Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 EU - DSGVO

[redacted]

zwischen

Michael Leuker
Stresemannstraße 44
40210 Düsseldorf

- 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 verarbeiten. 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 Mitarbeiter von Anexia sowie im Bedarfsfall durch Nutzung von Infrastrukturen und Systemen von Anexia durchgeführt werden. Die aktiven Zertifizierungen von Anexia in den Bereichen ISO 9001 (Qualitätsmanagement), ISO 27001 (Informationssicherheit) und weitere sind jeweils aktuell auf der Unternehmenshomepage von Anexia 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 ergeben sich aus den Verträgen zwischen den Parteien oder werden im optionalen **ANHANG 3** gesondert vom AG angegeben. Unter Anwendung der DSGVO obliegt es dem AG als Verantwortlichen, ein Verzeichnis von Verarbeitungstätigkeiten nach Art 30 Abs 1 DSGVO zu führen. Diese Verpflichtung entfällt, wenn für den AG die Ausnahmeregelung nach Art 30 Abs 5 DSGVO zutrifft. Davon unberührt obliegt es dem AN als Auftragsverarbeiter nach Art 30 Abs 2 DSGVO, ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung zu führen, welche sich auch aus **ANHANG 3** sowie aus dem Kontext der Verträge ergeben.

2. Über den Ort der Verarbeitung unter Berücksichtigung des Kapitels V DSGVO entscheidet ausschließlich der AG als Verantwortlicher. Er 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.

3. Die Laufzeit der Auftragsverarbeitung richtet sich nach der Laufzeit der Verträge und den darin vereinbarten Bestimmungen zwischen AG und AN, sofern sich aus den Bestimmungen dieser Vereinbarung oder aufgrund gesetzlicher Bestimmungen nicht darüberhinausgehende Verpflichtungen ergeben.

2. Anwendungsbereich und Verantwortlichkeit

1. Der AN ("Auftragsverarbeiter" gemäß Art 4 DSGVO) verarbeitet Daten im Auftrag des AG. Dies umfasst jene Tätigkeiten, die in den Verträgen konkretisiert sind. Der AG ("Verantwortlicher" gemäß Art 4 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 (auch elektronische Textform) an den AN durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Etwaige mündliche Weisungen sind unverzüglich schriftlich in Textform zu bestätigen.

3. Pflichten des AN als Auftragsverarbeiter

1. Der AN verpflichtet sich, Daten und Verarbeitungsergebnisse nur im Rahmen des Auftrages gemäß Vertrag und der Weisungen des AG zu verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Art 28 Abs 3 lit a DSGVO vor. Der AN informiert den AG unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der AN darf die Umsetzung dieser Weisung dann solange aussetzen, bis dies vom AG widerlegt oder die Weisung entsprechend gesetzeskonform abgeändert wurde.

2. Der AN verpflichtet sich zur Sicherheit der Verarbeitung nach Art 32 Abs 1 lit a bis c DSGVO als Auftragsverarbeiter unter Berücksichtigung der Machbarkeit im Rahmen der gültigen Verträge mit dem AG und gewährleistet nach Art 32 Abs 1 lit d DSGVO ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen einzusetzen. Dieses Verfahren ist unter anderem durch die erfolgreichen, wiederkehrenden Zertifizierungen von Anexia nach ISO 9001 und ISO 27001 gewährleistet und wird dem AG gemäß Kapitel 7 nachgewiesen. Einzelheiten zu den vom AN nach Art 32 DSGVO getroffenen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sind in **ANHANG 1** angeführt.

3. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem AN ohne gesonderte Ankündigung dann vorbehalten, wenn das vertraglich vereinbarte Schutzniveau dadurch nicht unterschritten wird und sie nicht der DSGVO widersprechen. Im Standardfall handelt es sich dabei um Verbesserungen der Datensicherheit durch Maßnahmen im Sinne von Informationssicherheit, Datenschutz und Qualitätsmanagement.

4. Der AN hat in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der AN und Anexia treffen technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des AG, die den Anforderungen des Art 32 DSGVO genügen. Der AN und Anexia treffen hierbei insbesondere Maßnahmen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfte Wirksamkeit wird auf die aktiven Zertifizierungen des Qualitätsmanagementsystems nach ISO 9001 und des Informationssicherheitsmanagementsystems nach ISO 27001 wesentlicher Teile der der Anexia-Unternehmensgruppe durch anerkannte, DAkkS-akkreditierte Prüf- und Zertifizierungsstellen verwiesen, deren Zertifikate dem AG als Nachweis geeigneter Garantien bezüglich dieser Normen ausreichen. Diese Zertifikate werden dem AG auf Anfrage vorgelegt und sind auch auf der Unternehmenshomepage von Anexia veröffentlicht.

5. Der AN gewährleistet, dass es den mit der Verarbeitung der Daten des AG befassten Mitarbeitern und anderen für den AN tätigen Personen per Verpflichtung untersagt ist, die Daten unbefugt zu verarbeiten (Datengeheimnis entsprechend § 53 BDSG). Diese Verpflichtung besteht auch nach Beendigung der Mitarbeit beim AN sowie nach

Beendigung des Vertragsverhältnisses fort.

6. Der AN unterstützt den AG im Rahmen seiner Möglichkeiten bei der Erfüllung der Rechte betroffener Personen nach Kapitel III DSGVO. Darüberhinausgehend unterstützt der AN den AG bei der Einhaltung der in Art 32 bis 36 DSGVO genannten Pflichten des AG im Rahmen der technischen und organisatorischen Machbarkeit, soweit dies nicht in den Verträgen mit dem AG anders geregelt ist.

7. 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.

8. Der AN berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der AG dies anweist und dies vom Weisungsrahmen umfasst ist. 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. 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. Daten, Datenträger sowie sämtliche sonstigen Materialien werden vom AN nach Vertragsende auf Verlangen des AG analog Punkt 3.8 entweder herausgegeben oder gelöscht. Im Falle von Test- und Ausschussmaterialien ist eine Einzelweisung für die Löschung nicht erforderlich. Entstehen zusätzliche Kosten durch vom AG davon abweichende, marktunübliche und nicht aus geltendem Datenschutzrecht oder aus den Verträgen resultierende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der AG.

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 AG durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art 82 DSGVO gilt Punkt 3.10 sinngemäß.

5. Datenschutzbeauftragter und Kontakt

1. Allgemeine Datenschutzfragen des AG können jederzeit an die explizit hierfür eingerichtete Stelle bei Anexia per E-Mail an data-protection@anexia-it.com gestellt werden. Unabhängig von gesetzlichen Erfordernissen des AN hat die Anexia-Unternehmensgruppe einen gemeinsamen Datenschutzbeauftragten (Group Data Protection Officer, DPO)

benannt, der die Einhaltung der datenschutzrechtlichen Vorschriften bei Anexia und beim AN überwacht und für den AG als Hauptansprechpartner zu Datenschutzfragen im Zuge der Vertragserfüllung fungiert. Die Kontaktdaten des Group DPO werden jeweils aktuell auf der Homepage des AN sowie auf der Anexia-Unternehmenshomepage 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. der AN leitet den Antrag der betroffenen Person unverzüglich an den AG weiter. Der AN unterstützt den AG bei der Erfüllung von Betroffenenanfragen im Rahmen seiner Möglichkeiten und auf Weisung des AG, soweit in den Verträgen nicht anders vereinbart.

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 weist bei Bedarf seitens AG die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach. Dieser Nachweis erfolgt nach Maßgabe von Anexia und des AN in Abstimmung mit dem AG und kann unter anderem umfassen:
    1. Zertifikat zum Informationssicherheitsmanagementsystem nach ISO 27001
    2. Zertifikat zum Qualitätsmanagementsystem nach ISO 9001
    3. Datenschutzzertifizierungen bzw. Datenschutzgütesiegel soweit vorhanden
    4. Aktualisiertes Verzeichnis der technischen und organisatorischen Maßnahmen (**ANHANG 1**)
    5. Datenschutzrelevante interne Auditberichte bei erweitertem Bedarf soweit vorhanden

2. Der AG erklärt hiermit, dass ihm im Sinne seiner Kontroll- und Inspektionsrechte die aufrechte ISO 27001 Zertifizierung von Anexia durch unabhängige DAkkS-akkreditierte Prüf- und Zertifizierungsstellen sowie gegebenenfalls vorhandene Datenschutzzertifizierungen grundsätzlich Genüge tun. Darüberhinausgehend steht für den Bedarf nicht anlassbezogener Inspektionen durch den AG oder einen von diesem beauftragten Prüfer die Möglichkeit, nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit von mindestens vier Wochen an periodisch stattfindenden Führungen an ausgewählten Betriebs- und Rechenzentrumsstandorten des AN teilzunehmen, um sich von der Umsetzung der technischen und organisatorischen Sicherheitsmaßnahmen vor Ort selbst zu überzeugen.

3. Der AN darf sowohl anlassbezogene als auch nicht anlassbezogene Inspektionen von der vorherigen Anmeldung entsprechend Punkt 7.2 und von der Unterzeichnung einer Vertraulichkeits- und Geheimhaltungsvereinbarung (Non Disclosure Agreement, NDA) hinsichtlich firmeninterner Informationen des AN, der Daten anderer Kunden des AN und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den AG

beauftragte Prüfer in einem Wettbewerbsverhältnis zu Anexia stehen, hat der AN gegen diesen ein Einspruchsrecht. Der AG stimmt dann der Benennung eines unabhängigen externen Prüfers durch den AN zu, dessen Auditbericht und Ergebnisse dem AG zur Verfügung gestellt werden.

4. Der Aufwand einer nicht anlassbezogenen Routineinspektion gemäß Punkt 7.2 durch den AG ist grundsätzlich auf einen Termin pro Kalenderjahr begrenzt, sofern in den Verträgen nicht gesondert geregelt. Für die Unterstützung bei der Durchführung von darüberhinausgehenden, nicht anlassbezogenen Inspektionen ist eine entsprechende Vergütung zwischen den Parteien zu vereinbaren. In diesem Zusammenhang allenfalls weitergehende in der DSGVO zwingend vorgesehene Rechte gelten als vereinbart und gehen im Falle von Widersprüchen mit den Bestimmungen unter Punkt 7 vor.

5. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des AG eine anlassbezogene Inspektion vornehmen, so ist eine Unterzeichnung einer Vertraulichkeits- und Geheimhaltungsvereinbarung gemäß Punkt 7.3 dann nicht erforderlich, wenn diese Aufsichtsbehörde bereits einer berufsrechtlichen oder gesetzlichen Verschwiegenheitspflicht unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

8. Weitere Auftragsverarbeiter

1. Der AG erteilt hiermit seine Zustimmung zur Verarbeitung der Daten durch die in **ANHANG 2** (Auflistung verbundener Unternehmen der Anexia-Unternehmensgruppe) konkret festgelegten Unternehmen als weitere Auftragsverarbeiter, soweit dies für die Leistungserbringung gemäß Verträgen erforderlich ist. Der AN verpflichtet sich hierbei zur vollinhaltlichen Überbindung der gesetzlichen und aller vertraglichen Datenschutzverpflichtungen an diese unternehmensgruppeninternen weiteren Auftragsverarbeiter. Anexia hat hierfür "Corporate Binding Rules" in Form einer Rahmenvereinbarung zu Datenschutz und Auftragsverarbeitung als verbindliches schriftliches Rechtsinstrument, eine unternehmensgruppenweite und für alle Mitarbeiter und beauftragten Personen verbindliche Datenschutzrichtlinie sowie ein Datenschutzmanagementsystem (DSMS) etabliert.

2. Der Einsatz von Subunternehmern bzw. Subdienstleistern als weitere Auftragsverarbeiter ist nur zulässig, wenn der AG vorher schriftlich zugestimmt hat. Die Regelung zu Subunternehmern in Angeboten oder Verträgen zwischen AG und AN gilt vorrangig zu dieser Regelung und entspricht einer solchen schriftlichen Zustimmung des AG.

3. Neben der konkreten Festlegung von verbundenen Unternehmen der Anexia-Unternehmensgruppe gemäß Punkt 8.1 werden ebenfalls in **ANHANG 2** alle zustimmungspflichtigen Subunternehmen, die als weitere Auftragsverarbeiter für den AG fungieren, angeführt und gelten durch Abschluss der gegenständlichen Vereinbarung als schriftlich genehmigt.

4. Ein zustimmungspflichtiges Subunternehmerverhältnis als weiterer Auftragsverarbeiter nach Punkt 8.2 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 ein nicht zustimmungspflichtiges 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).

5. Erteilt der AN nach erfolgter schriftlicher Zustimmung des AG Aufträge an weitere Auftragsverarbeiter, so ist der AN verpflichtet, alle gesetzlichen und vertraglichen Datenschutzverpflichtungen, denen er gegenüber dem AG unterliegt, an diese weiteren Auftragsverarbeiter vollinhaltlich zu überbinden.

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 Ergänzungsvereinbarungen in Schriftform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung zu dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Schriftformerfordernis.
3. Bei etwaigen datenschutzrechtlichen Widersprüchen oder Unschärfen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen der Verträge vor. Sollten einzelne Teile dieses Dokuments unwirksam sein oder werden, so berührt dies die Wirksamkeit des Dokuments im Übrigen nicht.
4. Es gilt deutsches Recht.

10. Haftung und Schadenersatz

Der AG und der AN haften gegenüber betroffenen Personen datenschutzrechtlich entsprechend der in Art 82 DSGVO getroffenen Regelung. Jegliche nicht datenschutzrechtlichen bzw. darüberhinausgehenden oder individuellen Haftungs- und Schadenersatzregelungen sind ausschließlich in den Angeboten und Verträgen zwischen dem AG und dem AN zu vereinbaren.

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 Verschwiegenheitsverpflichtung gemäß Punkt 7.5 unterliegen und letztlich auch weitere Auftragsverarbeiter und verbundene Unternehmen, für die die gegenständlichen Festlegungen einen integralen Bestandteil im Rahmen ihrer Tätigkeitserfüllung darstellen.

Auftraggeber	Auftragnehmer
Düsseldorf, den 09.05.2023	Karlsruhe, 09.05.2023
Ort, Datum	Ort, Datum
[redacted]	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.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Alarmanlage	☑ Schlüsselregelung / Liste
☑ Automatisches Zugangskontrollsystem	☑ Empfang / Rezeption / Pförtner
☑ Chipkarten / Transpondersysteme	☑ Besucherbuch / Protokoll der Besucher
☑ Manuelles Schließsystem	☑ Besucher in Begleitung durch Mitarbeiter
☑ Türen mit Knauf Außenseite	☑ Sorgfalt bei Auswahl Reinigungsdienste
☑ Videoüberwachung der Eingänge	☑ Richtlinie Informationssicherheit
	☑ Arbeitsanweisung Betriebssicherheit
	☑ Arbeitsanweisung Zutrittssteuerung

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
☑ Firewall	☑ Erstellen von Benutzerprofilen
☑ Einsatz VPN bei Remote-Zugriffen	☑ Zentrale Passwortvergabe
☑ Verschlüsselung von Datenträgern	☑ Richtlinie Informationssicherheit
☑ Verschlüsselung Smartphones	☑ Arbeitsanweisung IT-Benutzerordnung
☑ Automatische Desktopsperre	☑ Arbeitsanweisung Betriebssicherheit
☑ Verschlüsselung von Notebooks / Tablet	☑ Arbeitsanweisung Zugangssteuerung
☑ Zwei-Faktor-Authentifizierung im RZ-Betrieb und bei kritischen Systemen	☑ Mobile Device Policy

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
☑ Externer Aktenvernichtung mind. Sicherheitsstufe P-6 (DIN 66399)	☑ Minimale Anzahl an Administratoren
☑ Physische Löschung von Datenträgern	☑ Verwaltung Benutzerrechte durch Administratoren
☑ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☑ Richtlinie Informationssicherheit
☑ Zugriffe SSH Verschlüsselt	☑ Arbeitsanweisung Kommunikationssicherheit
☑ Zertifizierte SSL Verschlüsselung	☑ Arbeitsanweisung Umgang mit Informationen und Werten

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	☑ Steuerung über Berechtigungskonzept
☑ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☑ Festlegung von Datenbankrechten
☑ Mandantenfähigkeit relevanter Anwendungen	☑ Richtlinie Informationssicherheit
☑ VLAN-Segmentierung	☑ Richtlinie Datenschutz
☑ Kundensysteme logisch getrennt	☑ Arbeitsanweisung Betriebssicherheit
☑ Staging von Entwicklungs-, Test und Produktivumgebung	☑ Arbeitsanweisung Sicherheit in der Softwareentwicklung

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
☑ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem System (verschlüsselt)	☑ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren
☑ Auf Wunsch des Kunden werden Logfiles pseudonymisiert	☑ Richtlinie Informationssicherheit

☑ Richtlinie Datenschutz

☑ Richtlinie Datenschutz

☑ Separate, explizite Arbeitsanweisung Kryptographie (dzt. in Ausarbeitung)

2. Integrität

1. **Weitergabekontrolle**

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

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Einsatz von VPN	☑ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☑ Protokollierung der Zugriffe und Abrufe	☑ Weitergabe in anonymisierter oder pseudonymisierter Form
☑ Bereitstellung über verschlüsselte Verbindungen wie sftp, https und Secure Cloudstores	☑ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☑ Nutzung von Signaturverfahren (fallabhängig)	☑ Persönliche Übergabe mit Protokoll
	☑ Richtlinie Informationssicherheit
	☑ Richtlinie Datenschutz

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. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☑ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☑ Manuelle oder automatisierte Kontrolle der Protokolle (nach strikten internen Vorgaben)	☑ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
	☑ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☑ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	☑ Klare Zuständigkeiten für Löschungen
	☑ Richtlinie Informationssicherheit
	☑ Arbeitsanweisung IT-Benutzerordnung

3. Verfügbarkeit und Belastbarkeit

1. **Verfügbarkeitskontrolle**

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

sind (USV, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.).

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Feuer- und Rauchmeldeanlagen	☑ Backup-Konzept
☑ Feuerlöscher Serverraum	☑ Keine sanitären Anschlüsse im Serverraum
☑ Serverraumüberwachung Temperatur und Feuchtigkeit	☑ Existenz eines Notfallplans
☑ Serverraum klimatisiert	☑ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☑ USV-Anlage und Notrom-Dieselaggregate RZ	☑ Getrennte Partitionen für Betriebssysteme und Daten, wo notwendig
☑ Schutzsteckdosenleisten Serverraum	☑ Richtlinie Informationssicherheit
☑ RAID System / Festplattenspiegelung	☑ Arbeitsanweisung Betriebssicherheit
☑ Videoüberwachung Serverraum	☑ Regelmäßige Tests der Dieselaggregate RZ
☑ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

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
	☑ Existenz eines Notfallplans
	☑ Richtlinie Informationssicherheit
	☑ Arbeitsanweisung Betriebssicherheit

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. **Datenschutzmanagement**

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Zentrale Dokumentation aller Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter	☑ Interner Datenschutzbeauftragter bestellt: Group Data Protection Officer, DPO
☑ Sicherheitszertifizierung nach ISO 27001	☑ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet

☑ Eine Überprüfung der Wirksamkeit der TOM wird mind. jährlich durchgeführt und TOMs aktualisiert

☑ Datenschutzprüfpunkte durchgängig in Tool-gestütztem Risk Assessment implementiert

☑ Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich

☑ Interner Informationssicherheits-Beauftragter bestellt: Group Information Security Officer, ISO

☑ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt

☑ Prozess betr. Informationspflichten nach Art. 13 und 14 DSGVO etabliert

☑ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

☑ Datenschutzbetrachtung im Rahmen des Corporate Risk Managements etabliert

☑ ISO 27001 Zertifizierung wesentlicher Unternehmensteile inkl. RZ-Betrieb und jährliche Überwachungsaudits

2. **Incident-Response-Management**

Unterstützung bei der Reaktion auf Sicherheitsverletzungen sowie Data Breach Prozess.

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Einsatz von Firewall und regelmäßige Aktualisierung	☑ Dokumentierter Prozess zur Erkennung und
☑ Einsatz von Spamfilter und regelmäßige Aktualisierung	☑ Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☑ Einsatz von Virenscanner und regelmäßige Aktualisierung	☑ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☑ Intrusion Detection System (IDS) für Kundensysteme auf Bestellung	☑ Einbindung von DPO und ISO in Sicherheitsvorfälle und Datenpannen
☑ Intrusion Prevention System (IPS) für Kundensysteme auf Bestellung	☑ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
	☑ Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem
	☑ Formaler Prozess zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
	☑ Richtlinie Informationssicherheit
	☑ Richtlinie Datenschutz
	☑ Arbeitsanweisung Betriebssicherheit
	☑ Arbeitsanweisung IT-Benutzerordnung

3. **Datenschutzfreundliche Voreinstellungen**

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

Technische Maßnahmen	Organisatorische Maßnahmen
☑ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☑ Richtline Datenschutz (inkludiert Prinzipien "Privacy by design / default")
☑ Anwendung datenschutzfreundlicher Voreinstellung in Standard- sowie Individualsoftware	☑ OWASP Secure Mobile Development Security Checks werden durchgeführt
	☑ Perimeteranalyse bei Webapplikationen

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	☑ Arbeitsanweisung Lieferantenmanagement und Lieferantenbewertung
☑ 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 unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)

☑ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln

☑ Rahmenvereinbarung zur Auftragsverarbeitung innerhalb der Unternehmensgruppe

☑ Schriftliche Weisungen an den Auftragnehmer

☑ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis

☑ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer

☑ Regelung zum Einsatz weiterer Subunternehmer

☑ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

☑ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

5. Organisation und Datenschutz bei Anexia

Die Anexia Unternehmensgruppe hat sich in ihrer **strategischen Leitlinie Qualitäts-, Risiko- und Compliance-Politik** unter anderem zum Ziel gesetzt, ihren Kunden die zu liefernden Produkte und Services auf **höchstmöglichem Informationssicherheitsniveau rechtskonform** zur Verfügung zu stellen. Diese Leitlinie bildet den Rahmen für eine **transparente, nachhaltige, prozessbasierte und risikoorientierte Steuerung** der Unternehmensgruppe im Rahmen eines **Integrierten Management Systems (IMS)**. Anexia hat in diesem Zusammenhang eine ausgeprägte **Sicherheits-Querschnittsorganisation** etabliert, um einen umfassenden Schutz ihrer eigenen Unternehmensinformationen- und Daten sowie den Schutz der Daten ihrer Kunden und Auftraggeber zu gewährleisten. Dabei sind die Funktionen **Information Security Officer (ISO), Data Protection Officer (DPO), Quality Officer (QO), Risk Officer (RO)** sowie **Legal Compliance Officer (LCO)** mit gruppenweiter Verantwortung und direktem Weisungsrecht in diesen Wirkungsbereichen innerhalb der **direkt dem CEO zugeordneten Stabsabteilung "Quality, Risk & Compliance"** eingerichtet und ein umfassendes Regelwerk aus **internen Richtlinien und Regelungen ("Anexia Corporate Binding Rules"** u. a. zu Informationssicherheit und Datenschutz) etabliert, das für alle Mitarbeiter verbindlich einzuhalten ist und einen sicheren und datenschutzkonformen Umgang mit Informationen und Daten festlegt. Die **Mitarbeiter** werden laufend **auf dem Gebiet des Datenschutzes informiert und geschult**. Darüberhinausgehend sind alle Mitarbeiter dienstvertraglich zum **Datengeheimnis und zur Geheimhaltung verpflichtet**. **Externe**, die im Rahmen ihrer Tätigkeit für Anexia in Berührung mit personenbezogenen Daten kommen könnten, werden vor Beginn ihrer Tätigkeit zur Verschwiegenheit und Geheimhaltung sowie zur Einhaltung von Datenschutz und Datengeheimnis mittels einem sogenannten **NDA (Non-Disclosure-Agreement) verpflichtet**. Alle verbundenen Unternehmen der Anexia Unternehmensgruppe innerhalb der EU bzw. des EWR haben eine gemeinsame **Rahmenvereinbarung zu Datenschutz und Auftragsverarbeitung** als verbindliches schriftliches Rechtsinstrument gemäß Art 28 DSGVO abgeschlossen, um einen einheitlich hohen Datenschutz- und Datensicherheitsstandard über die gesamte Gruppe hinweg zu gewährleisten und die Rechte und Pflichten bei jeglichen Auftragsverarbeitungen klar zu regeln. Jegliche mit weiterer Auftragsverarbeitung betraute Subunternehmen werden erst nach Genehmigung des Verantwortlichen und nach Abschluss einer Auftragsverarbeitungsvereinbarung (AVV) nach Art 28

DSGVO eingesetzt, mit welcher ihnen alle datenschutzrechtlichen Pflichten, denen Anexia selbst unterliegt, vollinhaltlich überbunden werden. All diese organisatorischen Maßnahmen flankieren die jeweils aktuellen, **hohen technischen Sicherheitsstandards** von Anexia und beide Dimensionen werden **periodisch** im Zuge **interner Audits** sowie jährlich im Rahmen der **ISO 9001 und ISO 27001 Überwachungs- bzw. Re-Zertifizierungsaudits** von unabhängigen, externen, **DAkkS-akkreditierten Zertifizierungsstellen** auf ihre Angemessenheit und Wirksamkeit überprüft und bestätigt.

6. Zertifizierungen

Sowohl das **Qualitätsmanagementsystem nach ISO 9001** als auch das **Informationssicherheitsmanagementsystem nach ISO 27001** wesentlicher Teile von **Anexia inkl. DATASIX Rechenzentrumsbetrieb** sind durch die unabhängige TÜV NORD CERT GmbH **zertifiziert**.

Maßnahme	DSGVO-konform umgesetzt	Kommentare
Zutrittskontrolle	☑	ISO 27001 & ISO 9001 zertifiziert
Zugangskontrolle	☑	ISO 27001 & ISO 9001 zertifiziert
Zugriffskontrolle	☑	ISO 27001 & ISO 9001 zertifiziert
Weitergabekontrolle	☑	ISO 27001 & ISO 9001 zertifiziert
Eingabekontrolle	☑	ISO 27001 & ISO 9001 zertifiziert
Auftragskontrolle	☑	ISO 27001 & ISO 9001 zertifiziert
Verfügbarkeitskontrolle	☑	ISO 27001 & ISO 9001 zertifiziert
Trennungskontrolle	☑	ISO 27001 & ISO 9001 zertifiziert
Innerbetriebliche Organisation	☑	ISO 27001 & ISO 9001 zertifiziert

7. Technische und organisatorische Maßnahmen relevanter 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 und ISO 27001 zertifizierte Betriebe eingesetzt und regelmäßig dahingehend überprüft. **Hetzner Online**

RZ-Standort	Rechenzentrum Nürnberg, Sigmundstraße 135, DE-90431
Nürnberg Betreiber	Hetzner Online GmbH, Industriestraße 25, DE-91710
Gunzenhausen ISO 27001-Zertifikat	https://www.hetzner.com/pdf/FOX_Zertifikat.pdf
TOM	https://www.hetzner.com/AV/TOM.pdf

AVV ANHANG 2

Weitere Auftragsverarbeiter Anexia

Verbundene Unternehmen

Die folgenden verbundene Unternehmen (siehe Auswahl) im Geltungsbereich der "Anexia Corporate Rules zum Datenschutz" in Form einer Rahmenvereinbarung zu Datenschutz und Auftragsverarbeitung als verbindliches schriftliches Rechtsinstrument gem. Art 28 DSGVO und einer unternehmensgruppenweit gültigen Datenschutzrichtlinie sowie im Vollanwendungsbereich des Anexia Datenschutzmanagementsystems (DSMS) liegend innerhalb der Anexia-Unternehmensgruppe können - je nach Art und Umfang der Auftragsverarbeitung - als weitere Auftragsverarbeiter im Rahmen der Vertrags- und Auftragserfüllung zum Einsatz kommen. Für sie gelten jegliche Bestimmungen und Verpflichtungen der gegenständlichen Auftragsverarbeitungsvereinbarung (AVV) sinngemäß und vollinhaltlich. Konkrete Festlegung der tatsächlich für im Rahmen der gegenständlichen Auftragsverarbeitungsvereinbarung (AVV) als weiter Auftragsverarbeiter eingesetzten Unternehmen mittels Kontrollkästchenauswahl:

☑ ANX Holding GmbH, Klagenfurt, Österreich

☑ ANEXIA Internetdienstleistungs GmbH, Klagenfurt, Österreich

☑ ANEXIA Deutschland GmbH, München, Deutschland

☑ DATASIX Rechenzentrumsbetriebs GmbH, Wien, Österreich

Sonstige weitere Auftragsverarbeiter

Subunternehmen

Die folgenden Subunternehmen werden im Rahmen der Vertrags- bzw. Auftragserfüllung als sonstige weitere Auftragsverarbeiter eingesetzt. Sie unterliegen ausnahmslos denselben, sich aus der DSGVO und aus der gegenständlichen Vereinbarung ergebenden datenschutzrechtlichen Pflichten gegenüber dem Verantwortlichen und dem Auftragsverarbeiter, die ihnen mittels separater Verträge zur Auftragsverarbeitung als verbindliches schriftliches Rechtsinstrument gem. Art 28 DSGVO überbunden wurden:

☑ Derzeit keine sonstigen weiteren Auftragsverarbeiter

AVV ANHANG 3 (optional)

Auftragsverarbeitungsspezifikationen

1. Gegenstand (Art und Zweck) der Verarbeitung

entweder

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

oder

☑ Die Auftragsverarbeitung hat den folgenden konkreten Gegenstand:

Mitgliederverwaltung für und -aktionen über die Seite svm-fanforum.de

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 **und ist ausschließlich Deutschland**.

4. Kategorien betroffener Personen

entweder

☐ Die Kategorien der betroffenen Personen, deren Daten verarbeitet werden **ergeben sich aus den Verträgen** zwischen den Parteien **oder sind nur dem AG als Verantwortlichen bekannt** und dieser stellt dabei sicher, dass die Verarbeitung gemäß den Grundsätzen nach Kapitel II DSGVO erfolgt und die vom AN als Auftragsverarbeiter getroffenen technischen und organisatorischen 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 angemessen sind.

oder

☑ 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

entweder

☐ Die verarbeiteten Datenkategorien ergeben sich **im Detail aus den Verträgen** zwischen den Parteien **oder sind nur dem AG als Verantwortlichen bekannt** und dieser stellt dabei sicher, dass die Verarbeitung gemäß den Grundsätzen nach Kapitel II DSGVO erfolgt und die vom AN als Auftragsverarbeiter getroffenen technischen und organisatorischen 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 angemessen sind.

oder

☑ Es werden Daten der **folgenden Personenkategorien** 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
- ☐ Religiöse oder weltanschauliche Überzeugungen
- ☐ Genetischen Daten
- ☐ Biometrischen Daten
- ☐ Politische Meinungen
- ☐ Gewerkschaftszugehörigkeit
- ☐ Gesundheitsdaten
- ☐ Sexualleben oder sexuelle Orientierung