conNect
Organisation und
Netzwerk GmbH

Vereinbarung zur Auftragsverarbeitung

zwischen

Ihre Firma / Kanzlei
Straße und Hausnummer
PLZ und Ort
- nachstehend „Auftraggeber“ oder „Kunde“ genannt –

und

conNect Organisation und Netzwerk GmbH
Lübarser Str. 40-46
13435 Berlin
- nachstehend „Auftragnehmer“ oder „conNect“ genannt –

conNect Organisation und Netzwerk GmbH

Inhaltsverzeichnis

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Gegenstand der Auftragsverarbeitung ist der Service durch technische Mitarbeiter, telefonische Unterstützung der Anwender, ggf. Fernwartung, Instandsetzung, Wartung und / oder Installation der EDV-Systeme zur Sicherstellung der Arbeitsfähigkeit der Benutzer.

Die Dauer des Auftrags bestimmt sich nach Einzelbeauftragungen.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten im Sinne von Art. 4 Nr. 2 EU DSGVO für den Verantwortlichen auf Grundlage dieser Vereinbarung.

Gegenstand des Vertrages ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Im Zuge der Leistungserbringung des Auftragnehmers als zentraler IT-Dienstleister im Bereich der Leistungserbringung, des Supports bzw. der Aministration von Systemen des Auftraggebers, kann ein Zugriff auf personenbezogene Daten jedoch nicht ausgeschlossen werden.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. EU DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standardschutzklauseln, genehmigte Verhaltungsregeln).

§ 2 Art der Daten

(1) Gegenstand der Verarbeitung sind folgende Datenarten/-kategorien:

- Alle personenbezogenen Daten, die sich im System des Auftraggebers befinden, u.a.
- Stammdaten und Kontaktdaten natürlicher Personen
- Besondere Kategorien personenbezogene Daten (z.B. Konfession, Krankheitszeiten)
- Steuernummern, Steueridentifikationsnummern
- Berufsbezeichnungen
- Angaben zu Einkommen und Vermögensituation
- Sozialversicherungsdaten
- Vertragsabrechnungs- und Zahlungsdaten

(2) Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden / Mandaten
- Anwender / Nutzer
- Beschäftigte
- Geschäftspartner des Geschäftspartners / Mandanten
- Ansprechpartner

§ 3 Anwendungsbereich und Verantwortlichkeit

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die in § 1 dieser Vereinbarung benannt sind. Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 EU DSGVO).

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) EU DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 EU DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen (siehe Anlage). Der Auftraggeber trägt die Verantwortung dafür, dass für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau existiert.
Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

(3) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der EU DSGVO sowie bei der Einhaltung der in Art. 32 bis 36 EU DSGVO genannten Pflichten.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet wurden. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen dieser Vereinbarung anfallende Datenschutzfragen.

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen (Art. 32 Abs. 1 lit. d) EU DSGVO).

(8) Der Auftragnehmer berichtigt oder löscht Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese

Datenträger an den Auftraggeber zurück. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Schutzmaßnahmen hierzu sind gesondert zu vereinbaren.

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich.

Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(10) Die für Abrechnungszwecke relevanten Systemdokumentations- und Protokollierungsdaten im Rahmen der Zugriffskontrolle werden unter Beachtung der einschlägigen gesetzlichen Aufbewahrungsfristen gemäß Handelsgesetzbuch sowie der Abgabenordnung aufbewahrt und gelöscht.

Alle anderen Systemdokumentations- und Protokollierungsdaten werden nach Vertragsbeendigung zur Verteidigung von Rechtsansprüchen ein Jahr aufbewahrt und dann gelöscht.

(11) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt.

(12) Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit diese sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung ermittelt.

(13) Der Auftragnehmer hat einen Datenschutzbeauftragten benannt: Heike Zubovic, E-Mail: datenschutz@connect-berlin.de.

§ 5 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen dieser Vereinbarung anfallende Datenschutzfragen.

§ 6 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 7 Nachweismöglichkeiten

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Die Parteien gehen davon

aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Auftraggeber dem Auftragnehmer die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenen Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt.

(4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage zu diesem Vertrag zu überzeugen.

(5) Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfdokuments haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen.

(6) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

§ 8 Subunternehmer (Unterauftragsverarbeiter)

(1) Als Subunternehmer (Unterauftragsverarbeiter) im Sinne dieser Vereinbarung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftraggeber erteilt eine allgemeine Genehmigung, dass der Auftragnehmer weitere Unterauftragsverarbeiter heranziehen oder bestehende Unterauftragsverarbeiter auswechseln kann. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(3) Der Auftragnehmer informiert den Auftraggeber im Voraus über die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern.

Der Auftragnehmer führt auf seiner Homepage eine Liste mit den aktuell beauftragten Unterauftragsverarbeiter:
https://www.connect-berlin.de/datenschutz#subunternehmen

(4) Der Auftraggeber hat das Recht, mit einer Frist von 10 Tagen der Beauftragung eines neuen Unterauftragsverarbeiters zu widersprechen. Für den Widerspruch ist die Textform ausreichend. Sind die Parteien nicht in der Lage, den Widerspruch beizulegen, kann der Auftraggeber die Dienstleistung, die ohne den Einsatz des neuen Unterauftragsverarbeiters nicht erbracht werden kann, kündigen.

(5) Die aktuell beauftragten Unterauftragsverarbeiter sind in Anlage 2 mit Namen, Anschrift und Auftragsinhalt noch einmal aufgeführt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

(6) Der Auftragnehmer hat mit dem Unterauftragsverarbeiter als weiteren Auftragsverarbeiter einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat

der Auftragnehmer dem Subunternehmen als weiteren Auftragsverarbeiter dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind.
(7) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden.

§ 9 Benennung weisungsberechtigter Personen seitens des Auftraggebers

Folgende Personen seitens des Auftraggebers sind berechtigt, dem Auftragnehmer im Rahmen des in § 1 dieser Vereinbarung konkretisierten Auftrags, Einzelweisungen zu erteilen:

Name, Vorname	Position im Unternehmen
_____	_____
_____	_____
_____	_____
_____	_____

Personelle Änderungen hinsichtlich der Weisungsberechtigung sind dem Auftragnehmer frühzeitig schriftlich mitzuteilen.

§ 10 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 als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.
(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
(3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht
(4) Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland. Es gilt somit deutsches Recht.
(5) Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag, insbesondere über seinen Bestand und seine Erfüllung ist Berlin.

§ 11 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend Art. 82 EU DSGVO.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
conNect	Auftraggeber

conNect Organisation und Netzwerk GmbH

Anlage 1

Technische und organisatorische Maßnahmen
i. S. d. Art. 32 Abs. 1 EU DSGVO

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b EU DSGVO)

Zutrittskontrolle
Eingeleitete Maßnahmen, die Unbefugten den Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren:

- Mechanisches Schließsystem mit zusätzlichem Transponder;
- Sich zeitgesteuert, automatisch aktivierende Alarmanlage mit Aufschaltung zum Wachschutz;
- Bewegungsmelder;
- selbstschließende Sicherheits-Eingangstür mit Wechselsprechanlage;
- Fenster mit Außenrollos in der unteren Etage;
- Einbindung in das Sicherheitskonzept des Gewerbehofes (gesamtes Gelände nachts abgeriegelt);
- Regelung und Protokollierung der Schlüsselvergabe an Mitarbeiter;

Zugangskontrolle
Vorkehrungen die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Benutzerprofile mit individuellen Zugriffsrechten;
- Authentifikation mit persönlichem Benutzernamen und erzwungenem, komplexen Passwort;
- Einsatz von aktueller Anti-Viren-Software und mehrerer Firewalls;
- Durchgängiger Einsatz von VPN-Technologie;
- Passwortgesicherte mobile Endgeräte;
- Zusätzliche Hardware-Vollverschlüsselung der Notebooks;
- Verbindliche interne Richtlinie zur Nutzung der DV-Anlage;
- Regelung und Protokollierung der Schlüsselvergabe an Mitarbeiter;

Zugriffskontrolle
Wie wird gewährleistet, dass die zur Benutzung des 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:

- Verwaltung der Benutzerrechte durch Systemadministratoren;
- Anzahl der Systemadministratoren auf Minimum beschränkt (Vertreterregelung);
- Zugriffe geregelt durch ein Berechtigungskonzept;
- Genutzte Passwörter sind nach der Passwortrichtlinie des BSI erstellt und unterliegen einem Zwangswechsel und Vorgaben an die Komplexität;
- sichere Aufbewahrung von Datenträgern;
- Ordnungsgemäße Vernichtung von Datenträgern nach DIN 66399 mit Protokollierung;
- Einsatz von abgeschlossenen Aktentonnen und Entsorgung über zertifizierten Dienstleister;

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

- Zugriffsrechte nach striktem Berechtigungskonzept auf Basis von Benutzern, Gruppen und Rollen;
- Getrennte Datenbanken für unterschiedliche Bereiche;
- Speicherung auf gesonderten logischen Laufwerken;
- Trennung von Produktivsystem und Testumgebung (mehrere autarke, logische Testumgebungen);

Verschlüsselung

Zugriffe von extern auf unsere Systeme erfolgen ausschließlich über verschlüsselte Verbindungen. Die VPN-Einwahl ist zusätzlich über eine Zwei-Faktor-Authentifizierung abgesichert.

II. Integrität (Art. 32 Abs. 1 lit. b EU DSGVO)

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:

- Zentrale Datenhaltung und keine lokale Datenablage;
- Zugriff ausschließlich durch VPN-Tunnel;
- Einsatz verschlüsselter Datenträger;
- Sichere Emailübertragung durch Nutzung der E-Mailverschlüsselung;

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:

- Einsatz einer revisionssicheren Software im unternehmensrelevanten Umfeld;
- Protokollierungsfunktion im Buchhaltungsbereich;
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Nutzerspezifisch eingeschränkte Zugriffs- und Löschrechte;
- Automatische Emailarchivierung;

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b EU DSGVO)

Verfügbarkeitskontrolle

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

- Separater Serverraum mit Klimaanlage;
- Einsatz einer unterbrechungsfreien Stromversorgung (USV);
- Feuer- und Rauchmeldeanlage im Serverraum und im gesamten Gebäude;
- Feuerlöschgeräte im Serverraum;
- Datenredundanz durch RAID-System;
- Sicherungs- und Wiederherstellungskonzept mit Aufbewahrung der Datensicherung an unterschiedlichen Orten;
- Regelmäßige Test zur Datenwiederherstellung;
- Einsatz aktueller Hard- und Software (turnusmäßiger Hardwaretausch, Softwareupdates);

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d; Art. 25 Abs. 1 EU DSGVO)

- Es ist ein interner Datenschutzbeauftragter benannt.
- Alle Beschäftigten sind zum Datenschutz geschult. Datenschutzschulungen erfolgen 1 jährlich.
- Alle Beschäftigten sind zur Verschwiegenheit und auf die Beachtung des Datenschutzes verpflichtet.
- Es gibt ein Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 EU DSGVO.
- Auftragskontrolle
  - › Keine Auftragsverarbeitung im Sinne von Art. 28 EU DSGVO ohne entsprechende Weisung des Auftraggebers;
  - › Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit);
  - › Schriftliche Weisungen an den Auftragnehmer durch Vereinbarungen zur Auftragsverarbeitung gemäß Art. 28 EU DSGVO;
  - › Verpflichtung der Mitarbeiter des Auftragnehmers Vertraulichkeit und Datenschutz;
  - › Vorherige und laufende Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen;

conNect Organisation und Netzwerk GmbH

Anlage 2

Unterauftragsverarbeiter

Bezeichnung		Tätigkeit
DATEV eG Paumgartner Straße 6-14 90429 Nürnberg		Rechenzentrumsdienstleistungen, Fernwartung
LogMeIn Ireland Limited Bloodstone Building Block 70 C Sir John Rogerson´s Quay Dublin 2, Ireland		Fernwartung, Videokonferenzen
Octopus Cloud AG Baarerstraße 6300 Zug / Switzerland		ASP Software Inventar
Rhenus Data Office Lahnstraße 31 12055 Berlin		Daten- und Aktenvernichtung
c-entron Software GmbH Liststraße 1 89079 Ulm		ERP-Lösung: Kundenverwaltung, Erfassung von Dienstleistung, Angebotserstellung, Rechnungserstellung
ESTOS GmbH Petersbrunner Str. 3a 82319 Starnberg		interne Kommunikation, CTI-Lösung
NCP engineering GmbH Dombühler Str. 2 90449 Nürnberg		Remote Access VPN Lösung
Signotec GmbH, Am Gierath 20b 40885 Ratingen		Dienstleister elektronische Signatur
1&1 IONOS SE Elgendorfer Str. 57 56410 Montabaur		Webserver

Bezeichnung	Tätigkeit
TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen	Fernwartung
FP Digital Business Solutions GmbH Ein Unternehmen der FP-Gruppe Griesbergstraß 8 31162 Bad Salzdetfurth	Dienstleister elektronische Signatur
DRACOON GmbH Galgenbergstraße 2a 3053 Regensburg	Dienstleister Cloud-Services / Datenaustausch