Rahmenvertrag über die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten im Auftrag (gemäß Art. 28 europäische DS-GVO)

zwischen dem/der

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

Connectivity GmbH

Mallaustrasse 21

68219 Mannheim

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Gegenstand des Auftrags zum Datenumgang im Zusammenhang mit der Software **ConAktiv*** ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

- Durchführung von Wartungsarbeiten
- Support (Unterstützung bei Fragen zur Handhabung von ConAktiv)
- Unterstützung per Fernwartung
- Fehleranalysen

* ConAktiv ist eine Software, die zur betrieblichen Steuerung und Unterstützung von Prozessen in Unternehmen eingesetzt wird.

1.2 Dauer

Der Auftrag ist für die Dauer des Supportvertrags mit der Connectivity GmbH befristet.

2. Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

- Support- und Wartungsleistungen ConAktiv

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

2.2 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind u.a. folgende Datenarten/-kategorien, die in der vom Auftraggeber verwendeten ConAktiv-Datenbank angelegt sind:

- Personenstammdaten

  Umfassen alle in der Datenbank hinterlegten Informationen (z.B. Vorname, Name, Stadt)

- Kommunikationsdaten (z.B. Telefon, E-Mail)

  Umfassen alle in den Stammdaten hinterlegten Telefonnummern und E-Mailadressen sowie E-Mailkorrespondenz

- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
  Umfassen alle in der Datenbank hinterlegten Verträge

- Vertragsabrechnungs- und Zahlungsdaten

  Umfassen alle Rechnungs- und Eingangsrechnungsdaten

2.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen u.a.:

- Kunden
- Interessenten
- Beschäftigte
- Lieferanten
- Ansprechpartner

3.Technisch-organisatorische Maßnahmen

3.1 Die technischen und organisatorischen Maßnahmen der Connectivity GmbH sind Bestandteil des Rahmenvertrags über die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten im Auftrag. [Anlage 1] Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.2 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 EU-DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 EU-DSGVO zu berücksichtigen [Einzelheiten in Anlage 1].

3.3 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. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

4.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich

unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2 Sofern vom Auftraggeber beauftragt, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers und nach Prüfung auf Machbarkeit durch den Auftragnehmer umzusetzen und sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 EU-DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 EU-DSGVO ausübt.

Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
Der Datenschutzbeauftragter ist beim Auftragnehmer als

Vorname:	Moritz
Name:	Görmann
Organisationseinheit:	CTM-Com GmbH
Telefon:	06154 – 5760505 -100
E-Mail:	datenschutz@ctm-com.de

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

Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 EU-DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 EU-DSGVO [Einzelheiten in Anlage 1].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Der Auftragnehmer muss den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit sie 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 beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Der Auftragsnehmer hat eine Nachweisbarkeitspflicht der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages. Für die Ermöglichung dieser Pflicht kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

6. Unterauftragsverhältnisse

Als Unterauftragsverhältnisse im Sinne dieser Regelung 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 oder die Entsorgung von Datenträgern 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. Derzeit besteht ein Unterauftragsverhältnis mit der Firma Diginet, 64319 Pfungstadt für Wartungs- und Hostingdienstleistungen.

7. Kontrollrechte des Auftraggebers

7.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 EU-DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 EU-DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

7.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der EU-DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

9.1 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

9.2 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

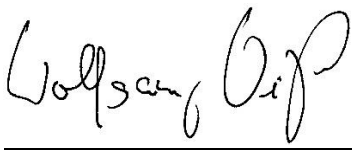
10. Löschung und Rückgabe von personenbezogenen Daten

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

10.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

_____, den	_____	_____Mannheim_____, den 01.04.2023	
Ort	Datum	Ort	Datum



_____ _____

- Verantwortlicher - - Auftragsverarbeiter –

Anlage 1:

Allgemeine technische und organisatorische Maßnahmen bei Connectivity GmbH

Technische-organisatorische Datensicherheit nach Art. 32 DSGVO

Sofern die Connectivity GmbH zu eigenen Zwecken oder im Auftrag von Kunden oder sofern Dienstleister im Auftrag von der Connectivity GmbH personenbezogene Daten erheben, verarbeiten oder nutzen, hat die Connectivity GmbH die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Vorgaben der Datenschutzgesetze, insbesondere die in der Anlage zu § 9 BDSG genannten Anforderungen, zu gewährleisten. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind, die nachfolgenden Ziele zu erreichen:

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

1. Zutrittskontrolle:

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Notwendige Maßnahmen: räumlich-physische Sicherungsmaßnahmen

Extern:

- Das Büro befindet sich in einem Bürogebäude.
- Der Zutritt zum Gebäude erfolgt über zwei Haupteingänge. Über das Wochenende und nachts ist das Gebäude abgeschlossen. Montags bis freitags öffnet sich das elektrische Türschloss an beiden Eingängen um 06:00 Uhr und verschließt sich ab 20 Uhr. Befugte, die einen Schlüssel besitzen, haben jederzeit Zutritt zum Gebäude.
- Der Zugang zum Büro im 1.OG erfolgt über einen weiteren Zugang mit abschließbarer Tür. Diese Tür ist immer verschlossen und kann nur durch Befugte mit einem Schlüssel geöffnet werden
- Der Zutritt in das Büro erfolgt über einen eigenen Schlüssel oder nach dem Benutzen der Klingel.

Intern:

- Über die Schlüsselvergabe wird eine entsprechende Dokumentation geführt.
- Beim Verlust eines Schlüssels werden die Schließanlage und die Schlüssel ausgetauscht.

Mitarbeiter werden angewiesen, bei Abwesenheit ihr Büro zu verschließen oder ihre Arbeitsunterlagen wegzuschließen. Unterlagen und Datenträger, die Informationen mit erhöhtem Schutzbedarf enthalten, sind verschlossen aufzubewahren.

Besucher:

- Es gibt einen Zugang zum Büro, durch den alle Besucher nach dem Klingeln eingelassen werden. Die Klingelanlage ist ohne Kamera.
- Der Empfang durch Mitarbeiter ist immer gewährleistet.
- Besucher werden am Eingang des Büros abgeholt und bis zum gewünschten Ziel begleitet. Beim Verlassen werden Besucher wieder zum Empfangsbereich begleitet.
- Zur Beaufsichtigung von externen Firmen bzw. Mitarbeiter gelten ähnliche Regelungen.

Server-Raum:

Das Büro der Connectivity GmbH verfügt über keinen Serverraum vor Ort. Die Connectivity GmbH hat die Firma Diginet GmbH, Hilpertstraße 31, 64295 Darmstadt beauftragt die Administration der Daten zu übernehmen. Die Daten befinden sich auf Servern der Firma Diginet im Rechenzentrum DARZ, Julius-Reiber-Str. 11, 64293 Darmstadt, Deutschland.

2. Zugangskontrolle:

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Notwendige Maßnahmen: Berechtigungsvergabe (Passwort), Firewall, Verschlüsselungsmaßnahmen, Festplattenverschlüsselung

- Die Vergabe von Zugangsberechtigungen erfolgt zur Regelung der Zugriffe auf die Domain. Hierzu wurden Benutzerprofile erstellt. Zur Einrichtung der Benutzergruppen erfolgt über entsprechende Tools.
- Der Zugriff auf die Datenbank erfolgt über ein separates Passwort und einen zusätzlichen 2FA-Login.

Passwörter:

- Die Identifikation und Authentifikation erfolgen durch Abfrage von User-ID und Passwort. Hierzu sind entsprechende Passwortregeln vorhanden:
  - Zeichen Mindestlänge
  - Alphanumerischer Zeichensatz
  - Kleinbuchstabe, zwingend
  - Großbuchstabe, zwingend
  - Zahl, zwingend
  - Sonderzeichen
  - Ausschluss von Trivialkennwörter

- Vorgeschriebenes Aktualisierungsintervall

Firewall:

- **Connectivity GmbH** betreibt zur Unterbindung unberechtigter Zugriffe auf Firmennetze hoch performante Firewall-Systeme. Hierbei handelt es sich um Systeme eines renommierten und bekannten Herstellers.
- Um den bestmöglichen Schutz der Daten gewährleisten zu können, wird das Firewall-System ständig aktualisiert und bei Bekanntwerden neuer Sicherheitsrisiken entsprechend angepasst.
- Die Konfiguration und Funktionsfähigkeit der Firewall wird von einer Fachfirma regelmäßig kritisch überprüft und kontrolliert. Der Betrieb der Firewall wird regelmäßig überwacht.

3. Zugriffskontrolle:

Die Zugriffsberechtigten dürfen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Notwendige Maßnahmen: Berechtigungskonzept, effektive, rollenbasierte Rechteverwaltung umsetzen.

- Die Zugriffskontrolle ist durch anwenderbezogene Zugriffsberechtigungen auf alle Daten innerhalb der Datenbank geregelt. Das Berechtigungskonzept ist programmtechnisch in der Anwendung hinterlegt und besitzt vorgefertigte Rechteprofile. Die Rechtevergabe erfolgt durch die Geschäftsführung.
- Die Zugriffsberechtigungen sind auf Dateien, Datensätze, Datenfelder und Anwendungsprogramme differenzierbar. Die Verarbeitungsmöglichkeiten sind auf das Lesen, Ändern und Löschen differenzierbar. Benutzer mit gleichen Rechten werden zu Benutzergruppen zusammengefasst.
- Der Entzug der Zugriffsrechte erfolgt durch das Entfernen der Berechtigung aus einer Gruppe.
- Das Büro verfügt über abschließbare Schränke, um den Zugriff auf sensible Daten für Unbefugte zu verhindern. Nur ausgewählte Mitarbeiter haben Zugriff.
- Das Büro verfügt über einen Aktenvernichter der Sicherheitsstufe P-4 nach DIN 66399.

4. Trennungskontrolle:

Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können.

Notwendige Maßnahmen: Logische Trennung und physikalische Trennung

- Die logische Trennung erfolgt durch ein Berechtigungskonzept mit Festlegung der Zugriffsrechte

- Die physikalische Trennung erfolgt durch die Speicherung der Daten in getrenntem Datensammler

II Integrität (Art. 32 Abs. 1 lit. b DS-GVO):

1. Weitergabe Kontrolle:

Personenbezogene Daten dürfen bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es muss überprüft und festgestellt werden können, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Notwendige Maßnahmen: Datensicherheitskonzept für die interne und Verschlüsselungsmaßnahmen für die internetbasierte Kommunikation

- Eine elektronische Übertragung von personenbezogenen Daten findet nur während des Backups der ERP-Daten statt.
- Alle Daten werden grundsätzlich auf den Servern verarbeitet. Eine lokale Datenhaltung auf den Notebooks und Workstations ist untersagt.

Formulare:

- Der Zugriff auf Formulare (Rechnungen) erfolgt per Berechtigung auf die entsprechende Datenbank.

Telefax:

- Das Faxgerät wird durch das Sekretariat überwacht.

Datenträgertransport:

- Es findet kein Datenträgertransport statt.

2. Eingabekontrolle:

Es muss nachträglich überprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Notwendige Maßnahmen: Protokollierung, Auswertung

- Die Zugriffe der Benutzer werden hinsichtlich der letzten Datenänderung in einem Datensatz durch einen Benutzer protokolliert. Diese Information bleibt bis zur nächsten Änderung bestehen. Im Falle einer böswilligen Löschung, kann man mit einem Rollback die Daten wiederherstellen.

III Gewährleistung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

(Art. 32 Abs. 1 lit. b DS-GVO):

1. Verfügbarkeit (der Daten):

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Verfügbarkeit von Daten.

Connectivity GmbH wird personenbezogene Daten gegen zufällige Zerstörung oder Verlust effektiv schützen. Die Zugriffe der Benutzer werden hinsichtlich der letzten Datenänderung in einem Datensatz durch einen Benutzer protokolliert. Diese Information bleibt bis zur nächsten Änderung bestehen. Im Falle einer böswilligen Löschung, kann man mit einem Rollback die Daten wiederherstellen.

Datensicherung:

- Die Datensicherung findet zentral und vollautomatisch statt.
- Zur Datensicherung wird ein Datensicherungs-Tool eingesetzt.
- Neben der automatisierten Sicherung werden regelmäßig manuelle Datensicherungen durchgeführt.
- Alle wichtigen Unternehmensdaten werden gesichert.
- Die Wiederherstellungen von Datensicherungen werden überprüft.

Notfallvorsorge:

- Es ist sichergestellt, dass bei einem Ausfall der Systeme (Server) der Normalbetrieb schnell wieder erreicht werden kann.

Schutzmaßnahmen und Unterbrechungsfreie Stromversorgung (USV):

- Die Server der Firma Diginet befindet sich im Rechenzentrum der DARZ GmbH. Alle Daten sind hier rund um die Uhr mit höchster Zuverlässigkeit und den höchsten Standards für Sicherheit und Datenschutz geschützt: u.a. Multiredundante Stromversorgung (USV (2N+1) und Dieselstrom), Brandschutzkonzept mit einem weichen Flutungssystem, Blitzschutz der Kategorie 1. Die Wirksamkeit der USV wurde getestet. Alle wichtigen Geräte werden bei einem Stromausfall automatisch heruntergefahren.
- Server bei DARZ erfüllen alle Bestimmungen des deutschen und EU- Datenschutzrechts.

Archivräume:

- Alle Akten sind im Sekretariat untergebracht.

2. Belastbarkeit (der Daten):

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Belastbarkeit der Systeme.

Virenschutz:

- Das Virenschutzprogramm wird regelmäßig aktualisiert.
- Alle eingehenden E-Mails werden auf Viren gescannt.
- Alle externen Dateien und/oder Datenträger werden auf Viren überprüft.

Firewall:

- siehe oben Zugangskontrolle

3. Rasche Wiederherstellbarkeit:

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Wiederherstellbarkeit von Daten und Systemen.

Die Daten der Connectivity GmbH hat die Firma Diginet beauftragt die Daten der Connectivity zu hosten. Über die beauftrage Firma Diginet werden die Daten auf einem Server der DARZ GmbH gehostet. Die Server bei DARZ erfüllen alle Bestimmungen des deutschen und EU- Datenschutzrechts. DARZ ist zudem nach den wichtigsten Standards ISO 27001, PCI-DSS zertifiziert.

IV Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)**:**

1. Auftragskontrolle:

Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden.

- Soweit die **Connectivity GmbH** im Auftrag Daten von Kunden verarbeitet, erfolgt dies im Wege der Auftragsverarbeitung nach Art. 28 DSGVO. Der Verantwortliche bleibt Alleinberechtigter an den Daten ("Herr der Daten"). **Connectivity GmbH** darf kunden- bzw. personenbezogene Daten nur im Rahmen der vertragsgegenständlichen Leistungen nach den Vorgaben des Verantwortlichen verarbeiten und nutzen.

- Die übergebenen Daten (der Kunden) werden grundsätzlich verschlüsselt gespeichert.

- Zur Gewährleistung der Sicherheit der Kundendaten wird die **Connectivity GmbH** die erforderlichen technischen und organisatorischen Maßnahmen, insbesondere gemäß Art. 32 DSGVO, welche vorliegend beschrieben sind, umsetzen.

- Eine Einschaltung von Dienstleistern (Subunternehmern) durch die **Connectivity GmbH** erfolgt nur mit Zustimmung des Verantwortlichen und nach Abschluss eines schriftlichen Vertrages (Anlage) mit dem Dienstleister, welcher die Vorgaben der Auftragsverarbeitung umsetzt.

2. Datenschutz-Management:

Maßnahmen, die gewährleisten, dass Methoden evaluiert wurden, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, organisieren, steuern und kontrollieren.

- **Connectivity GmbH** hat einen Datenschutzbeauftragten ernannt, welcher die gesetzlichen Organisations- und Kontrollaufgaben umsetzt.

- Es findet eine regelmäßige Sensibilisierung der Mitarbeiter zum Datenschutz durch den externen Datenschutzbeauftragten statt

- Die Mitarbeiter haben eine Verpflichtung auf Vertraulichkeit bzw. auf das Datengeheimnis unterzeichnet

- Die TOMs werden mindestens 1 x jährlich auf ihre Wirksamkeit überprüft

3. Vorfallreaktionsplan – Incident Response Plan (IRP):

Maßnahmen, die gewährleisten, dass Sicherheitsvorfällen vorgebeugt werden kann oder im Falle von bereits eingetretenen Sicherheitsvorfällen, dass Daten und Systeme geschützt werden, und eine schnelle Analyse und Behebung des Sicherheitsvorfalls durchgeführt werden kann.

Folgende Verhaltensregeln gelten allgemein für alle Mitarbeiter:

- Einbindung von externen Dienstleistern zur Untersuchung und Behebung von Datenpannen
- Bei Datenpannen wird umgehend der externe Datenschutzbeauftrage informiert.
- Bei Feststellung eines Ausfalls von Teilen des IT-Systems (Fileserver, Datenbankserver, Zugang zum Email-Server usw.) muss umgehend die Fa. Diginet, Hilpertstraße 31 64295 Darmstadt (externer IT-Dienstleister) informiert werden.
- Alle Mitarbeiter haben im Vorfeld die Erstellung des Notfallfallvorsorgekonzepts (z. B. Erstellung der Dokumentationen) nach Kräften zu unterstützen. Nur durch eine gute Vorbereitung ist es möglich, im Notfall Ruhe zu bewahren und nicht durch unüberlegte Handlungen den Schaden zu vergrößern.

- Unregelmäßigkeiten, die auf einen Sicherheitsvorfall hindeuten, sind unverzüglich zu melden.
- Es sind die Anweisungen des Notfall-Verantwortlichen und etwaige spezielle Verhaltensregeln zu beachten.
- Alle Begleitumstände sind ungeschönt, offen und transparent zu erläutern, um damit Schäden zu mindern, schnell Lösungen zu finden und Erkenntnisse zur Verbesserung des IT-Sicherheitskonzepts zu gewinnen.
- Informationen über den Notfall dürfen nicht an unautorisierte externe Dritte weitergegeben werden.

Nach einem Notfall ist der sichere Normalzustand wiederherzustellen und an der Aufarbeitung des Notfalls mitzuarbeiten.

- Derjenige, der einen Sicherheitsvorfall bemerkt, leitet umgehend erste Maßnahmen ein (z. B.: Alarmierung, Rechner ausschalten)

  Die verantwortlichen Stellen, die aktiv handeln oder Verantwortung übernehmen müssen, sind zu alarmieren (Geschäftsführung, Diginet). Sie übernehmen dann in der Regel die weitere Untersuchung und Bewertung des Vorfalls und leiten Maßnahmen ein. Maßnahmen, die auf die Wiederherstellung der Betriebsfähigkeit nach Ausfall eines IT-Systems ausgerichtet sind.

  - Backup aller Relevanten Daten und Verfügbarkeit der Backup-Daten
  - Hard- und Software, um ggf. kurzfristig Daten und Anwendungen auf Ersatzrechnern zu starten.

  Alarmierungspläne sowie Regelung der Verantwortlichkeiten:
  - Wenn es zu einem Sicherheitsvorfall z.B. Viren-Angriff oder zu einem Ausfall von Teilen des IT-Systems kommt, ist umgehend die Geschäftsführung zu informieren. Diese entscheidet über das weitere Vorgehen. Maßnahmen zur Schadensbegrenzung bzw. der Wiederherstellung werden mit Diginet abgestimmt. Die Durchführung dieser Maßnahmen darf nur durch Personen erfolgen, die laut Datenschutzrichtlinie der Connectivity GmbH autorisiert sind.

Der Einsatz von Virenscanner unterliegt einer regelmäßigen Aktualisierung

V Datenvernichtung

- Die ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln ist gewährleistet.
- Papier wird im Schredder (Sicherheitsstufe P-4 nach DIN 66399) vernichtet, Datenträger werden vor der Entsorgung zerstört.
- Zur Sammlung von Papier stehen entsprechende Behälter zur Verfügung.

Anlage 2:

Unterauftragnehmer

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Diginet GmbH	Hilpertstraße 31 64295 Darmstadt Deutschland	Hosting Kundenserver, Hosting Server Connectivity GmbH, Netzwerkadministration
Lohndirekt GmbH	Lise-Meitner-Straße 14A, 24941 Flensburg Deutschland	Lohnabrechnung
SYRIUS Online Marketing	Zehntwiesenstr. 44a 76275 Ettlingen Deutschland	Suchmaschinenoptimierung, Google Ads Administration
Salesviewer	Bongardstrasse 29 44787 Bochum Deutschland	Digitale Lead-Generierung über Identifizierung von Webseitenbesuchern