Firma Kontakt
	☒ Die Organisation kommt den Informationspflichten nach Art.13 und 14 DSGVO nach
	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

4.2 Incident-Response-Management

Maßnahmen zur Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Einbindung von ☒ DSB und ☒ ISB in Sicherheitsvorfälle und Datenpannen
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	
☒ Zweistufiges Intrusion Detection System (IDS)	
☒ Zweistufiges Intrusion Prevention System (IPS)	
☒ Einsatz eines Monitoring-Systems	

4.3 Datenschutzfreundliche Voreinstellungen

Maßnahmen zur Unterstützung von Privacy by design / Privacy by default.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	

4.4 Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln
	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis