Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO

zwischen dem Verantwortlichen

_____

- nachstehend Auftraggeber genannt -

und dem Auftragsverarbeiter

amexus Informationstechnik GmbH & Co. KG
Von-Braun-Straße 34
48683 Ahaus

- nachstehend Auftragnehmer genannt-

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten („Daten") des Auftraggebers verarbeiten.
Die Vereinbarung gilt entsprechend für (Fern-) Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

1. Gegenstand und Dauer des Vertrags

(1) Gegenstand

☐ Der Gegenstand des Vertrags ergibt sich aus der Leistungsvereinbarung/ SLA/dem Auftrag vom , auf die/den hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

☒ Gegenstand des Vertrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Technischer Support, Auftragsabwicklung, IT-Dienstleistungen, Kundenservice, Cloud-Services.

(2) Dauer

☐ Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)

☐ Der Vertrag beinhaltet eine einmalige Ausführung.

oder

☐ Die Dauer dieses Vertrags (Laufzeit) ist befristet bis zum

oder

☒ Der Vertrag wird für unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von 4 Wochen gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

(3) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

(4) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

2. Konkretisierung des Vertragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der Leistungsvereinbarung vom [redacted] konkret beschrieben
oder

☒ Nähere Beschreibung des Vertragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: Technischer Support, Auftragsabwicklung, IT-Dienstleistungen, Kundenservice, Cloud-Services.

(2) Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter:
oder

☒ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien

Aufzählung/Beschreibung der Datenkategorien
☒ Personenstammdaten
☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
☒ Kundenhistorie
☒ Vertragsabrechnungs- und Zahlungsdaten
☒ Planungs- und Steuerungsdaten
☒ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
☐

(3) Kategorien betroffener Personen

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter:
oder

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

Kategorien betroffener Personen
☒ Kunden
☒ Interessenten
☒ Abonnenten
☒ Beschäftigte
☒ Lieferanten
☒ Handelsvertreter
☒ Ansprechpartner
☐

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gem. Art. 32 DSGVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung **[Anlage 1]**. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.

(2) Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzten.

4. Rechte von betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, 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.

(2) Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 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 berechtigterweise 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.

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

c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag 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.

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

e) 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.

f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.

g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33 und Art. 34 DSGVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zu Verfügung.

i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DSGVO.

6. Unterauftragsverhältnisse

(1) 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 in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. 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 zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☐ Der Auftraggeber stimmt der Beauftragung der in **Anhang 2** bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO mit dem Unterauftragnehmer zu.

Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

c) ☒ Die Auslagerung auf Unterauftragnehmer oder

☒ der Wechsel der gemäß Anhang 2 bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine

Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☒ ist nicht gestattet;

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Internationale Datentransfers

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DSGVO.

☒ 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.

☐ Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland. In der **Anlage 2** werden die Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DSGVO im Rahmen der Unterbeauftragung spezifiziert.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DSGVO verantwortlich.

8. Kontrollrechte des Auftraggebers

(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 während der üblichen Geschäftszeiten zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 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.

(3) Der Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch

☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 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).

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

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(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

(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 Aufbewahrungspflichtenerforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber 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. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Ansprechpartner des Auftraggebers:	
Datenschutzbeauftragter des Auftraggebers:	
Ansprechpartner des Auftragnehmers:	Stefan Nacke
Datenschutzbeauftragter des Auftragnehmers:	**Heiner Niehüser; hniehueser@dsb-ms.de**
, den	, den
Auftraggeber	*Auftragnehmer*

Allgemeine Beschreibung
der technischen und organisatorischen Maßnahmen
gemäß Art. 32 Abs. 2 DSGVO für Auftragsverarbeiter (Art. 30 Abs. 2 lit. d DSGVO)

amexus Informationstechnik GmbH & Co.KG
Von-Braun-Straße 34, Ahaus, 48683 Deutschland
- nachfolgend Auftragnehmer-

Der Auftragnehmer setzt, unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen folgende technische und organisatorische Maßnahmen um, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

Regelungsgegenstand:

Unbefugten ist der Zutritt zu den Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten), mit denen Daten im Auftrag verarbeitet werden, zu verwehren. Der Grad der Schutzmaßnahmen richtet sich dabei nach dem Grad der Schutzbedürftigkeit der Daten.

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung oder unrechtmäßiges oder fahrlässiges Handeln von im Auftrag verarbeiteten Daten ist zu reduzieren.

Technische und organisatorische Maßnahmen:

1	Zutrittskontrollmaßnahmen zu Büroräumen und Arbeitsplätzen
	Die Zutrittskontrollen zu den Standorten und zu den Gebäuden sind lückenlos.
	Alle Zutritte zu dem Gebäude werden im Empfangsbereich durch das zuständige Personal kontrolliert.
	Das Bürogebäude und seine Zugänge sind videoüberwacht.
	Das Gebäude und die Büroräume sind mit einem elektronischen Schließsystem versehen.
	Der Zutritt von Berechtigten wird durch Transponder (Chip/Karte) ermöglicht. Zutrittsrechte werden personifiziert vergeben.
	Alle Zutrittsversuche werden protokoliert.
	Das Gebäude / die Büroräume sind mit einem mechanischen Schließsystem versehen. Jede Schlüsselausgabe wird von der Ausgabestelle protokoliert.
	Betriebsfremde Personen (Fremdleister wie z. B. Techniker, Besucher) unterliegen der Besucherbegleitpflicht bzw. der Aufsichtspflicht durch die beauftragenden Fachabteilungen. Fremdleister werden in Sicherheitsbereichen grundsätzlich durch Mitarbeiter begleitet.
2	**Zutrittskontrollmaßnahmen zu Serverräumen**
	Die Server von amexus befinden sich an drei Standorten- in Ahaus (2 räumlich getrennte Standorte) und Oberhausen.
	Serverräume sind durch Stahltüre von dem restlichen Gebäudeteil getrennt. Sie sind entweder fensterlos oder mit Gitter an jedem Fenster versehen.
	Der Serverraum in Ahaus ist mittels einer Einbruchmeldeanlage (EMA) alarmgesichert. Bei jeder Auslösung der Alarmanlage wird der beauftragte Wachdienst sofort informiert
	Der Zutritt von Berechtigten wird durch Transponder (Chip/Karte) ermöglicht. Zutrittsrechte werden personifiziert vergeben und jeder Zutrittsversuch wird protokoliert.
	Die Serverräume werden über Videoanlagen mit Bildaufzeichnung überwacht.
	Der Serverraum bildet einen eigenen Sicherheitsbereich, daher haben nur die Geschäftsleitung und die Administratoren Zutritt zum Serverraum.

3	Zugangs- und Zugriffskontrollmaßnahmen
	Es existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen. Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Systeme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen. Die Erteilung oder Änderung der Berechtigungen erfolgt in einem dokumentierten Genehmigungsverfahren.
	Es gibt vorgeschriebene Regeln zur Passwortvergabe (Passwort-Richtlinie). Dies betrifft die notwendige Komplexität, die Lebensdauer des Passwortes sowie die Wiederverwendung alter Passwörter.
	Bei Verlust der Benutzerkennung erfolgt der Zugriff auf Systeme nur nach Vergabe eines neuen Initialpassworts durch den Administrator.
	Der Zugriff auf Firmensysteme wird nach 3 erfolglosen Anmeldeversuchen gesperrt.
	Fernzugänge werden mit Token und Passwort abgesichert. Der Zugriff wird nach 3 erfolglosen Anmeldeversuchen gesperrt.
	Eine automatische Bildschirmsperre erfolgt bei Inaktivität spätestens 5 Minuten nach der letzten Eingabe.
	Die Systeme, auf denen personenbezogene Daten verarbeitet werden, sind über eine Firewall abgesichert.
	Die Firewall wird regelmäßig upgedatet und von der eigenen IT-Abteilung administriert.
4	**Maßnahmen zur sicheren Datenübertragung**
	Der Transfer personenbezogener Daten erfolgt per verschlüsselter Datei per verschlüsseltem Datenträger per VPN und per https/TLS.
5	**Maßnahmen zur Sicherung von Unterlagen, mobilen Datenträgern und mobilen Endgeräten**
	Papier-Unterlagen mit personenbezogenen Daten (bspw. Ausdrucke / Akten / Schriftwechsel) werden datenschutzkonform entsorgt. Hierfür stehen Schredder nach Schutzklasse DIN 66399 und verschlossenen Datentonne zur Verfügung.
	Nicht mehr benötigte Datenträger (USB-Sticks, Festplatten), auf denen personenbezogene Daten gespeichert sind werden datenschutzkonform entsorgt. Hierfür wir ein externer Dienstleister mit der Zerstörung beauftragt.
	Mobile Datenträger und einzelne Verzeichnisse sowie mobile Endgeräte mit personenbezogenen Daten werden verschlüsselt.
	Mobile Datenträger und mobile Endgeräte werden grundsätzlich von amexus gestellt und konfiguriert. Die Geräte unterliegen einer zentralen Verwaltung.
	Die Nutzung privater Endgeräte (BYOD) ist ausschließlich in eingeschränktem Umfang gestattet. Der Zugriff auf Unternehmensdaten erfolgt dabei ausschließlich über freigegebene Software oder Apps. Auf privaten Endgeräten dürfen keine personenbezogenen Auftraggeberdaten lokal gespeichert werden.
	Der Einsatz von KI-basierten Werkzeugen und Diensten durch Mitarbeiter von amexus unterliegt einer internen Richtlinie. Die Verarbeitung personenbezogener Daten sowie vertraulicher Auftraggeberdaten über externe KI-Systeme (z. B. cloudbasierte Large Language Models) ist grundsätzlich untersagt, sofern diese nicht ausdrücklich durch die Geschäftsleitung freigegeben und datenschutzrechtlich geprüft worden sind. Werden KI-Dienste eingesetzt, werden die verarbeiteten Daten nicht für das Training, die Optimierung oder die Weiterentwicklung von KI-Modellen des jeweiligen Anbieters verwendet. Mitarbeiter sind angewiesen, keine personenbezogenen Daten, Betriebs- oder Geschäftsgeheimnisse sowie Auftraggeberdaten in öffentlich zugängliche KI-Systeme einzugeben.
6	**Maßnahmen zur Sicherung von Anwendungen und Applikationen**
	Für Anwendungen/Applikationen ist ein restriktives Berechtigungskonzept definiert und umgesetzt.

Maßnahmen zur Sicherstellung der Verfügbarkeit

Regelungsgegenstand:

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und

Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Nichtverfügbarkeit von im Auftrag verarbeiteten Daten ist zu reduzieren.

Technische und organisatorische Maßnahmen:

1	Serveraum
	Die Türen, Fenster und Wände der Serverräume weisen einen ausreichenden Einbruch-, Rauch- und Feuerschutz auf.
	Der Serverraum in Oberhausen ist mit Rauchmeldern ausgestattet.
	Der Serverraum in Oberhausen ist an eine Brandmeldezentrale angeschlossen.
	Der Serverraum in Oberhausen istmit einem Löschsystem ausgestattet.
	Die Serverräume sind klimatisiert.
	Die Serverräume verfügen über eine unterbrechungsfreie Stromversorgung (USV).
	Die Funktionalität der oben genannten Punkte wird regelmäßig getestet.
2	**Backup- und Notfall-Konzept, Virenschutz & Patchmanagement**
	Es existiert ein Backupkonzept.
	Die Funktionalität der Backup-Wiederherstellung wird regelmäßig getestet.
	Die Backups sind verschlüsselt. Sie werden auf einem zweiten Server sowie in einem feuerfesten datensicheren Safe auf Festplatten und Sicherungsbänder aufbewahrt. Der Transport von Backups ist nur durch die Administration gestattet.
	Es existiert ein dokumentierter Prozess zum Software- bzw. Patchmanagement. Hierfür ist die eigene IT- Abteilung des Unternehmens zuständig.
	Es existiert ein Notfallkonzept.
	Die IT-Systeme sind technisch vor Datenverlusten / unbefugten Datenzugriffen mittels stets aktualisiertem Virenschutz, Anti-Spyware und Spamfilter geschützt. Hierfür ist die eigene IT- Abteilung des Unternehmens verantwortlich
	Es existiert ein Backup für Anwendungen / Applikationen
	Es existiert ein Notfallkonzept für Anwendungen / Applikationen.
	Es existiert ein angemessener Prozess für Lizenzierung und Lizenzmanagement für die eingesetzten Softwareprodukte.
3	**Netzanbindung**
	Das Unternehmen verfügt über eine redundante Internetanbindung.
	Das Unternehmen verfügt über eine redundante Firewall. Beide Firewalls sind im ständigen Betrieb.
	Die einzelnen Standorte des Unternehmens sind redundant miteinander verbunden.

Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Regelungsgegenstand:
Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu betreiben.

Organisatorische Maßnahmen:

1	Datenschutz-Management
	Die Wirksamkeit der Maßnahmen wird im Rahmen der Umsetzung des Datenkonzeptes nach VDS 10010 Richtlinie durch den Datenschutzbeauftragten in regelmäßigen Abständen geprüft.
	Alle Mitarbeiter von amexus, die personenbezogenen Daten verarbeiten, sind auf Datengeheimnis verpflichtet.
	Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten.
	Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO).
	Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO).
	Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO).
	Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO).

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen behält sich das Unternehmen vor, sofern das geforderte Schutzniveau nicht unterschritten wird.

Ahaus, 02.04.2026

Ort, Datum

amexus® Informationstechnik 48683 Ahaus, Am Bruch Straße 34

Unterschrift der Geschäftsführung