Bestellschein Schulen - netzklasse

kuravisma netzklasse

Lizenznehmerdaten: Lizenznehmer: _____

Name: _____ Vorname: _____ Position: _____

Schulname: _____

Straße: _____

PLZ: _____ Ort: _____ Bundesland: _____

Festnetznummer: _____ E-Mail: _____

Bitte kreuzen Sie an, welche Laufzeit Sie verbindlich mit diesem Bestellschein buchen möchten:

☐ **1 Jahr** (1.100,-€ netto zzgl. gesetzl. Mehrwertsteuer pro Jahr)

☐ **2 Jahre** (1.000,-€ netto zzgl. gesetzl. Mehrwertsteuer pro Jahr)

Bitte kreuzen Sie an, welchen Support-Service Sie verbindlich mit diesem Bestellschein buchen möchten:

☐ **Basic Support (inklusive)**

☐ **1 Jahr Premium Support** (1.100,-€ netto zzgl. gesetzl. Mehrwertsteuer pro Jahr)

☐ **2 Jahre Premium Support** (1.000,-€ netto zzgl. gesetzl. Mehrwertsteuer pro Jahr)

☐ **Ich bestätige, dass ich die Vertragsbestandteile erhalten, gelesen, verstanden habe und Ihnen zustimme. Ich bestätige zur Unterschrift im Namen meiner Schule berechtigt zu sein.**

Ort, Datum: _____ Unterschrift: ✗ _____

Anlagen:

Anlage 1: Vertragsbedingungen
Anlage 2: Auftragsverarbeitungsvertrag
Anlage 3: Technische und organisatorische Maßnahmen
Anlage 4: Anhang 1 - Umfang und technische Voraussetzungen

Vertragsbedingungen für das virtuelle Klassenzimmer netzklasse:

§ 1 Leistungsumfang netzklasse

1. Der Lizenzgeber stellt dem Lizenznehmer die Software „netzklasse“ zur Verfügung. Die Software wird als webbasierte SaaS- bzw. Cloud-Lösung betrieben. Dem Lizenznehmer wird ermöglicht, die auf den Servern der Kuravisma GmbH gespeicherte und ablaufende Software über eine Internetverbindung während der Laufzeit dieses Vertrags für eigene Zwecke zu nutzen und seine Daten mit ihrer Hilfe zu speichern und zu verarbeiten. Diese Vertragsbedingungen gelten ausschließlich. Vertragsbedingungen des Kunden finden keine Anwendung. Gegenbestätigungen des Kunden unter Hinweis auf seine eigenen Geschäftsbedingungen wird ausdrücklich widersprochen.

2. Als „Cloud-Lösung“ wird netzklasse auf einem von der Kuravisma GmbH gestellten Server installiert und betrieben, wobei der Lizenznehmer außerhalb der Wartungszeiten zu mindestens 98% des Jahres die Möglichkeit hat, netzklasse mittels eines Internetbrowsers und einer Internetverbindung zu benutzen. Der Internetbrowser, die Hardware, auf der der Browser installiert und betrieben wird, sowie die Internetverbindung werden in Anhang 1 technisch beschrieben; der Lizenznehmer beschafft, installiert und betreibt diesen Browser (Soft- und Hardware) und diese Internetverbindung auf eigene Kosten und in eigener Verantwortung. „Wartungszeiten“ werden soweit technisch möglichst mindestens 1 Woche vorab mitgeteilt und finden zwischen 22:00h und 07:00h statt.

3. Die Funktionalität von netzklasse ergibt sich aus Anhang 1. Im Falle der Weiterentwicklung von netzklasse obliegt es dem Lizenznehmer, die in seinem Bereich notwendigen Anpassungen nach Vorgaben der Kuravisma GmbH vorzunehmen. Änderungen der Systemvoraussetzungen sind nur unter Beachtung einer angemessenen Ankündigungsfrist zulässig und nur, soweit sie dem Lizenznehmer zumutbar sind.

4. Der Lizenzgeber stellt dem Lizenznehmer die Software in ihrer jeweils aktuellsten Version am Routerausgang des Rechenzentrums, in dem der Server mit der Software steht („Übergabepunkt“), zur Nutzung bereit. Die Software, die für die Nutzung erforderliche Rechenleistung und der erforderliche Speicher- und Datenverarbeitungsplatz werden vom Lizenzgeber bereitgestellt. Der Lizenzgeber schuldet jedoch nicht die Herstellung und Aufrechterhaltung der Datenverbindung zwischen den IT-Systemen des Lizenznehmers und dem beschriebenen Übergabepunkt.

5. Der Lizenzgeber weist den Lizenznehmer darauf hin, dass Einschränkungen oder Beeinträchtigungen der erbrachten Dienste entstehen können, die außerhalb des Einflussbereichs des Lizenzgebers liegen. Hierunter fallen insbesondere Handlungen von Dritten, die nicht im Auftrag des Lizenzgebers handeln, vom Lizenzgeber nicht beeinflussbare technische Bedingungen des Internets sowie höhere Gewalt. Auch die vom Lizenznehmer genutzte Hard- und Software und technische Infrastruktur kann Einfluss auf die Leistungen des Lizenzgebers haben. Soweit derartige Umstände Einfluss auf die Verfügbarkeit oder Funktionalität der vom Lizenzgeber erbrachten Leistung haben, hat dies keine Auswirkung auf die Vertragsgemäßheit der erbrachten Leistungen. Der Lizenznehmer ist verpflichtet, Funktionsausfälle, -störungen oder -beeinträchtigungen der Software unverzüglich und so präzise wie möglich beim Lizenzgebers anzuzeigen. Unterlässt der Lizenznehmer diese Mitwirkung, gilt § 536c BGB entsprechend.

§ 2 Support und Updates

1. Der Lizenzgeber leistet während der Vertragslaufzeit Support für netzklasse („Support“). Dieser umfasst die Korrektur von Fehlern innerhalb eines dem Schweregrad des Fehlers angemessenen Zeitraums („3rd-Level Support“). Der Lizenzgeber wird Support nicht gegenüber den Endnutzern, sondern ausschließlich gegenüber dem Lizenznehmer leisten.

Im **Basic Support Paket** richtet der Lizenznehmer seine Anfragen per Email an support@netzklasse.com. Der Lizenzgeber wird diese Supportanfragen innerhalb seiner Geschäftszeiten (Montag-Freitag, 08.00h bis 18.00h) bearbeiten.

Im **Premium Support Paket** steht dem Lizenznehmer ein persönlicher Ansprechpartner per E-Mail, sowie telefonisch, zur Verfügung. Supportanfragen werden priorisiert behandelt.

2. Der Lizenzgeber wird dem Lizenznehmer während der Laufzeit dieses Vertrages alle Fehlerkorrekturen, Modifikationen und Weiterentwicklungen der lizensierten Software zur Verfügung stellen („Updates“). Dem Lizenzgeber bleibt vorbehalten, im Zuge dessen Funktionalitäten der Software aufzuheben, einzuschränken oder durch neue zu ersetzen, sofern berechtigte Interessen des Lizenznehmers nicht unzumutbar beeinträchtigt werden.

§ 3 Nutzungsrecht

1. Die netzklasse Software und die darin integrierten Datenbanken sind urheberrechtlich geschützt. Das Urheberrecht und das Datenbankherstellerrecht sowie alle davon abgeleiteten Nutzungs- und Leistungsschutzrechte stehen ausschließlich der Kuravisma GmbH als Hersteller zu. Soweit in der Software geschützte Leistungen anderer Anbieter enthalten sind, bleiben deren Rechte unberührt und es gelten die Lizenzbedingungen dieser dritten Partei.

2. Der Lizenzgeber gewährt dem Lizenznehmer im Wege der Software-Miete bzw. im Wege der zeitlich begrenzten Zurverfügungstellung als Software-as-a-Service ein nicht-ausschließliches, nicht-übertragbares und nicht-unterlizenzierbares Recht zur Nutzung von netzklasse im Object Code während der Vertragsdauer durch Angestellte („Lizenz“). Die Lizenz erstreckt sich auf alle Updates.

3. Die Lizenz endet mit Beendigung dieses Vertrags automatisch, ohne dass es einer zusätzlichen Rechtshandlung bedarf.

§ 4 Daten / Recht zur Datenverarbeitung

1. Der Lizenzgeber hält sich an die gesetzlichen Datenschutzbestimmungen.

2. Der Lizenznehmer räumt dem Lizenzgeber für die Zwecke der Vertragsdurchführung das Recht ein, die vom Lizenzgeber für den Lizennehmer zu speichernden Daten vervielfältigen zu dürfen, soweit dies zur Erbringung der nach diesem Vertrag geschuldeten Leistungen erforderlich ist. Der Lizenzgeber ist auch berechtigt, die Daten in einem Ausfallsystem bzw. separaten Ausfallrechenzentrum vorzuhalten. Zur Beseitigung von Störungen ist der Lizenzgeber ferner berechtigt, Änderungen an der Struktur der Daten oder dem Datenformat vorzunehmen.

3. Der Lizenzgeber sichert die Daten des Lizenznehmers auf dem vom Lizenzgeber verantworteten Server regelmäßig auf einem externen Backup-Server. Der Lizenznehmer kann diese Daten, soweit technisch möglich, jederzeit zu Sicherungszwecken exzerpieren und ist verpflichtet, dies in regelmäßigen üblichen Abständen zu tun.

4. Wenn und soweit der Lizenznehmer auf dem vom Lizenzgeber technisch verantworteten IT-Systemen personenbezogene Daten Dritter verarbeitet, ist eine Auftragsdatenverarbeitungsvereinbarung abzuschließen. Diese ergibt sich aus dem als Anhang 2 beigefügten Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO („Auftragsverarbeitungsvertrag“). Werden infolge einschlägiger Rechtsvorschriften Änderungen dieses Auftragsverarbeitungsvertrags erforderlich, so teilt der Lizenzgeber dem Lizenznehmer diese Änderungen schriftlich mit, woraufhin diese Änderungen Gegenstand des Auftragsverarbeitungsvertrags werden, es sei denn, der Lizenznehmer widerspricht diesen Änderungen innerhalb eines Monats in Textform. Im Falle eines solchen Widerspruchs hat der Lizenzgeber ein außerordentliches Kündigungsrecht dieses Softwarevertrags.

§ 5 Mitwirkungspflichten des Lizenznehmers

1. Der Lizenznehmer wird den Lizenzgeber bei der Erbringung der vertraglichen Leistungen in angemessenem Umfang unterstützen.

2. Die ordnungsgemäße und regelmäßige Sicherung seiner Daten obliegt dem Lizenznehmer. Das gilt auch für dem Anbieter im Zuge der Vertragsabwicklung überlassene Unterlagen.

3. Für die Nutzung der Software müssen die sich aus der Produktbeschreibung ergebenden Systemvoraussetzungen beim Lizenznehmer erfüllt sein. Der Lizenznehmer trägt hierfür selbst die Verantwortung.

4. Soweit der Lizenznehmer dem Lizenzgeber geschützte Inhalte überlässt (z.B. Grafiken, Marken und sonstige urheber- oder markenrechtlich geschützte Inhalte), räumt er dem Lizenzgeber sämtliche für die Durchführung der vertraglichen Vereinbarung erforderlichen Rechte ein. Das umfasst insbesondere das Recht, die entsprechenden Inhalte der Öffentlichkeit zugänglich zu machen. Der Lizenznehmer versichert in diesem Zusammenhang, dass er alle erforderlichen Rechte an überlassenen Kundenmaterialien besitzt, um dem Lizenzgeber die entsprechenden Rechte einzuräumen.

5. Der Lizenznehmer hat die ihm zur Verfügung gestellten Zugangsdaten geheim zu halten und dafür zu sorgen, dass etwaige Mitarbeiter, denen Zugangsdaten zur Verfügung gestellt werden, dies ebenfalls tun. Die Leistung des Lizenzgebers darf Dritten nicht zur Verfügung gestellt werden, soweit das nicht von den Parteien ausdrücklich vereinbart wurde.

§ 6 Geheimhaltung

Die Parteien verpflichten sich, das von der jeweils anderen Partei zugänglich gemachte Know-how sowie die Bestimmungen dieses Vertrages vertraulich zu behandeln und nicht an Dritte weiterzugeben. „Know-how“ ist die Gesamtheit praktischer Kenntnisse, die nicht allgemein bekannt oder leicht zugänglich und für die Produkte und Dienstleistungen der Partei oder ihrer verbundenen Unternehmen nützlich sind. Die Parteien verpflichten sich, ihre Angestellten, freie Mitarbeiter und Berater zur Geheimhaltung der vertraulichen Informationen zu verpflichten und den Kontakt mit vertraulichen Informationen auf solche Angestellte, freie Mitarbeiter und Berater zu beschränken, die einer vertraglichen Geheimhaltungspflicht unterliegen und im Rahmen eines üblichen Betriebs auf die Kenntnis der vertraulichen Informationen angewiesen sind. Die vorstehenden Pflichten erstrecken sich nicht auf Know-how, das (a) der anderen Partei bereits bekannt war, das (b) der Öffentlichkeit ohne Rechtsverletzung der anderen Partei allgemein zugänglich wird, oder das (c) der anderen Partei ohne Geheimhaltungsverpflichtung durch einen Dritten mitgeteilt wird, der dieses Know-how unabhängig von den Parteien entwickelt oder erhalten hat.

§ 7 Gewährleistung, Haftungsbeschränkung

1. Die Kuravisma GmbH ist verpflichtet, Mängel an überlassener Software zu beheben.

2. Die Gewährleistung ist ausgeschlossen, wenn die Gebrauchstauglichkeit der Software durch das Vorhandensein der Mängel nur unwesentlich beeinträchtigt wird. Dem Lizenznehmer ist bekannt, dass Software und Datenbanken in Folge ihrer Komplexität technisch nicht fehlerfrei erstellt werden können und nicht jeder technische Fehler einen Fehler bzw. Mangel im Rechtssinne darstellt. Die Kuravisma GmbH übernimmt keine Gewähr für die Verfügbarkeit und Funktionstüchtigkeit der an netzklasse angebundenen hard- und softwaretechnischen Komponenten Dritter, es sei denn, deren Nicht-Verfügbarkeit oder Funktionsuntüchtigkeit wird durch Fehler der Software oder eine fehlerhafte Anbindung der Software durch die Kuravisma GmbH verursacht. Aussagen zu netzklasse in Werbematerialien und auf der Website der Kuravisma GmbH verstehen sich ausschließlich als Beschaffenheitsbeschreibung und nicht als Garantie oder Zusicherung einer Eigenschaft. Aussagen zum Leistungsgegenstand stellen nur dann Garantien oder Zusicherungen im Rechtssinne dar, wenn sie schriftlich erfolgen und ausdrücklich und wörtlich als „Garantie“ oder „Zusicherung“ gekennzeichnet sind.

3. Die Behebung von Mängeln erfolgt nach Wahl von der Kuravisma GmbH durch kostenfreie Nachbesserung oder Ersatzlieferung. Eine Kündigung des Lizenznehmers wegen Nichtgewährung des vertragsgemäßen Gebrauchs nach § 543 Abs. 2 Satz 1 Nr. 1 BGB ist erst zulässig, wenn die Kuravisma GmbH ausreichende Gelegenheit zur Mängelbeseitigung gegeben wurde und diese fehlgeschlagen ist.

4. Die Kuravisma GmbH haftet im Rahmen der gesetzlichen Bestimmungen jeweils unbeschränkt für Schäden (a) aus Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer vorsätzlichen oder fahrlässigen Pflichtverletzung bzw. sonst auf vorsätzlichem oder fahrlässigem Verhalten der Kuravisma GmbH oder eines gesetzlichen Vertreters oder Erfüllungsgehilfen beruhen; (b) wegen des Fehlens oder des Wegfalls einer zugesicherten Eigenschaft bzw. bei Nichteinhaltung einer Garantie; (c) die auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung bzw. sonst auf vorsätzlichem oder grob fahrlässigem Verhalten der Kuravisma GmbH oder eines gesetzlichen Vertreters oder Erfüllungsgehilfen beruhen.

5. Die Kuravisma GmbH haftet unter Begrenzung auf Ersatz des vertragstypischen vorhersehbaren Schadens für solche Schäden, die auf einer leicht fahrlässigen Verletzung von wesentlichen Pflichten durch die Kuravisma GmbH oder einen seiner gesetzlichen Vertreter oder Erfüllungsgehilfen beruhen. Wesentliche Pflichten sind Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Lizenznehmer vertrauen darf.

6. Die Kuravisma GmbH haftet für sonstige Fälle leicht fahrlässigen Verhaltens begrenzt auf die Kosten einer Jahreslizenz je Schadensfall.

7. Die verschuldensunabhängige Haftung der Kuravisma GmbH nach § 536 a Abs. 1, 1. Alternative BGB wegen Mängeln, die bereits zum Zeitpunkt des Vertragsschlusses vorhanden sind, ist ausgeschlossen.

8. Die Kuravisma GmbH haftet bei einfach fahrlässig verursachtem Datenverlust nur für den Schaden, der auch bei ordnungsgemäßer und regelmäßiger, der Bedeutung der Daten angemessener Datensicherung durch den Lizenznehmer angefallen wäre; diese Begrenzung gilt nicht, wenn die Datensicherung aus von der Kuravisma GmbH zu vertretenden Gründen behindert oder unmöglich war.

9. Die vorstehenden Bestimmungen gelten sinngemäß für die Haftung der Kuravisma GmbH im Hinblick auf den Ersatz vergeblicher Aufwendungen.

10. Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

11. Die vorstehenden Haftungsbeschränkungen gelten auch für verbundene Unternehmen der Kuravisma GmbH sowie für die persönliche Haftung der Mitarbeiter, Vertreter und Organe der Kuravisma GmbH und den mit der Kuravisma GmbH verbundenen Unternehmen.

§ 8 Referenz/ Feedback

Der Lizenznehmer erklärt sich bereit, öffentlich als Referenzkunde des Lizenzgebers genannt zu werden und nach Abstimmung mit dem Lizenzgeber und unter Wahrung des gesetzlichen Datenschutzes Erfahrungsberichte von Endnutzern und Kunden zu den Kuravisma Produkten einzuholen und dem Lizenzgeber in anonymisierter Form zur Verfügung zu stellen.

§ 9 Folgen der Vertragsbeendigung

1. Der Lizenznehmer verpflichtet sich, mit der Vertragsbeendigung die Nutzung der Lizenz einschließlich des Know-hows einzustellen und beide Parteien verpflichten sich, alle vertraulichen Informationen der anderen Partei in physischer oder elektronischer Form zurückzugeben bzw. zu löschen und dies der anderen Partei auf Aufforderung schriftlich zu bestätigen.

2. Die Kuravisma GmbH wird dem Lizenznehmer nach Beendigung des Vertrages auf sein Verlangen und seine Kosten sämtliche für ihn im Zuge der Vertragserfüllung gespeicherte Daten in sonstiger geeigneter Form zur Verfügung stellen. Die Kuravisma GmbH ist berechtigt, einen kostendeckenden Vorschuss zu fordern. Verlangt der Lizenznehmer seine Daten innerhalb einer Frist von drei Monaten nach Beendigung des Vertrages nicht zurück oder verweigert er die Übernahme der insoweit entstehenden Kosten, ist die Kuravisma GmbH berechtigt, die Daten nach Ablauf einer Frist von einem weiteren Monat nach Zugang einer Ankündigung in Textform, dass die Daten im Falle eines unterbleibenden Herausgabeverlangens oder bei Nicht-Übernahme der Kosten gelöscht werden, zu löschen.

3. §§ 6, 7 und 8 dieses Vertrags bleiben von einer Vertragsbeendigung unberührt.

§ 10 Allgemeine Bestimmungen

Dieser Vertrag weist zwischen den Parteien verbindlich definierte Begriffe mit Anführungszeichen aus (Beispiel: „Definition“).

Rechte aus diesem Vertrag können nur mit schriftlicher Zustimmung der anderen Partei abgetreten werden.

Soweit dieser Vertrag für Willenserklärungen oder Mitteilungen ein Formerfordernis konstituiert, sind diese unwirksam, wenn sie der verlangten Form nicht entsprechen. Wenn nichts anderes bestimmt ist, genügen Email, Fax oder sonstige elektronische Kommunikation dem Schriftformerfordernis nach diesem Vertrag nicht. Nebenabreden zu diesem Vertrag bestehen nicht. Änderungen dieses Vertrages (einschließlich der Änderung dieser Schriftformklausel) sowie Nebenabreden bedürfen zu ihrer Wirksamkeit der Schriftform. Soweit einzelne Bestimmungen dieses Vertrages unwirksam oder undurchsetzbar sein sollten, lässt dies die Wirksamkeit des Vertrages im Übrigen unberührt, es sei denn, ein entgegenstehender Wille der Parteien ist nachweisbar.

Das als Anhang 1 bezeichnete Dokument ist Bestandteil dieses Vertrags; im Zweifel gehen die Bestimmungen dieses als Softwarevertrag bezeichneten Dokuments dem Anhang 1 vor.

Dieser Vertrag unterliegt deutschem Recht. Die Bestimmungen des UN-Kaufrechts finden keine Anwendung. Soweit zulässig ist ausschließlicher Gerichtsstand Dresden.

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO:

Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO

zwischen

Dem Lizenznehmer

– nachfolgend „**Auftraggeber**“ genannt –

und

Kuravisma GmbH, Käthe-Kollwitz-Ufer 76, 01309 Dresden

– nachfolgend „**Auftragnehmer**“ genannt –

1. Vertragsgegenstand

Im Rahmen der Leistungserbringung nach dem oben genannten Vertrag (nachfolgend „**Hauptvertrag**“ genannt) ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „**Auftraggeber-Daten**“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

2. Umfang der Beauftragung

2.1. Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.

2.2. Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie im Rahmen des Hauptvertrages spezifiziert. Die Verarbeitung betrifft die in Anlage 2 aufgeführten Arten personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

2.3. Dem Auftragnehmer bleibt es vorbehalten, die Auftraggeber-Daten zu anonymisieren oder zu aggregieren, so dass eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist, und in dieser Form zum Zweck der bedarfsgerechten Gestaltung, der Weiterentwicklung und der Optimierung sowie der Erbringung des nach Maßgabe des Hauptvertrags vereinbarten Dienstes zu verwenden. Die Parteien stimmen darin überein, dass anonymisierte bzw. nach obiger Maßgabe aggregierte Auftraggeber-Daten nicht mehr als Auftraggeber-Daten im Sinne dieses Vertrags gelten.

2.4. Der Auftragnehmer darf die Auftraggeber-Daten im Rahmen des datenschutzrechtlich Zulässigen für eigene Zwecke auf eigene Verantwortung verarbeiten und nutzen, wenn eine gesetzliche Erlaubnisvorschrift oder eine Einwilligungserklärung des Betroffenen das gestattet. Auf solche Datenverarbeitungen findet dieser Vertrag keine Anwendung.

2.5. Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44 - 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

3. Weisungsbefugnisse des Auftraggebers

3.1. Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In

letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2. Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens, in dem die Weisung zu dokumentieren und die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den Auftraggeber zu regeln ist.

3.3. Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Auftraggeber-Daten beim Auftraggeber liegt.

4. Verantwortlichkeit des Auftraggebers

4.1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

4.2. Dem Auftraggeber obliegt es, dem Auftragnehmer die Auftraggeber-Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Auftraggeber-Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4.3. Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.

4.4. Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

5. Anforderungen an Personal

Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten.

6. Sicherheit der Verarbeitung

6.1. Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.

6.2. Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen.

7. Inanspruchnahme weiterer Auftragsverarbeiter

7.1. Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus

Anlage 1. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.

7.2. Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.

7.3. Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.

7.4. Unter Einhaltung der Anforderungen der Ziffer 2.5 dieses Vertrags gelten die Regelungen in dieser Ziffer 7 auch, wenn ein weiterer Auftragsverarbeiter in einem Drittstaat eingeschaltet wird. Der Auftraggeber bevollmächtigt den Auftragnehmer hiermit, in Vertretung des Auftraggebers mit einem weiteren Auftragsverarbeiter einen Vertrag unter Einbeziehung der EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern vom 5.2.2010 zu schließen. Der Auftraggeber erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Art. 49 DSGVO im erforderlichen Maße mitzuwirken.

8. Rechte der betroffenen Personen

8.1. Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

8.2. Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

8.3. Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Auftraggeber-Daten, die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt, und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.

8.4. Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten, Auftraggeber-Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

8.5. Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten nach Art. 20 DSGVO besitzt, wird der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei der Bereitstellung der Auftraggeber-Daten in einem gängigen und maschinenlesbaren Format unterstützen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

9. Mitteilungs- und Unterstützungspflichten des Auftragnehmers

9.1. Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber zeitnah über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten unterstützen.

9.2. Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

10. Datenlöschung

10.1. Der Auftragnehmer wird die Auftraggeber-Daten nach Beendigung dieses Vertrages löschen, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.

10.2. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

11. Nachweise und Überprüfungen

11.1. Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

11.2. Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.

11.3. Zur Durchführung von Inspektionen nach Ziffer 11.2 ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 18 Uhr) nach rechtzeitiger Vorankündigung gemäß Ziffer 11.5 auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen Auftraggeber-Daten verarbeitet werden.

11.4. Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

11.5. Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.

11.6. Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 11 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

11.7. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrage anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

12. Vertragsdauer und Kündigung

12.1. Die Laufzeit und Kündigung dieses Vertrags richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

13. Haftung

13.1. Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

13.2. Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

14. Schlussbestimmungen

14.1. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.

14.2. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

Anlage 1:

Unterauftragnehmer

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
1&1 IONOS SE	Elgendorfer Straße 57 56410 Montabaur Deutschland	Rechenzentrum für die Anwendungs- und Datenbank Server Hosting Dienstleister

Technische und organisatorische Maßnahmen:

1.Zutrittskontrolle

Begleitung der Besucher durch Mitarbeiter
Besucher dürfen sich nicht frei im Unternehmen bewegen. Sie werden ständig von Mitarbeitern begleitet.

Dokumentation der Anwesenden (Datum, Zeit, Dauer) in Sicherheitsbereichen
Zeit, Datum und Dauer des Aufenthalts in den Bereichen der Datenverarbeitungsanlagen werden dokumentiert durch:
Mitarbeiter: Personalbüro Dokument: Besucherbuch im Personalbüro

Dokumentation v. Zutrittsrechten Zutrittsrechte zu den Datenverarbeitungsanlagen werden dokumentiert durch: IT-Administratoren
Dokument: kein Dokument, gesichert durch gesteuerte Schlüsselvergabe

Erfassung von Besuchern
Der Besuch wird dokumentiert durch:
Eintrag in ein Besucherbuch

Liste von berechtigten Personen (Serverraum)
Es wird eine Liste mit zugangsberechtigten Personen geführt. Diese sind: IT-Administratoren weitere Mitarbeiter: Helmut Radtke, Marion Richter Dokument: kein Dokument, gesichert durch gesteuerte Schlüsselvergabe

Schädigende Umwelteinflüsse für die Datenverarbeitung
Es existieren in den Räumen der Datenverarbeitung folgende Gefahren durch Umwelteinflüsse: Feuer: Feuerlöscher Stromausfall: USV's für die wichtigsten Server Überspannung: das EDV-Stromnetz ist überspannungsgesichert

Schutzmaßnahmen für Serverraum
Der Server befindet sich in einem verschlossenem Raum und ist gesichert durch: Sicherheitstür: ja, mit Stahlkern Sicherheitsfenster: nein, 1. OG

Sicherheitsmaßnahmen gegen Umwelteinflüsse
Die Sicherheitsmaßnahmen gegen diese Gefahren durch Umwelteinflüsse sind: Feuerfeste wasserdichte Aufbewahrung der Akten, Datenträger Unterbrechungsfreie Stromversorgung Leistungsschutzschalter Überspannungsschutz

Sicherung der Zugänge (Nebentüren, Fenster)
Die weiteren Zugänge (Nebentüren, Fenster) sind gesichert durch:
Sicherheitsfenster Sicherheitstüren Fenster/Türen werden beim Verlassen der Räume geschlossen

Verantwortlicher für die Bestimmung welche Räume, Bereiche, Objekte gesichert werden müssen
Die zu sichernden Objekte und Bereiche des Unternehmens werden festgelegt durch: Geschäftsführung

Verantwortlicher für die Zutrittskontrolle

Der Verantwortliche für die Zutrittskontrolle in unserem Unternehmen ist:
Verantwortlicher d. Rechenzentrums Geschäftsführer

2.Zugangskontrolle

Abmeldung vom PC bei Verlassen des Arbeitsplatzes
Mitarbeiter müssen sich beim Verlassen des Arbeitsplatzes abmelden. Eine automatische Abmeldung erfolgt ab 5 Minuten

Authentifizierung bei IT-Systemen
Eine Authentifizierung des Benutzer erfolgt über:
Passwort

Benutzerrechte
Benutzer haben ausschließlich die Rechte, die sie zur Erledigung ihrer Aufgaben benötigen. Über diese Rechte wird ebenfalls geregelt welche Software-Module (z.B. Einkauf, Auftragsverarbeitung, Personal) und damit welche Daten sichtbar sind.

Entsperrung von administrativen Zugängen
Im Falle einer Sperrung eines administrativen Zugangs erfolgt die Entsperrung folgendermaßen: Entsperrung wird dokumentiert über Service Desk

Erstellung v. Protokollen über Tätigkeiten auf Datenverarbeitungsanlagen
Die Erstellung von Protokollen über Tätigkeiten auf Datenverarbeitungsanlagen erfolgt:
automatisch

Kontrolle der Protokolle über Tätigkeiten auf Datenverarbeitungsanlagen
Die Protokolle über Tätigkeiten auf Datenverarbeitungsanlagen werden automatisch folgendermaßen kontrolliert: manuelle Kontrolle nach Bedarf.

Maßnahmen zum Schutz der Datenverwaltung
Zum Schutz der Datenverwaltung werden folgende Maßnahmen getroffen:
Für IT-Systeme: Passwortvergabe Protokollierung der Login-Daten Für die Aktenablage: verschlossene Aktenschränke verschlossener Aktenraum

Personelle Passwortvergabe
Die Sicherheit der personellen Passwortvergabe wird gewährleistet durch:
Jeder Mitarbeiter verfügt über eigenes Passwort; Verbot der Weitergabe

Der Schutz der administrativen Passwörter wird gewährleistet durch:
Hinweisblatt für Berechtigte über den Umgang mit administrativen Passwörtern:
Zugang nur für ausgewählte Personen Liste der Mitarbeiter Dokument:

Sichere Aufbewahrung von Administrationspasswörtern
Die sichere Aufbewahrung von Administrationspasswörtern wird folgendermaßen gewährleistet:
Aufbewahrungsort ist nur ausgewählten Mitarbeitern bekannt Aufbewahrung in Papierform, Sicherung durch: verschlossener Schrank Tresor Verschlüsseltes Dokument, Zugriff haben nur die MA IT

Sicherheit der Passwörter
Die Sicherheit der Passwörter wird gewährleistet durch: Vorgabe einer Mindestlänge Vorgabe der Komplexität (z.B. Gebrauch v. Sonderzeichen, Zahlen)

Sicherung der IT-Systeme gegen Unbefugte
Die IT-Systeme des Unternehmens sind durch folgende Maßnahmen gesichert: Standleitung Teilnehmererkennung

Speicherung der Passwörter Nutzer
Passwörter werden verschlüsselt gespeichert

Speicherung der Systempasswörter
Systempasswörter werden verschlüsselt gespeichert

Sperrung bei falscher Passworteingabe
Eine Sperrung des Benutzers bei falscher Passworteingabe findet
Für Domain-Zugriff nicht aktiviert.

Verantwortlicher für die Zugangskontrolle
Der Verantwortliche für die Zugangskontrolle in unserem Unternehmen ist:
Geschäftsführer IT-Administratoren

Vergabe von Gruppenpasswörtern
Gruppenpasswörter werden vergeben Bereich: Praktikanten Hinweis:
Gruppenpasswörter sollten nach Möglichkeit vermieden werden.

3.Zugriffskontrolle

Aufbewahrungsort bzw. -art der Datenträger
Datenträger werden folgendermaßen aufbewahrt:
verschlossenes Archiv verschlossene Schränke
Tresor

Aufteilung der Zugriffsberechtigung
Die Zugriffberechtigung ist aufgeteilt in/durch:
Anwendungsprogramme (bzw. einzelne Module der Software)
Dateien Datensätze Datenfelder Betriebssystem Server IT-System

Protokollierung der Zugriffsberechtigungen
Die Zugriffsberechtigungen werden protokolliert:
Dokument: aktuell nicht verfügbar

Verantwortlicher für die Zugriffskontrolle
Der Verantwortliche für die Zugriffskontrolle in unserem Unternehmen ist:
Geschäftsführer; IT-Administratoren

Zugriff der Nutzer auf Software
Mitarbeitern ist lediglich der Zugriff auf
getestete freigegebene Software möglich

Zugriffkontrolle für Mitarbeiter
Der Zugriff durch Mitarbeiter wird folgendermaßen kontrolliert: Benutzer haben ausschließlich die Rechte, die sie zur Erledigung ihrer Aufgaben benötigen. Über diese Rechte wird ebenfalls geregelt welche Software-Module (z.B. Einkauf, Auftragsverarbeitung, Personal) und damit welche Daten sichtbar sind.

4.Weitergabekontrolle/Übermittlungskontrolle

Maßnahmen zur Organisation der Datenübertragung
Zur Organisation der Datenübertragung wurden folgende Maßnahmen getroffen: Dokumentation und Regelung der Übermittlungswege/-Stellen Speicher-, Ablageort: Daten werden auch sicheren Server gespeichert, Zugriff haben zur Mitarbeiter mit spezieller Berechtigung

Mitbringen von privaten Datenträgern
Das Mitbringen von privaten Datenträgern ist folgendermaßen geregelt:
generelles Verbot

Nutzung von Online-Banking- RS Marion
Das Online-Banking wird mit folgendem Programm ausgeführt:
Direct Banking

Regelungen beim Ausscheiden v. Mitarbeitern
Beim Ausscheiden eines Mitarbeiters aus dem Betrieb wird das Benutzerkonto umgehend gesperrt

Bei der Versetzung von Mitarbeitern werden nicht mehr benötigte Rechte umgehend gelöscht.

Schutz der Daten vor Unbefugten bei der Übertragung
Daten werden bei der Übertragung vor Unbefugten geschützt durch:
Verschlüsselung

Sicherheitsmaßnahmen bei der Durchführung der Fernwartung
Bei der Fernwartung gelten folgende Sicherheitsmaßnahmen: Fernwartung ist nur über einen unternehmenseigenen Login-Server erlaubt Zugriff ist zeitlich begrenzt Zugriff wird beobachtet Zugriff wird durch Log-Dateien detailliert protokolliert

Sicherheitsmaßnahmen bei der Nutzung des Internets
Die Sicherheit der Nutzung des Internets wird durch folgend Maßnahmen gewährleistet: Einsatz Antivirenscanner (Hersteller automatisches update) Einsatz Firewall (Hersteller automatisches Update) Verwendung von https (SSL, TLS) FTP Verwendung Intrusion Detection System (IDS) Intrusion Prevention System (IPS) VPN

Sicherheitsmaßnahmen bei der Nutzung von Online-Banking
Die Sicherheit des Online-Bankings wird durch folgende Maßnahmen gewährleistet: Push- Tan, SMS-Tan (je nach Bank)

Sicherheitsmaßnahmen bei der Versendung. E-Mails
Bei der Versendung von E-Mails werden folgende Sicherheitsmaßnahmen getroffen. E-Mails werden: immer verschlüsselt bei sensiblen Daten (S/MiME, PGB) verschlüsselt

Sicherheitsmaßnahmen bei externen Dienstleistern, Dienstleistung (z.B. Reparatur) erfolgt außerhalb des Betriebs
Werden Dienstleistungen außerhalb des Betriebes erbracht, werden folgende Sicherheitsmaßnahmen getroffen: Daten werden verschlüsselt

Verantwortlicher für die Genehmigung der Fernwartung
Die Genehmigung zur Durchführung einer Fernwartung wird erteilt durch:
Geschäftsführer Abteilungsleiter IT-Administratoren

Vernichtung von Datenträgern

Datenträger werden vernichtet durch: magnetische Datenträger: durch ein gesichertes Verfahren mehrfaches Überschreiben Physisches Vernichtung zertifizierter externer Entsorger oder Shredder inhouse Papierakten: Aktenvernichter zertifizierter Entsorger Vernichtung wird dokumentiert

Verschlüsselung von Daten beim Transport

Beim Transport werden folgende Daten verschlüsselt: sensible Daten

Verwahrung von unbenutzten Datenträgern

Unbenutzte Datenträger werden folgendermaßen verwahrt: Verschlossener Schrank Tresor Verschlossener Raum

5.Eingabekontrolle/Plausibilitätskontrolle/Transaktionskontrolle

Installation von neuer Software

Folgende Sicherheitsmaßnahmen gelten bei der Installation von neuer Software: Anti-Virenscan Integritätsprüfung

Intervalle der Überprüfung durch Antiviren-Software

Eine Überprüfung durch Antiviren-Software findet statt: laufend

Netzwerkdokumentation

Die Erstellung einer Netzwerkdokumentation erfolgt: Regelmäßig Speicher-, Ablageort: Goole Docs/DC1
Hinweis: Die Mindestanforderung an eine Netzwerkdokumentation sollte einem bereinigten Netzplan entsprechen. Handelt es sich um Auftragsdatenverarbeitung, sollte darüber hinaus vom Auftragnehmer eine Anwendungslandkarte mit den Informationsflüssen der beauftragten IT-Umgebung bereitgestellt werden.

Schutz vor Schadsoftware

Das System wird folgendermaßen vor Schadsoftware geschützt:
Antiviren-Software: Fortinet Antivirenscan, MS Defender
Firewall: Fortinet 6

Speicherung von Daten und Programmen

Daten und Programme werden folgendermaßen gespeichert: in unterschiedlichen Verzeichnissen

Überprüfung fremder Datenträger

Für die Benutzung fremder Datenträger gelten folgende Sicherheitsmaßnahmen: Benutzung fremder Datenträger ist ausgeschlossen

Update der Anwendungsprogramme

Updates der Anwendungsprogramme erfolgen: automatisch

Update des Betriebssystems

Die Installation von sicherheitsrelevanten Updates des Betriebssystems erfolgt: Umgehend automatisch

Update des Schadsoftwareschutzes
Updates des Schadsoftwareschutzes erfolgen:
automatisch

6.Auftragskontrolle/Vertragskonformitätskontrolle

Maßnahmen zur Gewährleistung, dass Datenverarbeitung weisungsgemäß stattfindet Durch folgende Maßnahmen wird gewährleistet, dass die Verarbeitung der Daten weisungsgemäß ausgeführt wird: schriftlicher Vertrag Auftraggeber erhält Datenausgaben zur Kontrolle Kontrolle vor Ort durch Auftraggeber möglich

7.Verfügbarkeitskontrolle

Anzahl der Generationen der Sicherheitskopien
Sicherheitskopien werden nach dem Generationenprinzip erstellt.
Anzahl der Generationen: Großvater-Vater-Sohn- Prinzip

Archivierung wichtiger E-Mails Wichtige E-Mails
werden folgendermaßen archiviert: automatisch

Archivordnung Eine Archivordnnung liegt vor
Hinweis: In einer Archivordnung wird z.B. geregelt
welche Dokumente archiviert werden Wer der
Verantwortliche ist Wann welche Daten archiviert
werden Aufbewahrungsfristen Löschfristen
Anforderungen an Einsicht, Ausgabe der Daten

Archivverwalter Der Archivverwalter unseres Unternehmens ist:
Frau Marion Richter

Aufbewahrung Backupmedien Die
Backupmedien werden aufbewahrt: Tresor
Serverraum

Backup-Methode Bei einem Backup wird
Folgendes gesichert: Totalsicherung
Datenbestände veränderte Daten

Dokumentation Backupverfahren Das
Backupverfahren wird dokumentiert
regelmäßig

Gesetzlichen Aufbewahrungspflichten Die gesetzlichen Aufbewahrungspflichten werden eingehalten. Die Einhaltung wird kontrolliert.

Klimatisierung des Serverraums
Der Serverraum ist klimatisiert

Kontrolle Backupverfahren Das
Backupverfahren wird kontrolliert
regelmäßig, durch Geschäftsführer IT-
Administratoren

Schutzmaßnahmen des Archivs Das Archiv ist durch folgende Maßnahmen geschützt: eigener Raum, verschlossen Zugang nur für Berechtigte Archivverwalter vor Ort

Zeitintervall Backup Ein Backup wird erstellt gemäß Backupplan https://docs.google.com/spreadsheets/d/1MYY78hlbQ41S3gDex_RwPVgOo0JaS0EkrWIeA4FcfWE/edit#gid=0

9 Prüfung der Betriebsorganisation und Rechenschaftspflicht

Organisatorische Maßnahmen zur Einhaltung des Datenschutzes bzgl. der Daten Durch folgende organisatorische Maßnahmen wird die Einhaltung des Datenschutzes bzgl. der Daten gewährleistet: Dokumentation aller Programme Regelung der Aufbewahrung/Archivierung aller Protokolle Verfahren für die Erteilung von Zugangsberechtigungen

Organisatorische Maßnahmen zur Einhaltung des Datenschutzes bzgl. der Rechte der Betroffenen Durch folgende organisatorische Maßnahmen wird die Einhaltung des Datenschutzes bzgl. der Rechte der Betroffenen gewährleistet: Geltendmachung der Rechte (Auskunft, Löschung usw.) werden umgehend bearbeitet und dokumentiert Einhaltung des Schutzniveaus der Art. 44 ,46, 49 DS-GVO bei Übertragung in Drittländer

Organisatorische Maßnahmen zur Einhaltung des Datenschutzes bzgl. Mitarbeiter Durch folgende organisatorische Maßnahmen wird die Einhaltung des Datenschutzes durch Mitarbeiter gewährleistet: Verarbeitungsverzeichnis vollständig und aktuell Mitarbeiterschulungen zum Datenschutz Vertraulichkeitsverpflichtungen für Mitarbeiter externer Datenschutzbeauftragter Fachkundenachweis des Datenschutzbeauftragten Vertraulichkeitsverpflichtungen freier Mitarbeiter Vertrag mit Auftragsverarbeiter

Diese Angaben beziehen sich auf den Serverraum in unserem Unternehmen. Die Web-Applikation wird extern gehostet, von einer Firma, die dies professionell macht und gesonderte Sicherheitsstandards verwirklicht hat.

Bestellschein Schulen - netzklasse

Anhang 1 - Umfang und technische Voraussetzungen

Virtuelles Klassenzimmer netzklasse als Cloud Lösung

Netzklasse ist eine cloudbasierte Software für Kommunikation, Präsentation und Dokumentation von virtuellen Schulstunden.

Das Schul-Paket umfasst netzklasse als reine Cloud-Lösung für Präsenz- und virtuelle Schulstunden. Als Cloud-Lösung ist netzklasse via Internet und Browser-Zugang auf den Cloud-Servern der 1&1 IONOS SE zugänglich.

Leistungsbeschreibung netzklasse

Virtuelle Schulstunden und Präsentation		
Import von Präsentationsfolien (PDF, Bilddateien)	✔	
Regiefunktion für Lehrer	✔	
Darstellung von Präsentationsfolien	✔	
Erstellung von Unterrichtssleitfäden	✔	
Zeichenfunktion	✔	
Multi-User Videostream (Aug' 2020)	✔	
Textchat	✔	
Screensharing (Aug' 2020)	✔	
Eigene Inhalte	✔	
Dokumentation der Unterrichtsstunde	✔	
Support		
Persönlicher (bei Premium Support Buchung)	✔	
Extras		
Dashboard mit Schnellstart zu Stunden	✔	
Übersicht vergangener Stunden	✔	

Legende:

✔ vorhanden
x nicht unterstützt

Geräteanforderungen netzklasse (SaaS)

Minimum Hardware Anforderung

Bildschirmgröße	10 Zoll mit Auflösung 1280 x 1024
RAM Größe Rechenleistung	2 GB zu Windows 7 kompatibler Rechner

Browser

Es werden die Browser Chrome, Firefox und Safari in der jeweils letzten oder vorletzten veröffentlichen Version unterstützt, Stand derzeit: Dezember 2019.

Internetverbindung

Es wird mindestens eine für den geographischen Nutzungsraum (Deutschland) übliche Internetverbindung mit 13,9 Mbit / s benötigt.

Vergleiche Statista:
https://de.statista.com/infografik/1064/top-10-laender-mit-dem-schnellsten-internetzugang/