Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 EU - DSGVO

zu den Verträgen unter der

Kundennummer: 244005

zwischen

Marco Schäfer
Damaschkestr. 3
07985 Elsterberg

- im Folgenden "AG" genannt - als "Verantwortlicher" gemäß DSGVO

und

netcup GmbH
Daimlerstr. 25
76185 Karlsruhe

- im Folgenden "AN" genannt - als "Auftragsverarbeiter" gemäß DSGVO

- zusammen "Vertragspartner" oder "Parteien" genannt -

Preamble

Diese Vereinbarung dient als Ergänzung und konkretisiert die Verpflichtungen der Vertragspartner zum Datenschutz für alle bestehenden und zukünftigen rechtswirksamen Verträge, Master Service Agreements, Service Level Agreements, Leistungsbeschreibungen etc. (im Folgenden zusammengefasst als "Vertrag" oder "Verträge" bezeichnet) zwischen AG und AN. Sie findet Anwendung auf alle Tätigkeiten, die mit den Verträgen zwischen AG und AN in Zusammenhang stehen und bei denen Beschäftigte des AN oder durch den AN Beauftragte personenbezogene Daten (im Folgenden "Daten" genannt) des AG als Verantwortlichen im Auftrag verarbeitet. Im Übrigen gelten für dieses Dokument alle Bestimmungen und Begriffe der EU-Datenschutzgrundverordnung [Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG)] (im Folgenden "DSGVO" genannt) sowie darüberhinausgehend das für den AG zutreffende respektive für die Verträge anwendbare nationalstaatliche Datenschutzrecht. Zum besseren Verständnis und zur leichteren Lesbarkeit gilt in diesem Dokument bei allen personenbezogenen Bezeichnungen die gewählte Form gleichermaßen für alle Geschlechter. Es wird darauf hingewiesen, dass der AN als verbundenes Unternehmen der Anexia-Unternehmensgruppe mit der ANEXIA Internetdienstleistungs GmbH als Leitgesellschaft (im Folgenden zusammengefasst als "Anexia" bezeichnet) allen unternehmensgruppenweiten Regelungen ("Anexia Corporate Binding Rules") unterliegt und die Auftragsverarbeitungen, die der AN für den AG als Verantwortlichen durchführt, vor allem durch für Anexia tätige Personen sowie im Bedarfsfall durch Nutzung von Infrastrukturen und Systemen von Anexia durchgeführt werden. Die aktiven Zertifizierungen der Anexia-Unternehmen netcup GmbH, der ANEXIA Internetdienstleistungs GmbH sowie der DATASIX Rechenzentrumsbetriebs GmbH in den Bereichen ISO 9001 (Qualitätsmanagement), ISO 27001 (Informationssicherheit) sowie ISO 27701 (Datenschutz) und weitere sind jeweils aktuell auf den jeweiligen Unternehmenshomepages publiziert.

1. Gegenstand, Ort und Dauer der Auftragsverarbeitung

1. Gegenstand und Dauer des Auftrags, Art und Zweck, Ort der Verarbeitung und die verarbeiteten Datenkategorien sowie die Kategorien der betroffenen Personen werden in ANHANG 3 gesondert vom AG angegeben.
2. Über den Ort der Verarbeitung unter Berücksichtigung des Kapitels V DSGVO entscheidet ausschließlich der AG als
3. Der Verantwortliche weist den AN vertraglich, mittels Weisung oder mittels ANHANG 3 an, die Verarbeitung entweder ausschließlich innerhalb der EU bzw. des EWR durchzuführen oder diese teilweise oder zur Gänze unter Berücksichtigung der dafür anwendbaren Rechtsgrundlagen auch in vom AG zu benennenden Drittländern oder an bestimmten vom AG zu benennenden spezifischen Standorten durchzuführen. Die Laufzeit der Auftragsverarbeitung richtet sich nach der Laufzeit der Verträge zwischen AG und AN.

2. Anwendungsbereich und Verantwortlichkeit

1. Der AN ("Auftragsverarbeiter" gemäß Art. 4 Z. 8 DSGVO) verarbeitet Daten im Auftrag des AG. Dies umfasst jene Tätigkeiten, die in den Verträgen konkretisiert sind. Der AG ("Verantwortlicher" gemäß Art. 4 Z. 7 DSGVO) ist im Rahmen dieser Verträge für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Verarbeitung an sich sowie der Datenweitergabe an den AN als Auftragsverarbeiter allein verantwortlich.

2. Die Weisungen des AG werden durch die Verträge festgelegt und können vom AG in schriftlicher Form oder in einem dokumentierten elektronischen Format an den AN durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Etwaige mündliche Weisungen sind unverzüglich schriftlich in Textform zu bestätigen. Alle erteilten Weisungen sind vom AG zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Weisungen, die über die vertraglichen Vereinbarungen hinausgehen und auch nicht erforderlich sind, um Rechtsverstöße im Zuständigkeitsbereich des AN zu verhindern bzw. abzustellen, können kostenpflichtig sein.

3. Pflichten des AN als Auftragsverarbeiter

1. Der AN darf Daten nur im Rahmen der Verträge und gemäß den Weisungen des AG erheben, nutzen oder auf sonstige Weise verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der AN durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, es sei denn das anzuwendende Recht verbietet solche Benachrichtigungen.

2. Der AN informiert den AG unverzüglich, wenn er der der Auffassung ist, dass eine Weisung des AG gegen die DSGVO oder andere Datenschutzbestimmungen der Europäischen Union oder Mitgliedstaaten verstößt. Der AN ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis diese durch den AG bestätigt oder geändert wird. Der AN kann angemessene Sicherheiten verlangen, bevor er Weisungen ausführt, die nach objektiv nachvollziehbarer (nicht notwendig richtiger) Einschätzung des AN rechtswidrig sind und bei deren Umsetzung dem AN Schäden drohen.

3. Der AN wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des AG gemäß Art. 32 DSGVO, insbesondere die in ANHANG 1 aufgeführten Maßnahmen, zu ergreifen. Eine Änderung der getroffenen Maßnahmen ohne gesonderte Ankündigung bleibt dem AN vorbehalten, wobei das vertraglich vereinbarte Schutzniveau nicht unterschritten werden darf.

4. Den mit der Verarbeitung der Daten des AG befassten Personen des AN ist es untersagt, die Daten unbefugt zu verarbeiten. Der AN wird die vorgenannten Personen entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO). Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung der Mitarbeit beim bzw. des Tätigwerdens für den AN sowie nach Beendigung dieses Vertrages fortbestehen.

5. Der AN unterstützt den AG im Rahmen seiner Möglichkeiten bei der Erfüllung der Rechte betroffener Personen nach Kapitel III DSGVO. Darüberhinausgehend unterstützt der AN unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den AG bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten.

6. Der AN unterrichtet den AG unverzüglich, wenn ihm Verletzungen des Schutzes der Daten des AG bekannt werden. Der AN trifft in solchen Fällen die erforderlichen Maßnahmen zur Sicherung der Daten (entsprechend der Weisung des AG) zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und spricht sich hierzu unverzüglich mit dem AG ab.

7. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der AN die datenschutzkonforme Vernichtung von jeglichen betroffenen Datenträgern und sonstigen Materialien aufgrund einer Einzelweisung durch den AG oder gibt diese Datenträger an den AG zurück, sofern nicht anders im Vertrag vereinbart.

8. In besonderen, vom AG zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe an vom AG zu bestimmende Dritte, wobei Vergütung und Schutzmaßnahmen hierzu gesondert zu vereinbaren sind, sofern nicht bereits in den Verträgen geregelt.

9. Der AN wird nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des AG entweder löschen oder zurückgeben und die vorhandenen Kopien löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht oder die personenbezogenen Daten noch in etwaigen Backups des AN enthalten sind. Die personenbezogenen Daten in etwaigen Backups werden nach maximal 14 Tagen gelöscht.

10. Im Falle einer Inanspruchnahme des AG durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art 82 DSGVO, verpflichtet sich der AN, den AG bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten bestens zu unterstützen.

4. Pflichten des AG als Verantwortlicher

1. Der AG als Verantwortlicher stellt sicher, dass die Verarbeitung gemäß den Grundsätzen nach Kapitel II DSGVO erfolgt und die vom AN als Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen (**ANHANG 1**) und jene in den Verträgen gegebenenfalls darüberhinausgehend festgelegten Maßnahmen unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen ein angemessenes Schutzniveau bieten.

2. Der AG hat den AN unverzüglich und vollständig zu informieren, wenn er in den Auftragsverarbeitungsergebnissen Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

3. Im Falle einer Inanspruchnahme des AN durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art 82 DSGVO gilt Punkt 3.10. sinngemäß.

5. Datenschutzbeauftragter und Kontakt

1. Die Kontaktdaten des Datenschutzbeauftragten des AN werden jeweils aktuell auf der Homepage des AN veröffentlicht.

2. Der AG nennt dem AN einen oder mehrere Ansprechpartner für alle im Rahmen der Verträge inklusive der gegenständlichen Vereinbarung anfallenden Datenschutzfragen:

Vorname	Nachname	E-Mail	Telefon

6. Anfragen betroffener Personen

1. Wendet sich eine betroffene Person mit Forderungen nach Kapitel III DSGVO (z. B. Berichtigung, Löschung oder Auskunft) an den AN, wird dieser die betroffene Person an den AG verweisen, sofern eine Zuordnung zum AG nach Angaben der betroffenen Person möglich ist.

2. Der AN haftet nicht, wenn das Ersuchen der betroffenen Person vom AG nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

7. Nachweismöglichkeiten und Inspektionsrechte

1. Der AN stellt dem AG auf Anforderung innerhalb einer angemessenen Frist alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten des AN erforderlich sind. Hierzu kann der AN insbesondere Zertifizierungen des AN und gegebenenfalls weiterer Anexia-Unternehmen sowie von Subunternehmern außerhalb der Anexia-Unternehmensgruppe in den Bereichen ISO 9001 (Qualitätsmanagement) und/oder ISO 27001 (Informationssicherheit) und/oder ISO 27701 (Datenschutz) vorlegen. Der AN behält sich das Recht vor, bestimmte Unterlagen nur nach vorheriger Unterzeichnung einer entsprechenden Geheimhaltungsvereinbarung (NDA) vorzulegen, soweit diese vertrauliche Informationen des AN betreffen.

2. Der AN wird Überprüfungen - einschließlich Inspektionen -, die vom AG oder einem anderen von diesem beauftragten Prüfer, sofern dieser nicht in einem unmittelbaren Wettbewerbsverhältnis mit dem AN steht, durchgeführt werden, ermöglichen und dazu beitragen. Der AG wird Kontrollen nur im erforderlichen Umfang durchführen und diese dürfen nicht zu einer übermäßigen Beeinträchtigung des Geschäftsablaufs des AN führen. Kontrollen können in der Regel nur nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt werden, sofern nicht eine Kontrolle ohne vorherige Anmeldung erforderlich erscheint, weil andernfalls der Kontrollzweck gefährdet wäre.

3. Soweit die Kontrolle nicht wegen eines Gesetzes- oder Vertragsverstoß durch den AN erforderlich wurde, trägt der AG die Kosten der Kontrolle einschließlich des dem AN im Rahmen der Kontrolle entstehenden Aufwandes.

8. Weitere Auftragsverarbeiter

1. Der AG erteilt hiermit seine Zustimmung, dass die vertraglich vereinbarten Leistungen bzw. die in **ANHANG 2** beschriebenen Teilleistungen unter Einschaltung der dort genannten weiteren Auftragsverarbeiter („Subunternehmer“) durchgeführt werden.

2. Etwaige Regelung zu Subunternehmern in Angeboten oder Verträgen zwischen AG und AN gelten als Zustimmung des AG hinsichtlich der Einschaltung dieser Subunternehmer.

3. Der AN ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Vor der Begründung von weiteren Unterauftragsverhältnissen informiert der AN den AG in Textform. Der AG kann gegen die Änderung aus sachlichem Grund innerhalb von 14 Kalendertagen Einspruch erheben. Ein Subunternehmerverhältnis mit einem weiteren Auftragsverarbeiter liegt vor, wenn der AN weitere Unternehmen mit der ganzen oder einer Teilleistung der in den Verträgen zwischen AG und AN vereinbarten Leistung beauftragt und dabei die Kerntätigkeit in der Verarbeitung personenbezogener Daten des AG als Verantwortlichen besteht. Um kein Subunternehmerverhältnis handelt es sich bei der bloßen Erbringung von untergeordneten Nebenleistungen, bei denen die Kerntätigkeit nicht in der Auftragsverarbeitung personenbezogener Daten liegt (z. B. reine Infrastrukturbereitstellung, Telekommunikations-, Post- oder Reinigungsdienstleistungen, Wachschutz).

4. Nimmt der AN die Dienste eines Subunternehmers in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des AG auszuführen, so ist der AN verpflichtet, alle gesetzlichen und vertraglichen Datenschutzverpflichtungen, denen er gegenüber dem AG unterliegt, an diese weiteren Auftragsverarbeiter vollinhaltlich zu überbinden, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

9. Informationspflichten, Schriftform, Salvatorische Klausel und Rechtswahl

1. Sollten die Daten des AG beim AN durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der AN den AG unverzüglich darüber zu informieren. Der AN wird alle in diesem Zusammenhang Agierenden unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim AG als Verantwortlichem im Sinne der DSGVO liegen.

2. Änderungen und Ergänzungen dieser Vereinbarung und all ihrer Bestandteile bedürfen der Schriftform oder eines dokumentierten elektronischen Formats. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

3. Bei etwaigen datenschutzrechtlichen Widersprüchen oder Unschärfen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen der Verträge vor. Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nichtberührt.

4. Es gilt deutsches Recht.

10. Haftung und Schadenersatz

Der AG verpflichtet sich, den AN von jeglichen Ansprüchen Dritter mit oder im Zusammenhang einer vom AG verschuldeten Verletzung von datenschutzrechtlichen Vorschriften schad- und klaglos zu halten. Ansonsten gilt Art. 82 DSGVO.

11. Vertraulichkeit und Verschwiegenheit

Beide Parteien verpflichten sich zur grundsätzlichen Vertraulichkeit und zur Verschwiegenheit bezüglich der Inhalte dieser Vereinbarung. Davon ausgenommen sind gesetzliche Offenlegungspflichten gegenüber Behörden, in Gerichts- oder Strafverfahren sowie vertragliche Verpflichtungen gegenüber Personen und Auditoren sowohl des AG als auch des AN, die sich zur Vertraulichkeit gegenüber dem AG bzw. dem AN verpflichten oder einer berufsrechtlichen oder Verschwiegenheitsverpflichtung unterliegen, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist, und letztlich auch weitere Auftragsverarbeiter und verbundene Unternehmen, für die die gegenständlichen Festlegungen einen integralen Bestandteil im Rahmen ihrer Tätigkeitserfüllung darstellen.

Auftraggeber	Auftragnehmer
	Karlsruhe, 19.07.2025
Ort, Datum	Ort, Datum
	netcup GmbH Daimlerstraße 25, D-76185 Karlsruhe Tel: +49-721-7540755-0 / Fax: +49-721-7540755-9 mail@netcup.de / UID: DE262851304
	Oliver Werner
Unterschrift	Unterschrift

Anlagen

☑ ANHANG 1 - Technische und organisatorische Maßnahmen (TOM)

☑ ANHANG 2 - Weitere Auftragsverarbeiter

☑ ANHANG 3 - Auftragsverarbeitungsspezifikationen (optional)

AVV ANHANG 1

Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage (ANHANG 1)

Das gegenständliche Dokument ergänzt das Kapitel 11 der zwischen AG und AN abgeschlossenen Auftragsverarbeitungsvereinbarung (AVV) gemäß Art 28 DSGVO (EU-Datenschutzgrundverordnung). Die technischen und organisatorischen Maßnahmen werden vom AN und Anexia entsprechend Art 32 DSGVO umgesetzt. Sie werden laufend nach Machbarkeit und Stand der Technik - nicht zuletzt auch im Sinne der aktiven ISO 27001 Zertifizierung - verbessert und auf ein höheres Sicherheits- und Schutzniveau gebracht.

1. Vertraulichkeit

1. **Zutrittskontrolle**

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

1. **Bürostandort Karlsruhe**

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Alarmanlage	☑ Schlüsselregelung / Liste
☑ Manuelles Schließsystem	☑ Besucherbuch / Protokoll der Besucher
☑ Türen mit Knauf Außenseite	☑ Mitarbeiter- / Besucherausweise
	☑ Besucher in Begleitung durch Mitarbeiter
	☑ Sorgfalt bei Auswahl von Reinigungsdiensten

2. **Rechenzentrumsstandort Nürnberg**

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Alarmanlage	☑ Schlüsselregelung / Liste
☑ Chipkarten / Transpondersysteme	☑ Mitarbeiter- / Besucherausweise
☑ Türen mit Knauf Außenseite	☑ Besucher in Begleitung durch Mitarbeiter
☑ Klingelanlage mit Kamera	☑ Sorgfalt bei Auswahl Reinigungsdienste
☑ Videoüberwachung	

3. **Rechenzentrumsstandort Wien**

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Alarmanlage	☑ Schlüsselregelung / Liste
☑ Biometrische Zutrittskontrolle	☑ Protokoll der Besucher
☑ Chipkarten / Transpondersysteme	☑ Mitarbeiter- / Besucherausweise
☑ Türen mit Knauf Außenseite	☑ Besucher in Begleitung durch Mitarbeiter
☑ Videoüberwachung der Eingänge	☑ Sorgfalt bei Auswahl Reinigungsdienste

2. **Zugangskontrolle**

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

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Login mit Benutzername + Starkes Passwort	☑ Verwalten von Benutzerberechtigungen
☑ Anti-Viren-Software Server	☑ Zentrales Erstellen von Benutzerprofilen
☑ Anti-Virus-Software Clients	☑ Passwortgeschützte Useraccounts
☑ Firewall	☑ Anwendung von Sicherheitsmaßnahmen für Telearbeit nach Stand der Technik
☑ IDS im Einsatz (Intrusion Detection Systeme)	☑ Eingeschränkte Nutzung von administrativen Useraccounts
☑ IPS im Einsatz (Intrusion Prevention Systeme)	
☑ Einsatz VPN bei Remote-Zugriffen	
☑ Verschlüsselung Smartphones	
☑ Automatische Desktopsperre	
☑ Verschlüsselung von Festplatten bei Notebooks / Tablets / Smartphones	
☑ Zwei-Faktor-Authentifizierung im RZ-Betrieb und bei kritischen Systemen	

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
☑ Aktenshredder mind. empfohlene Sicherheitsstufe P-4 (DIN 66399)	☑ Einsatz Berechtigungskonzepte
☑ Physische Löschung von Datenträgern Sicherheitsstufe H-4 (DIN66399)	☑ Minimale Anzahl an Administratoren
☑ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☑ Verwaltung Benutzerrechte durch Administratoren
☑ Zugriffe auf Systeme mittels SSH	☑ Anwendung kryptografischer Verfahren nach aktuellem Stand der Technik
☑ TLS-Verschlüsselung	

4. **Trennungskontrolle**

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Trennung von Produktiv- und Testumgebung	☑ Festlegung von Datenbankrechten
☑ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☑ Definierte Anforderungen für Entwicklungsumgebungen
☑ Mandantenfähigkeit relevanter Anwendungen	
☑ VLAN-Segmentierung von Netzwerken	
☑ Kundensysteme logisch getrennt	
☑ Staging von Entwicklungs-, Test und Produktivumgebung	

2. Integrität

1. **Weitergabekontrolle und Eingabekontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder bzw. Eingabe 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	☑ Umsetzung des Need-to-know Prinzips
☑ Protokollierung der Zugriffe und Abrufe	
☑ Bereitstellung über verschlüsselte Verbindungen wie sftp, https – Secure Cloudstores	
☑ Technische Protokollierung von Eingabe, Änderung und Löschung von Daten	

3. Verfügbarkeit und Belastbarkeit

1. **Verfügbarkeitskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (USV, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.).

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Feuer- und Rauchmeldeanlagen	☑ Bestehende Notfallvorsorgeplanung
☑ Feuerlöscher Serverraum	☑ Regelmäßige Tests der Dieselaggregate RZ
☑ Serverraumüberwachung Temperatur und Feuchtigkeit	
☑ Serverraum klimatisiert	
☑ USV-Anlage und Notstrom-Dieselaggregate RZ	
☑ Schutzsteckdosenleisten Serverraum	
☑ RAID-System / Festplattenspiegelung	
☑ Videoüberwachung Serverraum	
☑ Einsatz von Schutzprogrammen gegen Schadsoftware	

2. **Wiederherstellbarkeit**

Maßnahmen, die dazu befähigen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Backup-Monitoring und -Reporting	☑ Recovery-Konzept
☑ Wiederherstellbarkeit aus Automatisierungs-Tools	☑ Kontrolle des Sicherungsvorgangs
☑ Backup-Konzept nach Kritikalität und Kundenvorgaben	☑ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
	☑ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. **Datenschutzmanagement**

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Zentrale Dokumentation aller Regelungen zum Datenschutz mit technischer Zugriffsmöglichkeit für Mitarbeiter	☑ Datenschutzmanagementsystem implementiert
☑ Jährliche Überprüfung der Angemessenheit der TOM	☑ Informationssicherheitsmanagement implementiert

2. **Incident-Response-Management**

Unterstützung bei der Reaktion auf Sicherheitsverletzungen sowie Data Breach Prozess.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Einsatz von Firewall und regelmäßige Aktualisierung	☑ Dokumentierte Vorgehensweise zum Umgang mit Sicherheits- und Datenschutzvorfällen
☑ Einsatz von Spamfilter und regelmäßige Aktualisierung	☑ Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem
☑ Einsatz von Virenscanner und regelmäßige Aktualisierung	
☑ Intrusion Detection System (IDS) für Kundensysteme auf Bestellung	
☑ Intrusion Prevention System (IPS) für Kundensysteme auf Bestellung	

3. **Datenschutzfreundliche Voreinstellungen**

"Privacy by design" / "Privacy by default" gem. Art 25 Abs 2 DSGVO.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Berücksichtigung der Grundsätze "Datenschutz durch Technikgestaltung" ("Data Protection by Design") und "Datenschutz durch datenschutzfreundliche Voreinstellungen" ("Data Protection by Default") bei der Softwareentwicklung	

4. **Auftragskontrolle (Outsourcing, Subauftragnehmer und Auftragsverarbeitung)**

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

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Überwachung von Remote-Zugriffen Externer z. B. im Rahmen von Remote-Support	☑ Lieferantenbewertungen werden risikobasiert durchgeführt
☑ Überwachung von Subunternehmern nach den Prinzipien und mit den Technologien gem. vorausgehenden Kapiteln 1, 2	☑ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☑ Auswahl des Auftragnehmers auf Basis definierter Kriterien
	☑ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung
	☑ Rahmenvereinbarung zur Auftragsverarbeitung innerhalb der Unternehmensgruppe
	☑ Regelmäßige Überprüfung des Auftragnehmers und seines Schutzniveaus

5. Technische und organisatorische Maßnahmen Infrastruktur bereitstellender Subunternehmer

Als Subunternehmer im betrieblichen und betriebswirtschaftlichen Sinn werden vom AN Colocation Rechenzentrumsdienstleister in Anspruch genommen. Es handelt sich hierbei nicht um "weitere Auftragsverarbeiter" gem. DSGVO, da deren Kerntätigkeit zu keinem Zeitpunkt in der Verarbeitung personenbezogener Daten liegt, sondern um eine sogenannte untergeordnete Nebenleistung in Form von Infrastrukturbereitstellung. Aufgrund der informationssicherheitstechnischen Relevanz für den AN sowie für den AG - vor allem betreffend die Verfügbarkeit - werden vom AN für diese Nebentätigkeiten ausschließlich sorgfältig ausgewählte Betriebe eingesetzt und regelmäßig überprüft.

6. Zertifizierungen

Sowohl das **Qualitätsmanagementsystem nach ISO 9001** als auch das **Informationssicherheitsmanagementsystem nach ISO 27001 der netcup GmbH** sowie wesentlicher Teile der Anexia-Unternehmensgruppe inkl. DATASIX Rechenzentrumsbetrieb sind durch die unabhängige TÜV NORD CERT GmbH zertifiziert. Zudem ist das **Datenschutzmanagementsystem nach ISO 27701 der netcup GmbH** sowie wesentlicher Teile der Anexia-Unternehmensgruppe inkl. DATASIX Rechenzentrumsbetrieb sind durch die unabhängige CIS - Certification & Information Security Services GmbH zertifiziert.

AVV ANHANG 2

☑ **ANX Holding GmbH**, Feldkirchner Straße 140, 9020 Klagenfurt, Österreich; **Auftragsinhalt**: Erbringung von Unterstützungsleistungen in diversen Bereichen (bspw. bei regulatorischen Anfragen, Abrechnung etc.)

☑ **ANEXIA Internetdienstleistungs GmbH**, Feldkirchner Straße 140, 9020 Klagenfurt, Österreich; **Auftragsinhalt**: Bereitstellung von Infrastrukturleistungen im Rechenzentrumsumfeld sowie Bereitstellung von Personal

☑ **ANEXIA Deutschland GmbH**, Daimlerstraße 25, 76185 Karlsruhe, Deutschland; **Auftragsinhalt**: Bereitstellung von Infrastrukturleistungen im Rechenzentrumsumfeld sowie Bereitstellung von Personal

AVV ANHANG 3 (optional)

Auftragsverarbeitungsspezifikationen

1. Gegenstand (Art und Zweck) der Verarbeitung

☑ Die Auftragsverarbeitung hat den folgenden konkreten Gegenstand:

---

2. Dauer der Verarbeitung

☑ Die Dauer der Auftragsverarbeitung durch den AN für den AG als Verantwortlichen richtet sich nach der Auftragsdauer, die sich **aus den Verträgen** zwischen den Parteien ergibt.

3. Ort der Verarbeitung

☑ Der Ort der Auftragsverarbeitung durch den AN für den AG als Verantwortlichen ergibt sich konkret aus den **bestehenden Verträgen** zwischen den Parteien.

4. Kategorien betroffener Personen

☑ Es werden Daten der **folgenden Personenkategorien** verarbeitet:

- ☑ Kunden
- ☑ Interessenten
- ☑ Lieferanten
- ☑ Besucher der Website
- ☑ Mitarbeiter des AG
- ☑ Externe Mitarbeiter
- ☑ Auftragsverarbeiter
- ☑ Newsletter-Abonnenten

☐ Weitere Daten (Eine pro Zeile)

---

5. Kategorien personenbezogener Daten

☑ Es werden Daten der **folgenden Kategorien personenbezogener Daten** verarbeitet:

- ☑ Namensdaten
- ☑ Geburtsdatum
- ☑ Bank- und Zahlungsdaten
- ☑ Standort und Geoinformationsdaten
- ☑ Bildungsdaten
- ☑ Verkehrsdaten
- ☑ Strafrechtsrelevante Daten
- ☑ Kontakt- und Adressdaten
- ☑ Kundenvertragsdaten
- ☑ Logindaten
- ☑ Daten zu Vorlieben und Verhaltensweisen
- ☑ Bewegungsprofildaten
- ☑ Foto- und Videodaten

☐ Weitere Daten (Eine pro Zeile)

---

und/oder

☐ Es werden **keine besonderen Kategorien personenbezogener Daten** („sensible Daten") verarbeitet.

oder

☑ Es werden die **folgenden besonderen Kategorien personenbezogener Daten** („sensible Daten”) verarbeitet:

- ☑ Rassische und ethnische Herkunft
- ☑ Politische Meinungen
- ☑ Religiöse oder weltanschauliche Überzeugungen
- ☑ Gewerkschaftszugehörigkeit
- ☑ Genetischen Daten
- ☑ Gesundheitsdaten
- ☑ Biometrischen Daten
- ☑ Sexualleben oder sexuelle Orientierung