

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 zur IT-Systemwartung zu erbringenden Leistungen und zu erfüllenden Aufgaben, kann nicht gesichert ausgeschlossen werden, dass der Auftragnehmer bzw. Mitarbeiter oder Subunternehmer des Auftragnehmers mit personenbezogenen Daten des Auftraggebers in Berührung kommen kann und diese somit im Auftrag für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages verarbeitet werden.

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**)

Bei den im IT-Systemwartungs-Vertrag zu erbringenden Leistungen und zu erfüllenden Aufgaben kann nicht gesichert ausgeschlossen werden, dass der Auftragnehmer bzw. Mitarbeiter oder Subunternehmer des Auftragnehmers mit personenbezogenen Daten des Auftraggebers in Berührung kommen kann und diese somit im Auftrag für den Auftraggeber verarbeitet werden.

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

- Stammdaten (Name, Adresse, Telefonnummer, E-Mailadresse)
- ggfs. Finanzdaten (Bankverbindung, Kreditkartennummer, Darlehen)
- ggfs. Vertragsdaten (Bestellungen, Vertragslaufzeiten, Umsätze, Rechnungen, Kosten etc.)
- ggfs. Kommunikationsdaten, Verbindungsdaten, Inhaltsdaten, IP-Adressen, Cookie-IDs

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

- Beschäftigte
- ggfs. Kunden und deren Mitarbeiter
- ggfs. Lieferanten und Subunternehmer und deren Mitarbeiter
- ggfs. Interessenten und deren Mitarbeiter

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 ausgeführten 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 berechnete 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

Herr Gerd Bachmann
Nürnberger Baugruppe GmbH + Co. KG
Tel.: 0911-3607-450
E-Mail: gerd.bachmann@baugruppe.de

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

BRZ IT-Systemwartung Net express	
Störungsbehebung	
<p>BRZ führt die Störungsbehebung nach eingegangener Serviceanforderung wie folgt durch:</p> <ul style="list-style-type: none"> (a) Innerhalb von 4 Stunden, bezogen auf den Eingang der Serviceanforderung und der Servicezeiten, wird sich BRZ mit dem Kunden in Verbindung setzen und mit der Bearbeitung der Serviceanforderung beginnen. (b) Sollte die Störungsbehebung per Telefon oder Fernwartung nicht möglich sein, wird umgehend veranlasst, dass ein BRZ-IT-Consultant vor Ort die Störung behebt. (c) Gegebenenfalls werden Spezialisten aus der Entwicklungsabteilung zur Behebung der Störung hinzugezogen. (d) Sollte zur Störungsbehebung Hardware, die seitens BRZ geliefert wurde, zu reparieren sein, werden Ersatzteile im Rahmen der Kaufgarantie ohne Berechnung von Arbeitszeit und Reisekosten ausgetauscht. Nach Garantieablauf werden nur die Ersatzteile gesondert berechnet. (e) Nach Störungsbehebung wird die Wiederherstellung der Lauffähigkeit des Servers sowie die Wiederherstellung aller Nutzerrechte und die Datenrücksicherung laut letzter erfolgreicher Sicherung gewährleistet. <p>Der Kunde erhält bei Störungen und Anfragen seitens BRZ eine priorisierte Behandlung.</p> <p>Bitte beachten Sie die Aufgaben des Kunden lt. den besonderen Geschäftsbedingungen für BRZ IT-Systemwartung.</p>	
Wartung	
<p>Bei der IT-Systemwartung „Net Save, Net Express und Net Azure Server-Wartung“ führt BRZ für den Kunden folgende Tätigkeiten durch:</p> <ul style="list-style-type: none"> (a) BRZ-Software: Aktualisierung der Software (Release-Wechsel, Hotfix, Patch) nach Aufforderung des Kunden, Bereitstellung eines Arbeitsplatzinstallationspaketes, Verwaltung Datenbank-Reorg, Verwaltung Benutzer und Lizenzen, Störungsanalyse- und Behebung (nicht beinhaltet ist die Performanceanalyse bei nicht von BRZ gelieferter Hardware). (b) Windows Server Betriebssystem: Aktualisierung des Betriebssystems (Update, Patch), Verwaltung der Active-Directory-Benutzer und -Gruppen sowie den Exchange Postfächern, Verwaltung NTFS-Berechtigungen, Verwaltung DHCP/DNS/IS, Verwaltung Lizenzen und SSL-Zertifikate, Störungsanalyse- und Behebung (nicht beinhaltet ist die Performanceanalyse bei nicht von BRZ gekaufter Hardware). (c) Microsoft/Office 365: Verwaltung der Benutzer, Gruppen, Lizenzen und Postfächer, Störungsanalyse- und Behebung. (d) Antivirus: Aktualisierung der Software (Release, Update, Patch), Verwaltung der Konfiguration, Bereitstellung eines Arbeitsplatzinstallationspaketes, Störungsanalyse- und Behebung (nicht enthalten ist die manuelle Überprüfung auf Viren sowie deren Bereinigung). (e) Backup: Aktualisierung der Software (Release, Update, Patch), Verwaltung der Konfiguration, Wiederherstellung gemäß Punkt 1 „Störungsbehebung“, Störungsanalyse- und Behebung (nicht beinhaltet ist die Datenwiederherstellung im Fall einer Löschung oder Veränderung durch den Kunden oder Dritte) (f) Lokale Server-Hardware und direkt angebundene durch BRZ gelieferte Peripherie (z.B. USV, Switch, Sicherungslaufwerk): Aktualisierung notwendiger Treiber und Firmware, Störungsanalyse- und Behebung. Diese Tätigkeiten sind nicht bei der IT-Systemwartung „Net Azure Server-Wartung“ enthalten. (g) Virtualisierungs-Host: Aktualisierung der notwendigen Software, Störungsanalyse- und Behebung. <p>Alle Tätigkeiten der Wartungsinhalte werden, wenn möglich, aus der Ferne durchgeführt. Bei der IT-Systemwartung „Net Express und Net Azure Server-Wartung“ sind folgende Leistungen zusätzlich inbegriffen:</p> <ul style="list-style-type: none"> (h) Periodisch vorbeugende Systemprüfung mit anschließendem Beratungsgespräch, in welchem Empfehlungen für die vorhandene und zukünftige Systemumgebung ausgesprochen werden. (i) Können die Tätigkeiten im Rahmen der Wartungsinhalte nicht per Ferne durchgeführt werden, wird ein vor Ort Termin ohne Berechnung von Arbeitszeit und Reisekosten durchgeführt. (j) Abweichend zu 1 (a) beträgt die Zeit anstatt 4 Stunden nur 2 Stunden. 	
Serviceleistungen gegen gesonderte Berechnung	
<p>Leistungen, die nicht unter Punkt 2 „Wartung“ oder in den besonderen Geschäftsbedingungen für BRZ IT-Systemwartung selbst beschrieben sind, werden gesondert berechnet, insbesondere sind dies:</p> <ul style="list-style-type: none"> (a) Serviceleistungen außerhalb der Servicezeiten. (b) Serviceleistungen, die durch nicht von BRZ zu vertretenden äußeren Einflüssen oder Bedienungsfehler verursacht wurden, oder die durch nicht von BRZ durchgeführten Wartungsleistungen an der IT-Umgebung oder Betriebssystemen oder Anwendungsprogrammen verursacht wurden, wie z.B. fehlerhafte Bedienung oder Konfiguration durch Kunden/Dritter, Fehler oder Performanceprobleme in Verbindung mit nicht von BRZ gelieferter Hardware. (c) Die Stellung von Leihsystemen und deren Installation und Deinstallation (außer Ziffer 1 (d)). (d) Neuinstallationen und komplette Umstrukturierungen bzw. Umzüge bestehender Systeme. (e) Fachliche Schulung oder Beratung zur Bedienung von Anwendungen oder Geräten. (f) Alle in den besonderen Geschäftsbedingungen für BRZ IT-Systemwartung ausgeschlossenen Leistungen. 	

Anlage 2 Liste der Unterauftragnehmer

Firma/Unterauftragnehmer	Anschrift	Auftragsinhalt
ADN – Advanced Digital Network Distribution GmbH	Josef-Haumann-Straße 10 44866 Bochum	Softwarepartner
Allgeier SE	Wehrlestraße 12 81679 München	Softwarepartner, Support
Check Point Software Technologies GmbH	Oskar-Messter-Straße 13 85737 Ismaning	Softwarepartner
Crossinx GmbH	Hanauer Landstr. 291a 60314 Frankfurt am Main	Softwarepartner, Support
Ing.-Büro f. Steuerung- und Messtechnik Minderlein	Am Leitenbrunnlein 25 91056 Erlangen	Systemprogrammierung, Support
M-SOFT Organisationsberatung GmbH	Große Str. 10 49201 Dissen	Softwarepartner, Support
Microsoft Deutschland GmbH	Walter-Gropius-Straße 5 80807 München	Softwarepartner, Support
SAP Deutschland SE & Co. KG	Hasso-Plattner-Ring 7 69190 Walldorf	Softwarepartner, Support
Veeam Software GmbH	Konrad-Zuse-Platz 8 81829 München	Softwarepartner

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.

<input checked="" type="checkbox"/> Alarmanlage	<input checked="" type="checkbox"/> Schlüsselregelung / Liste
<input checked="" type="checkbox"/> Automatisches Zugangskontrollsystem	<input checked="" type="checkbox"/> Empfang / Rezeption / Pförtner
<input checked="" type="checkbox"/> Vereinzelnungsanlage	<input checked="" type="checkbox"/> Besucherbuch / Protokoll der Besucher
<input checked="" type="checkbox"/> Chipkarten / Transpondersysteme	<input checked="" type="checkbox"/> Mitarbeiter- / Besucherausweise
<input checked="" type="checkbox"/> Manuelles Schließsystem	<input checked="" type="checkbox"/> Besucher in Begleitung durch Mitarbeiter
<input checked="" type="checkbox"/> Sicherheitsschlösser	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl Reinigungsdienste
<input checked="" type="checkbox"/> Schließsystem mit Codesperre	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl des Wachpersonals
<input checked="" type="checkbox"/> Absicherung der Gebäudeschächte	
<input checked="" type="checkbox"/> Türen mit Knauf Außenseite	
<input checked="" type="checkbox"/> Schleusensystem	
<input checked="" type="checkbox"/> Videoüberwachung der Eingänge	

1.2 Zugangskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Login mit Benutzername + Passwort	<input checked="" type="checkbox"/> Verwalten von Benutzerberechtigungen
<input checked="" type="checkbox"/> Anti-Viren-Software Server	<input checked="" type="checkbox"/> Erstellen von Benutzerprofilen
<input checked="" type="checkbox"/> Anti-Virus-Software Clients	<input checked="" type="checkbox"/> Richtlinie „Sicheres Passwort“
<input checked="" type="checkbox"/> Firewall	<input checked="" type="checkbox"/> Richtlinie „Löschen / Vernichten“
<input checked="" type="checkbox"/> Intrusion Detection Systeme	<input checked="" type="checkbox"/> Allg. Richtlinie Datenschutz und / oder Sicherheit
<input checked="" type="checkbox"/> Einsatz VPN bei Remote-Zugriffen	
<input checked="" type="checkbox"/> Verschlüsselung von Datenträgern	
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> Aktenschredder (mind. Stufe 3, cross cut)	<input checked="" type="checkbox"/> Einsatz Berechtigungskonzepte
<input checked="" type="checkbox"/> Externer Aktenvernichter (DIN 66399)	<input checked="" type="checkbox"/> Datenschutztresor
<input checked="" type="checkbox"/> Vernichtung von Datenträgern	<input checked="" type="checkbox"/> Verwaltung Benutzerrechte durch Administratoren

1.4 Trennungsgebot

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

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Trennung von Produktiv- und Testumgebung	<input checked="" type="checkbox"/> Festlegung von Datenbankrechten
<input checked="" type="checkbox"/> Physikalische Trennung (Systeme / Datenbanken / Datenträger)	
<input checked="" type="checkbox"/> 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
	<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> Einsatz von VPN	
<input checked="" type="checkbox"/> Bereitstellung über verschlüsselte Verbindungen wie sftp, https	
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	<input checked="" type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen	<input checked="" type="checkbox"/> Backup & Recovery-Konzept (ausformuliert)
<input checked="" type="checkbox"/> Feuerlöscher Serverraum	<input checked="" type="checkbox"/> Kontrolle des Sicherungsvorgangs
<input checked="" type="checkbox"/> Serverraumüberwachung Temperatur und Feuchtigkeit	<input checked="" type="checkbox"/> Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
<input checked="" type="checkbox"/> Serverraum klimatisiert	<input checked="" type="checkbox"/> Keine sanitären Anschlüsse im oder

	oberhalb des Serverraums
<input checked="" type="checkbox"/> USV	<input checked="" type="checkbox"/> Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
<input checked="" type="checkbox"/> Schutzsteckdosenleisten Serverraum	<input checked="" type="checkbox"/> Getrennte Partitionen für Betriebssysteme und Daten
<input checked="" type="checkbox"/> RAID System / Festplattenspiegelung	<input checked="" type="checkbox"/> Regelmäßige Wartung technischer Anlagen
<input checked="" type="checkbox"/> Videoüberwachung Serverraum	<input checked="" type="checkbox"/> Spam- und Virenschutzkonzept
<input checked="" type="checkbox"/> Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

4.0 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Maßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Anderweitiges dokumentiertes Sicherheitskonzept	<input checked="" type="checkbox"/> Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten
	<input checked="" type="checkbox"/> Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
	<input checked="" type="checkbox"/> Interner / externer Informationssicherheitsbeauftragter Name / Firma Kontakt
	<input checked="" type="checkbox"/> Die Organisation kommt den Informationspflichten nach Art.13 und 14 DSGVO nach
	<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> Einsatz von Firewall und regelmäßige Aktualisierung	<input checked="" type="checkbox"/> Einbindung von <input checked="" type="checkbox"/> DSB und <input checked="" type="checkbox"/> ISB in Sicherheitsvorfälle und Datenpannen
<input checked="" type="checkbox"/> Einsatz von Spamfilter und regelmäßige Aktualisierung	
<input checked="" type="checkbox"/> Einsatz von Virens Scanner und regelmäßige Aktualisierung	
<input checked="" type="checkbox"/> Zweistufiges Intrusion Detection System (IDS)	
<input checked="" type="checkbox"/> Zweistufiges Intrusion Prevention	

System (IPS)	
<input checked="" type="checkbox"/> Einsatz eines Monitoring-Systems	

4.3 Datenschutzfreundliche Voreinstellungen

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

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> 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
	<input checked="" type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	<input checked="" type="checkbox"/> Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln
	<input checked="" type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis