Vertrag zur Auftragsdatenverarbeitung
als Ergänzung zum Vertrag vom Klicken Sie hier, um ein Datum einzugeben.

zwischen der

[Name und Anschrift des Auftraggebers]

- Auftraggeber, nachstehend Verantwortlicher genannt -

und

PAGENTUS Systems S.á r.l., 17 Fausermillen, 6689 Mertert, Luxembourg

- Auftragnehmer, nachstehend genannt PAGENTUS SYSTEMS -

zusammen auch – die Parteien – genannt

Präambel

PAGENTUS SYSTEMS verarbeitet personenbezogene Daten für den Verantwortlichen. Dieser Vertrag regelt insbesondere die Verarbeitung personenbezogener Daten im Rahmen der Nutzung der Dienste wie sie im Lizenzvertrag festgelegt sind („Dienste“), die von PAGENTUS SYSTEMS unter Nutzung der Amazon-Web-Services-Cloud (AWS –Cloud) zur Verfügung gestellt wird.

Entsprechend den gesetzlichen Vorschriften über die Auftragsdatenverarbeitung werden die folgenden Punkte geregelt:

1. Gegenstand, Dauer und Spezifizierung der Auftragsdatenverarbeitung
   - 1.1. Dieser Auftragsdatenverarbeitungsvertrag regelt die Verpflichtungen der Vertragsparteien in Zusammenhang mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten des Verantwortlichen durch PAGENTUS SYSTEMS. Grundlage dieser Leistungen ist das Angebot der PAGENTUS SYSTEMS vom Klicken Sie hier, um ein Datum einzugeben. inklusive der Nutzungsbedingungen der Dienste und der Annahme durch die Bestellung des Verantwortlichen am Klicken Sie hier, um ein Datum einzugeben.(„Lizenzvertrag“). Der Lizenzvertrag ist als Kopie im Anlage 1 beigefügt.
   - 1.2. Auf Basis des Lizenzvertrags stellt PAGENTUS SYSTEMS dem Verantwortlichen den Zugang zu den Diensten.
   - 1.3. Dieser Vertrag zur Auftragsdatenverarbeitung konkretisiert in diesem Zusammenhang die datenschutzrechtlichen Verpflichtungen der Parteien aus diesem Vertragsverhältnis und findet Anwendung auf alle Tätigkeiten, die mit dem Lizenzvertrag in Zusammenhang stehen und soweit Beschäftigte von PAGENTUS SYSTEMS oder von PAGENTUS SYSTEMS Beauftragte mit personenbezogenen Daten des Verantwortlichen und/oder der Kunden des Verantwortlichen und/oder der Partner des Verantwortlichen in Berührung kommen könnten.
   - 1.4. Dieser Vertrag entspricht den Anforderungen an einen Vertrag über die Auftragsdatenverarbeitung nach den Vorschriften des Bundesdatenschutzgesetzes (BDSG) sowie den Vorschriften der Datenschutz-Grundverordnung (DSGVO). Soweit sich in diesem Vertrag Verweise auf das BDSG finden, gelten diese ab dem 25. Mai 2018 mit der Maßgabe, dass sie sich auf die inhaltlich entsprechenden Regelungen der DSGVO beziehen. Insbesondere sind vorhandene Verweise auf Verpflichtungen nach § 11 BDSG ab diesem Zeitpunkt als Verweise auf die entsprechenden Verpflichtungen nach Art. 28 DSGVO zu verstehen. Soweit sich in diesem Vertrag Verweise auf Vorschriften der DSGVO befinden, gelten die entsprechenden Vertragsregelungen ab dem 25. Mai 2018.
   - 1.5. Die in diesem Vertrag verwendeten datenschutzrechtlichen Rechtsbegriffe orientieren sich an den in der DSGVO verwendeten Begriffen. Vor dem 25. Mai 2018 (unter Anwendbarkeit des BDSG) sind diese Rechtsbegriffe und die entsprechenden Vertragsregelungen deshalb im Hinblick auf die Bedeutung der verwendeten Begriffe so auszulegen und anzuwenden, wie sie nach Maßgabe der DSGVO auszulegen sind.
   - 1.6. PAGENTUS SYSTEMS hostet die Dienste in europäischen Rechenzentren der Firma Amazon WEB SERVICES INC in Frankfurt. Das Video-Transcoding erfolgt am Standort Irland, da der Service innerhalb Europas nur dort angeboten wird.

1.7. Die Firma Amazon WEB SERVICES INC organisiert die Sicherheit des Rechenzentrums (Host-Betriebssysteme, Virtualisierungsebenen und physische Sicherheit) selbst und wird diesbezüglich als Subunternehmer gem. § 5 dieses Vertrages für PAGENTUS SYSTEMS tätig. Es gilt das Prinzip der geteilten Verantwortung im Rahmen der sog. Amazon-Web-Services (AWS), vgl. Anhang 2.

1.8. Neben den cloudbasierten Diensten findet eine Datenverarbeitung der „Organisations- und User-Daten" am Standort von PAGENTUS SYSTEMS in Mertert, Luxemburg ausschließlich zu Abrechnungszwecken statt. Hierbei existiert keine direkte Verbindung zwischen den Datenverarbeitungssystemen. Details hierzu ergeben sich aus den technischen und organisatorischen Maßnahmen in Anhang 1 dieses Vertrages.

1.9. Die Verarbeitung von Dateianhängen und Videodateien, die von den Nutzern des Verantwortlichen zu der PAGENTUS SYSTEMS hochgeladen werden (sog. Artefakte) werden zur Beschleunigung des Datentransfers und zum Zwecke einer latenzfreien Verteilung an die andere berechtigte Nutzer auf weltweit verteilten Caching-Servern zwischengespeichert (= Content-Delivery-Network), so dass diese nicht für den Austausch personenbezogener Daten genutzt werden dürfen. Dateiuploads dienen lediglich dem vereinfachten Datenaustausch, nicht personenbezogener und nicht geheimhaltungsbedürftiger Informationen. Die PAGENTUS SYSTEMS bedient sich hierzu ausschließlich der Caching-Dienste der in Ziffer 6 genannten Unterauftragnehmer. Die Nutzer des Verantwortlichen sind angehalten, nur Dateianhänge ohne jeglichen Personenbezug als Artefakte hochzuladen, da die Dateien von jedem beliebigen Internetnutzer bei Kenntnis der jeweiligen URL abgerufen werden können. Aus diesem Grund ist der Datei-Upload der Dienste auch nicht geeignet, sonstige geheimhaltungsbedürftige Artefakte, auszutauschen, auch wenn diese keinen Personenbezug aufweisen.

1.10. Die Laufzeit dieses Auftrages richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieses Auftrages nicht darüber hinausgehende Verpflichtungen ergeben.

1.11. Art der Daten:

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien (zutreffende Kategorie (n) bitte ankreuzen):

- [x] Kommunikationsdaten (z.B. Telefon, E-Mail)
- [x] Vertragsstammdaten (z.B. Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- [x] Kundendaten (z.B. Name, Profilbild, Anschrift)
- [x] Mitarbeiterdaten (z.B. Anrede, Vorname, Name, Profilbild)
- [x] Vertragsabrechnungs- und Zahlungsdaten
- [x] Statistische Auswertungen (Reporting)
- [ ] Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- [ ] Klicken Sie hier, um Text einzugeben.

1.12. Kreis der Betroffenen:

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst (zutreffende Kategorie (n) bitte ankreuzen)):

- [ ] Kunden
- [x] Nutzer/ User
- [ ] Interessenten
- [ ] Abonnenten
- [x] Beschäftigte i. S. d. § 3 Abs. 11 BDSG (z.B. User mit der Rolle Organisations-Manager und Themen-Manager, Buchhaltung)
- [ ] Lieferanten
- [ ] Handelsvertreter
- [x] Ansprechpartner
- [ ] Klicken Sie hier, um Text einzugeben.

2. Anwendungsbereich und Verantwortlichkeit, Haftungsfreistellung

2.1. EUROBASE verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Dies umfasst Tätigkeiten, die im Vertrag und im Auftrag konkretisiert sind. Der Verantwortliche ist im Rahmen dieses Auftrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an EUROBASE sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („verantwortliche Stelle" im Sinne des § 3 Abs. 7 BDSG bzw. „Verantwortlicher" im Sinne des Art. 4 Nr. 7 DSGVO).

2.2. Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

2.3. Soweit EUROBASE gemäß den Weisungen des Verantwortlichen handelt und die technischen und organisatorischen Maßnahmen und die sonstigen ihm durch diese Vereinbarung auferlegten Verpflichtungen beachtet, stellt der Verantwortliche EUROBASE auf erstes Anfordern von allen rechtlichen Ansprüchen, Schäden und Kosten frei, soweit diese dadurch entstehen, dass Dritte oder betroffene Personen aus der Datenverarbeitung resultierende Ansprüche gegen EUROBASE geltend machen. Hiervon umfasst sind insbesondere auch die Kosten der notwendigen Rechtsverteidigung einschließlich sämtlicher Gerichts- und Anwaltskosten in der jeweiligen gesetzlichen Höhe, sowie Bußgelder in tatsächlich festgesetzter Höhe. Gegenstand der Freistellung sind demnach insbesondere Ansprüche aufgrund von rechtswidrigen Weisungen des Verantwortlichen gemäß Art. 28 Abs. 3 S. 3 DSGVO sowie nicht ausreichender technisch-organisatorischer Maßnahmen, die gemäß Ziffer 3 dieser Vereinbarung vom Verantwortlichen freigegeben wurden. Dem Verantwortlichen bleibt im Nachgang vorbehalten, nachzuweisen, dass die gegen EUROBASE gerichteten, vorgenannten Ansprüche und Bußgelder nicht auf Weisungen oder Pflichtverletzungen des Verantwortlichen beruhen.

3. Technisch-organisatorische Maßnahmen

3.1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und EUROBASE geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

3.2. EUROBASE hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Verantwortlichen zur Prüfung zu übergeben. Der Verantwortliche hat die technischen und organisatorischen Maßnahmen zu prüfen und EUROBASE Änderungswünsche mitzuteilen. EUROBASE ist berechtigt, Änderungswünsche abzulehnen und/oder unter den Vorbehalt der Kostenübernahme durch den Verantwortlichen zu stellen. Soweit die technischen und organisatorischen Maßnahmen gem. Anlage 2 von dem Verantwortlichen akzeptiert werden, werden diese ausschließliche Grundlage des Auftrages i.S.d. Ziffer 2.3. Soweit die Prüfung des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.3. Der Verantwortliche ist im Rahmen dieser Vereinbarung allein verantwortlich für die Beurteilung der Angemessenheit der technischen und organisatorischen Maßnahmen. EUROBASE setzt die vom Verantwortlichen geprüften Maßnahmen entsprechend dem gemäß Ziffer 3.2 dokumentierten Umfang um.

3.4. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen, die den angemessenen Schutz der Daten des Verantwortlichen treffen und die den Anforderungen des Bundesdatenschutzgesetzes (Anlage zu § 9 BDSG) bzw. der DSGVO (Art. 32) genügen. Diese Maßnahmen werden wie folgt festgelegt und sind entsprechend zu dokumentieren und dem Verantwortlichen vorzulegen: Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebots, sowie andererseits um auftragsspezifische Maßnahmen, insbesondere im Hinblick auf die Art des Datenaustauschs / Bereitstellung von Daten, Art / Umstände der Verarbeitung / der Datenhaltung sowie Art / Umstände beim Output / Datenversand. Die Maßnahmen schließen unter anderem Folgendes ein: die Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

3.5. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es EUROBASE gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. EUROBASE hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG dem Verantwortlichen zur Verfügung zu stellen.

3.6. Der Verantwortliche und EUROBASE unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

4. Anfragen Betroffener, Berichtigung, Sperrung und Löschung von Daten; Unterstützung durch EUROBASE

4.1. EUROBASE hat nur nach Weisung des Verantwortlichen die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an EUROBASE zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird EUROBASE dieses Ersuchen

unverzüglich an den Verantwortlichen weiterleiten. Die Prüfung der Anfrage obliegt ausschließlich dem Verantwortlichen.

4.2. EUROBASE verpflichtet sich, den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen in Ansehung der Art der Verarbeitung dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in § 34 BDSG und Kapitel III der Datenschutzgrundverordnung genannten Rechte der betroffenen Person nachzukommen.

4.3. Ist der Verantwortliche auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu erteilen, oder ist der Verantwortliche zur Berichtigung, Löschung, Einschränkung der Verarbeitung oder zur Datenübertragung verpflichtet, wird EUROBASE den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung dieser Rechte nachzukommen.

4.4. Der Verantwortliche wird EUROBASE schriftlich oder in Textform zur Mitwirkung auffordern, sofern solche Mitwirkungshandlungen von EUROBASE erforderlich sind. Der Verantwortliche stellt EUROBASE auf erste Anforderung von den durch diese Unterstützung entstandenen Kosten frei, soweit EUROBASE dem Verantwortlichen vorab den Kostenrahmen schriftlich oder in Textform mitgeteilt hat.

4.5. EUROBASE wird keine Auskunftsverlangen oder anderweitige Anfragen bezüglich der Rechte Betroffener beantworten und den Betroffenen insoweit an den Verantwortlichen verweisen.

4.6. Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung oder Sperrung an EUROBASE, wird EUROBASE den Betroffenen an den Verantwortlichen verweisen.

5. Kontrollen und sonstige Pflichten von EUROBASE

EUROBASE hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags folgende Pflichten:

- ⇨ Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 4f, 4g BDSG bzw. Art. 37 bis 39 DSGVO ausüben kann. Dessen Kontaktdaten werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt.
- ⇨ Die Wahrung des Datengeheimnisses. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Verantwortlichen zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.
- ⇨ Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und Anlage bzw. entsprechend Art. 32 DSGVO.
- ⇨ Unterstützung des Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der EUROBASE zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit der Verarbeitung (z.B. Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Durchführung einer Datenschutz-Folgenabschätzung oder der vorherigen Konsultation der Aufsichtsbehörde).
- ⇨ Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG, soweit die Datenverarbeitungsprozesse die von EUROBASE für den Verantwortlichen ausgeführt werden, betroffen sind. Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG bei EUROBASE ermittelt.
- ⇨ Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch EUROBASE im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

6. Unterauftragsverhältnisse

6.1. Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten von EUROBASE Unterauftragsverarbeiter einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

- ⇨ Die Einschaltung von Unterauftragsverarbeitern ist grundsätzlich nur mit schriftlicher Zustimmung des Verantwortlichen gestattet. Ohne schriftliche Zustimmung kann EUROBASE zur Vertragsdurchführung unter Wahrung seiner unter Punkt 5 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie im Einzelfall andere Unterauftragsverarbeiter mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Verantwortlichen vor Beginn der Verarbeitung oder Nutzung mitteilt und der Verantwortliche hierdurch die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.
- ⇨ EUROBASE hat die vertraglichen Vereinbarungen mit dem / den Unterauftragsverarbeiter/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen dem Verantwortlichen und EUROBASE entsprechen, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass sie den gesetzlichen Anforderungen des Datenschutzrechts entsprechen.

⇨ Bei der Unterbeauftragung sind Kontroll- und Überprüfungsrechte des Verantwortlichen entsprechend dieser Vereinbarung und des § 11 BDSG i.V.m. Nr. 6 der Anlage zu § 9 BDSG beim Unterauftragsverarbeiter einzuräumen. Dies umfasst auch das Recht des Verantwortlichen, von EUROBASE auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

6.2. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die EUROBASE bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. EUROBASE ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

6.3. Soweit der Auftragsverarbeiter Unterauftragsverarbeiter zur Erfüllung seiner Leistungen nach diesem Auftrag einsetzt, sind diese nachfolgend zu bezeichnen:

Unterauftragsverarbeiter	Gegenstand	Zertifikate, Mitgeltende Unterlagen
Amazon WEB SERVICES INC	AWS-Cloud Services Irland	ISO 27018 und DIN ISO/IEC 27001

7. Kontrollrechte des Verantwortlichen

7.1. Der Verantwortliche überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen von EUROBASE und dokumentiert das Ergebnis.

⇨ Hierfür kann er z. B. Auskünfte von EUROBASE einholen,

⇨ sich ein ggf. vorhandenes Testat eines Sachverständigen vorlegen lassen

⇨ oder nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zu EUROBASE steht.

7.2. EUROBASE verpflichtet sich, dem Verantwortlichen auf Anforderung in Textform innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen und Prüfungen – einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen oder dazu beizutragen, die zur Durchführung einer Kontrolle erforderlich sind.

8. Mitteilung bei Verstößen von EUROBASE

EUROBASE unterrichtet den Verantwortlichen unverzüglich bei schwerwiegenden Verstößen von EUROBASE oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Verantwortlichen oder die im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Verantwortlichen ab. EUROBASE unterstützt den Verantwortlichen bei der Erfüllung der Informationspflichten nach § 42a BDSG.

9. Weisungsbefugnis des Verantwortlichen

9.1. Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen in dem zu Grunde liegenden Vertrag und diesem Auftragsdatenverarbeitungsvertrag und nach dokumentierter Weisung von dem Verantwortlichen. Der Verantwortliche behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

9.2. Auskünfte an Dritte darf EUROBASE nur nach vorheriger schriftlicher Zustimmung des Verantwortlichen erteilen.

9.3. Der Verantwortliche wird mündliche Weisungen unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. EUROBASE verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen von des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

9.4. Die vorstehenden Beschränkungen der Ziffern 9.1 bis 9.3 bezüglich der Verarbeitung personenbezogener Daten gelten nur, sofern EUROBASE nicht durch das Recht der Union oder der Mitgliedstaaten, dem EUROBASE unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt EUROBASE dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

9.5. EUROBASE hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. EUROBASE ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

9.6. Bezüglich der Weisungsbefugnis wird Folgendes vereinbart:

Weisungsberechtigte Personen des Verantwortlichen sind:

Name	Funktion	Telefon / E-Mail-Adresse

Weisungsempfänger beim Auftragsverarbeiter sind:

Name	Funktion	Telefon / E-Mail-Adresse
Peter Kühnel	Geschäftsführer/ Managing Director	Tel. +352 74 92 92 – 35, ds@pagentus.com

9.7. Die Parteien verpflichten sich, bei Wechsel oder längerfristiger Verhinderung des jeweiligen Ansprechpartners unverzüglich schriftlich einen Nachfolger bzw. Vertreter zu benennen.

10. Löschung von Daten und Rückgabe von Datenträgern

10.1. Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung des Vertrages hat EUROBASE sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Verantwortlichen an den Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten, sofern nicht nach dem Unionsrecht oder dem anwendbaren Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

10.2. Von den vorgenannten Löschungsregelungen nicht umfasst sind die bei PAGENTUS SYSTEMS automatisiert angefertigten Backups, die erst nach Durchlauf eines Backup-Intervalls von 14 Tagen nach Löschung der operativ genutzten Datenbestände automatisiert aktualisiert und dementsprechend gelöscht werden.

11. Informationspflichten, Schriftformklausel, Rechtswahl

11.1. Sollten die Daten des Verantwortlichen bei EUROBASE durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat EUROBASE den Verantwortlichen unverzüglich darüber zu informieren. EUROBASE wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei dem Verantwortlichen als »verantwortlicher Stelle« im Sinne des Bundesdatenschutzgesetzes bzw. als »Verantwortlicher« im Sinne der Datenschutzgrundverordnung liegen.

11.2. Änderungen und Ergänzungen dieses Auftrages und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen von EUROBASE – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

11.3. Bei etwaigen Widersprüchen gehen Regelungen dieses Auftragsdatenverarbeitungsvertrages zum Datenschutz, ggf. bestehenden datenschutzrechtlichen Regelungen des zu Grunde liegenden Vertrages vor. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts.

Ort: _____ Datum:_____ Ort: _____ Datum:_____

EUROBASE Verantwortlicher

ANHANG 1: Angebot vom Klicken Sie hier, um ein Datum einzugeben.**inklusive der Nutzungsbedingungen zu den Diensten und der Annahme durch die Bestellung des Verantwortlichen am** Klicken Sie hier, um ein Datum einzugeben.

ANHANG 2 - Technische und organisatorische Maßnahmen der PAGENTUS SYSTEMS

I. Technische und organisatorische Maßnahmen für die Dienste

1. Zutrittskontrolle

1.1. Die Dienste basieren auf einer Cloud-Infrastruktur. Dies betrifft die Produktiv-, Konsolidierungs- und Testsysteme. Hierbei finden Amazon AWS „Infrastruktur Services“ (EC2, EBS, Auto Scaling...) Amazon AWS „Container Services“ (RDS) und Amazon AWS „Abstrakte Services“ (S3, SES…).

1.2. Für die zugrundeliegende Cloud Infrastruktur gilt das Prinzip der geteilten Verantwortung (https://aws.amazon.com/de/compliance/shared-responsibility-model/). Vereinfacht kann man festhalten, das Amazon für die relevanten Maßnahmen zur Sicherheit der Cloud-Infrastruktur als solche und PAGENTUS SYSTEMS für die Sicherheit der Daten „in der Cloud“ verantwortlich ist. Daher verweist die PAGENTUS SYSTEMS für die Umsetzung und Einhaltung der Zutrittskontrolle an den Cloud Provider, Amazon WEB SERVICES INC, 410 Terry Avenue North, Seattle, WA 98109-5210. USA. Amazon AWS ist u.a gemäß DINISO/IEC27001 zertifiziert, https://aws.amazon.com/de/compliance/iso-27001-faqs/ und gemäß ISO 27018 zertifiziert, https://aws.amazon.com/de/compliance/iso-27018-faqs/.).

1.3. Neben den cloudbasierten Dienste findet eine Datenverarbeitung der „Organisations- und User-Daten“ am Standort der PAGENTUS SYSTEMS in Mertert ausschließlich zu Abrechnungszwecken statt. Hierbei existiert keine direkte Verbindung zwischen den Datenverarbeitungssystemen. Die TOMs für diesen Bereich sind unter „TOMs für die PAGENTUS SYSTEMS“ zu finden.

2. Zugangskontrolle

2.1. Die Zugangskontrolle fällt in Teilen, analog der Zutrittskontrolle, unter das oben beschriebene Prinzip der geteilten Verantwortung. Durch die Verwendung von Amazon AWS IAM (Identity and Access Management) entsteht jedoch bei beiden Parteien (Amazon AWS und PAGENTUS SYSTEMS) eine Pflicht zur Umsetzung und Einhaltung der Zugangskontrollen. Der physische Zugang zu den AWS-Rechenzentren richten sich nach den unter Ziffer III beschriebenen Gegebenheiten.

2.2. Die Serversysteme der Dienste innerhalb der AWS-Cloud werden von PAGENTUS SYSTEMS-eigenem Personal konfiguriert und gepflegt.

2.3. Administrationsaufgaben innerhalb der AWS-Cloud wie z.B. die der Systemverwaltung, Netzverwaltung, Datenbankverwaltung oder die Verwaltung der Applikationsserver werden ausschließlich von Administratoren der PAGENTUS SYSTEMS wahrgenommen.

2.4. Der administrative Zugang zur Infrastruktur der Dienste der verwendeten AWS Cloud-Services, welche die Datenverarbeitungsanlagen der Dienste abbilden, wird über das AWS IAM (Identity and Access Management) geregelt. Dabei wird die Integrität in Abhängigkeit des Sicherheitsniveaus durch Ein-Faktor-Authentifizierung (Benutzername und Kennwort) über Zugriffsschlüssel bei API-Aufrufen und Zwei-Faktor-Authentifizierung (Wissen und Besitz) mit Hardware-Token bei administrativen Systemzugriffen auf die AWS Cloud Management Systeme gewährleistet.

2.5. Der administrative Zugang zu den Applikationsservern der Dienste die als Cloud-Service betrieben werden, erfolgt ausschließlich über SSH, abgesichert mit dem RSA-Verschlüsselungsverfahren.

2.6. Der administrative Zugang zu den Datenbanken erfolgt zum einen über die AWS Cloud Management Systeme, und unterliegt somit dem oben beschriebenen AWS IAM, und zum anderen über native Datenbank Administrationssoftware. Hierbei erfolgt der Zugriff TLS-verschlüsselt.

2.7. Sowohl der administrative Zugang zu den Applikationsservern per SSH, als auch der native administrative Datenbankzugang unterliegen einer zusätzlichen IP-Beschränkung auf Adressen aus dem PAGENTUS SYSTEMS-eigenen AS-60288 Adressbereich.

2.8. Der Zugang zu den „Video-Tutorials“ durch die user der Dienste (Endbenutzer) ist uneingeschränkt öffentlich (kein IP blocking etc.) und unterliegt jedoch einer Authentifizierung

2.9. Die Benutzereingaben der Endbenutzer über Formularfelder werden für den Transport von und zur Umgebung der Dienste per TLS verschlüsselt. Diese TLS-Verschlüsselung ist nicht optional, sondern wird vom System erzwungen (globale HTTP > HTTPS Umleitung)

2.10. Der Zugang zu den administrativen Bereichen der Dienste (service admin) ist uneingeschränkt öffentlich (kein IP blocking etc.), unterliegt jedoch einer integrierten Benutzerauthentifizierung. Dabei wird die Integrität durch eine Ein-Faktor-Authentifizierung (Benutzername und Kennwort) gewährleistet.

2.11. Die Benutzereingaben zu den administrativen Bereichen der Dienste (service admin) werden für den Transport von und zur admin-Umgebung der Dienste,,per TLS verschlüsselt. Diese TLS-Verschlüsselung ist nicht optional, sondern wird vom System erzwungen (globale HTTP > HTTPS Umleitung).

2.12. Die Benutzerauthentifizierung verhindert proaktiv das systematische Ausprobieren der Kennwörter (Brute-Force-Angriff)

2.13. Passwörter werden per Hashverfahren geschützt gespeichert.

2.14. Das Authentifizierungs-/Autorisierungs-Modul veranlasst nach außen hin bei Nichtaktivität eine automatische Unterbrechung der Verbindung nach 20 Minuten.

3. Zugriffskontrolle

3.1. Administratoren

- Die PAGENTUS SYSTEMS-Administratoren haben Zugriff auf das gesamte System.
- Die PAGENTUS SYSTEMS-Administratoren genießen das Vertrauen von PAGENTUS SYSTEMS. Ihre Verhaltensweise ist von Selbstdisziplin und Verantwortungsbewusstsein geprägt.
- Administratoren sind Personen mit besonderen Zugriffsmöglichkeiten zu allen Ressourcen der Datenverarbeitung. Sie stehen immer im Spannungsfeld zwischen den Handlungen, die ihnen möglich wären, und dem, was sie tun dürfen und müssen.

3.2. service admin

- Der Zugriff auf die administrativen Bereichen der Dienste erfolgt zum einen über „technische Accounts“ für die Administration durch die PAGENTUS SYSTEMS und zum anderen über sogenannte „OrganisationManager, ThemenManager und MediaManager“.
- In allen Fällen sorgt das integrierte Rechte/Rollen-System für die Gewährleistung des internen Berechtigungskonzeptes der Dienste.

3.3. Zeitliches Sicherheitsmanagement

- Das Authentifizierungs-/Autorisierung-Modul veranlasst nach außen hin bei Nichtaktivität eine automatische Unterbrechung der Verbindung nach 20 Minuten.

4. Gewährleistung, dass Daten bei der Übermittlung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können

4.1. PAGENTUS SYSTEMS stellt dies durch eine zertifizierte TLS-Verbindung (HTTPS) sicher (s.o.). Sobald diese Verbindung durch eine korrekte Authentifizierung des Benutzers (übereinstimmende Benutzererkennung und Passwort) etabliert wurde, ist es nur dem eingeloggten (befugten) Benutzer möglich, die Daten zu sehen.

5. Weitergabekontrolle

5.1. PAGENTUS SYSTEMS gewährleistet die Eingabekontrolle, d.h., dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch folgende Maßnahmen:

- Es laufen Protokolle, die alle Programmaufrufe dokumentieren (wer sich wann und wie oft eingeloggt hat), und die es ermöglichen zu überprüfen, ob und welche Dateneingaben, Datenbewegungen erfolgt sind.
- Jeder Zugriff (wer, wann, wie oft etc.) und jede Veränderung der Datenbank werden durch ein systemeigenes **Audit** mitgeloggt. Diese Daten werden in der Datenbank abgelegt.

6. Eingabekontrolle

6.1. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

6.2. PAGENTUS SYSTEMS kann dies feststellen, da grundsätzlich protokolliert wird, welche Daten wann geändert wurden, wie auch systemintern mitgeloggt wird, wer zuletzt welche Daten geändert hat.

7. Auftragskontrolle

7.1. Die Auftragskontrolle bedeutet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden dürfen.

7.2. Dies wird von PAGENTUS SYSTEMS dadurch gewährleistet, dass aufgrund eines Berechtigungssystems nur Berechtigte zugreifen können.

7.3. Zugriffe auf die Datenbanken **der Dienste** erfolgen ausschließlich aus den dafür erstellten Programmen heraus. Ausnahmen bestehen in äußerst selten vorkommenden Korrektureingriffen durch Administratoren von PAGENTUS SYSTEMS zum Zwecke der Datenbankverwaltung und -wartung.

7.4. Ausschließlichkeit: Es erhalten nur ausdrücklich Berechtigte Zugriff zu den Datenbanken der Dienste. Durch diese strikte Trennung wird sichergestellt, dass auf die Daten nicht zugegriffen werden kann, um sie weiterzuverarbeiten.

7.5. Eine Neuentwicklung oder Programmänderung im Authentifikations- / Autorisierungsmodul erfolgt stets nur bei Vorliegen eines schriftlichen Auftrages in Form eines Online-Ticketsystems, dessen Gültigkeit durch den Projektleiter bestätigt werden muss. Diese Aufträge werden ohne zeitliche Beschränkung aufbewahrt.

7.6. Gewährleistung, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

8. Verfügbarkeitskontrolle / Datensicherung

8.1. Die Datenbanken werden täglich über eine spezielle Schnittstelle für ein Online-Backup komplett gesichert, d.h., sie müssen nicht heruntergefahren werden, um die Daten konsistent zu sichern.

8.2. Die Backups der Datenbanken werden 14 Tage vorgehalten.

8.3. Nur die PAGENTUS SYSTEMS-Systemadministratoren sind befugt, aus den Sicherungen zerstörte Dateiinhalte wiederherzustellen. Die Rekonstruktion kann nur in den Administrationskennungen ausgeführt werden. In dieser Kennung wird die Recovery-Funktion der Sicherungssoftware benutzt, in der auch die richtigen Datenträger benannt werden.

8.4. Die PAGENTUS SYSTEMS-Systemadministratoren führen solche Arbeiten in Eigenverantwortung aus.

8.5. Die benutzereigenen Artefakte, welche per upload durch die Benutzer selbst dem System hinzugefügt wurden, werden täglich über eine spezielle Schnittstelle komplett gesichert.

8.6. Diese Backups der Benutzerartefakte werden ebenfalls 14 Tage vorgehalten.

8.7. Nur die PAGENTUS SYSTEMS-Systemadministratoren sind befugt, aus diesen Sicherungen zerstörte Dateiinhalte wiederherzustellen. Die Rekonstruktion kann nur in den Administrationskennungen ausgeführt werden.

9. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden

9.1. Auf allen Ebenen findet eine strikte Trennung zwischen Produktiv-, Konsolidierungs- und Testsystemen statt.

9.2. Innerhalb der Anwendung der Dienste sind die verschiedenen Datenbereiche logisch voneinander getrennt

9.3. Zum anderen werden separat von der Benutzerverwaltung in der Prozessdatenverwaltung die Login-Daten und die Protokollierungen festgehalten. Es findet keine Weitergabe an Dritte oder sonstige Datenverarbeitung statt. PAGENTUS SYSTEMS speichert die Daten ausschließlich zur Erfüllung seiner vertraglichen Verpflichtungen gegenüber dem Verantwortlichen.

II. Technische und organisatorische Maßnahmen bei der PAGENTUS SYSTEMS

- Die PAGENTUS SYSTEMS verarbeitet keine personenbezogene Daten aus den Datenverarbeitungsprozessen bzgl. der Dienste,unmittelbar auf den IT-System der PAGENTUS SYSTEMS in Mertert, Luxemburg.

- Allerdings werden Daten, die zu Abrechnungszwecken notwendig sind auch unmittelbar auf IT-Systemen der PAGENTUS SYSTEMS in Mertert, Luxemburg verarbeitet und gespeichert.

- Zudem administrieren die PAGENTUS SYSTEMS Systemadministratoren die AWS-Services von dem Firmensitz der PAGENTUS SYSTEMS in Mertert, Luxemburg.

- Die technischen und organisatorischen Maßnehmen betreffend die am Firmensitz in Mertert, Luxemburg vorgehaltenen IT-Systeme werden nachfolgend dargestellt:

1. Zutrittskontrolle

Um die Zutrittskontrolle zu gewährleisten und Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, sind folgende Maßnahmen getroffen worden:

1.1. Der unbediente Teil der Maschinen wie Server, Netzelemente, Plattensubsysteme und Bandstationen sind in einem in einem nicht öffentlich zugänglichen, eigens dafür hergerichteten Raum untergebracht, dem **Serverraum.** Ausschließlich Zutritt zu diesem-gesicherten Raum haben nur Administratoren, die als einzige - abgesehen von der Geschäftsführung - einen Schlüssel zu diesem Raum besitzen.

1.2. Die ausgegebenen Schlüsse! sind in einem Schlüsselbuch vermerkt. Sie bleiben auch außerhalb der Dienstzeit bei ihren Empfängern.

1.3. Der Serverraum ist von der übrigen Büroumgebung getrennt. Im Serverraum halten sich grundsätzlich keine Menschen auf. Wenn dies zu Wartungsarbeiten erforderlich sein sollte, so sind dies nur die berechtigten Administratoren und externe Dienstleister, die unter Aufsicht Wartung an Elektrik und Klimaanlage durchführen.

1.4. Der Serverraum ist klimatisiert. Bei der redundant ausgelegten **Klimaanlage** handelt es sich um Systeme mit geschlossenem Kühlmittelkreislauf.

1.5. Die Klimawerte werden unabhängig von der Klimaanlage überwacht. Bei Über- und Unterschreiten vorgegebener Grenzen werden automatisch E-Mail- und SMS-Benachrichtigungen an die Systemadministratoren gesendet und in Abhängigkeit der Schwere der Abweichung die Serversysteme ordnungsgemäß heruntergefahren.

1.6. Der Eingangsbereich des Gebäudes wird außerhalb der Bürozeiten durch eine **Kamera** überwacht. Die Überwachung erfolgt von 18.00 Uhr bis 6.00 Uhr und ist durch integrierte Bewegungsmelder realisiert.

1.7. Die **Reinigung** der Betriebsräume wird nur von eigenem Personal vorgenommen. Während der Reinigung können keine vertraulichen Unterlagen eingesehen werden, da diese verschlossen verwahrt werden.

1.8. Der verschlossene Serverraum kann nur in **Begleitung** eines Befugten betreten werden. Daher wird dieser Raum bei Bedarf stets nur unter Aufsicht gereinigt.

2. Zugangskontrolle

2.1. Um die Zugangskontrolle zu gewährleisten und Unbefugten die Nutzung der Datenverarbeitungsanlagen zu verwehren, sind folgende Maßnahmen getroffen worden:

2.2. Benutzer-Authentifikation im internen Netzwerk

- Die Authentifizierung der Netzwerkbenutzer erfolgt über eine zentrale Benutzerverwaltung.
- Eine Benutzung der IT-Systeme ist nur nach erfolgreicher Authentifikation und Autorisation an der zentralen Benutzerverwaltung möglich. .
- Eine Passwortrichtlinie erzwingt komplexe Passwörter sowie den regelmäßigen Passwortwechsel.
- Bei wiederholter Fehleingabe erfolgt eine Sperrung, welche nur durch die Systemadministratoren aufgehoben werden kann.
- Gruppenkennungen sind im Umfeld des Benutzerkontextes nicht zulässig.

- Eine Passwortweitergabe innerhalb der Mitarbeiter ist ausdrücklich untersagt.
- Eine Sperrung ausgeschiedener Mitarbeiter erfolgt unverzüglich.

2.3. Virenschutz

- Der Virenschutz wird zentral und intern von den Administratoren verwaltet.
- Die Ausbringung der lokalen Antiviren-Software sowie Updates und Kontrolle der definierten Regeln erfolgen hierbei automatisiert.
- Benutzer sind nicht in der Lage, die lokalen Virenschutz-Einstellungen zu ändern

2.4. Serversysteme

- Die Serversysteme werden ausschließlich vom eigenen Personal konfiguriert und gepflegt.
- Administrationsaufgaben, wie z.B. die der System-, Netz- und Datenbankverwaltung, sowie der Verwaltung und Anpassung sonstiger Software-Produkte werden von den Administratoren wahrgenommen.
- Die Kennungen der Administratoren, denen besonders weit gefasste Berechtigungen zugebilligt werden, sind analog der Benutzer durch Benutzernamen und Passworte geschützt.

2.5. Internet

- Der Zugang zum Internet ist mit einem „Unified Threat Management"-System (kurz: UTM) gesichert.
- Der Zugang zum Internet erfolgt ausschließlich über das UTM-System.

2.6. UTM

- Die Administration des UTM-Systems obliegt ausschließlich den Administratoren.
- Eine Überprüfung auf neueste Patches und Updates erfolgt täglich. Neue Patches und Updates werden nach einer internen Risikobewertung und sofern es die betrieblichen Belange zulassen, zügig installiert.
- Die Überprüfung auf neueste Virendefinitionen erfolgt 15-minütig und diese werden, sofern vorhanden, umgehend automatisch aktualisiert.
- Neben der aktiven Durchsetzung der Regeln zur Netzwerknutzung und dem Schutz der internen Benutzer und Systeme durch Webfilter sowie Viren- und Spamschutz, findet zum Schutz gegen Angriffe auf die IT-Infrastruktur und die Daten - von innen wie von außen- auch eine proaktive Überwachung des ein- und ausgehenden Datenverkehrs mit Hilfe eines IPS-Systems statt.

3. Zugriffskontrolle

3.1. Administratoren

- Die Administratoren haben Zugriff auf das gesamte System.
- Die Administratoren genießen, wie auch in anderen Unternehmen einen hohen Vertrauensvorschuss. Ihre Verhaltensweisen werden von Selbstdisziplin und Verantwortungsbewusstsein geprägt.
- Administratoren sind Personen mit besonderen Zugriffsmöglichkeiten zu allen Ressourcen der Datenverarbeitung. Sie stehen immer im Spannungsfeld zwischen den Handlungen, die ihnen möglich wären, und dem, was sie tun dürfen und müssen.
- Mit der Kenntnis des Benutzernamens und des Passwortes eines Administrators stehen ihm alle Systemressourcen offen. Er hat eine nahezu unbeschränkte Eindringtiefe in das jeweilige System und in die Anwendungen. Damit kann er alle Anwendungspassworte, die Berechtigungstabellen, die individuellen Rechte und Verbote einsehen und auch verändern. Er kann sämtliche systemeigenen Schutzrechte umgehen und auf alles zugreifen, was möglicherweise als Verursacher eines Fehlers auftreten könnte. Er kann neue Benutzer einrichten und ihnen Rechte erteilen, vorhandene Benutzer löschen oder ihre Berechtigungen ganz oder teilweise sperren. Er kann ihre Systempassworte zwar in den meisten Systemen nicht lesen, wohl aber löschen und neue zuweisen. Alle diese Tätigkeiten muss er ausführen können, um bei Systemfehlern reagieren zu können, um aus dem System die höchstmögliche Leistung herauszuholen und um die Nutzer auf die ihnen erlaubte Ausbreitung im System einzuschränken.
- Aufgrund dieser Funktionsvielfalt ist ihm das System im oben erwähnten Umfang geöffnet und die hohe Eindringtiefe ermöglicht.

3.2. Benutzer

- Die Benutzerzugriffe auf Datei-, Applikations- und Datenbanksysteme sowie der HTTP/S-basierte Internetzugriff unterliegen in allen Bereichen einer von den Administratoren zentral oder dem jeweiligen System zugeordneten Rechte/Rollen-Prüfung.

4. Weitergabekontrolle

4.1. Der manuelle Datenaustausch für den Zweck der internen Verwaltung und Buchhaltung (Rechnungsstellung) zwischen den Dienste und der PAGENTUS SYSTEMS findet ausschließlich über TLS-verschlüsselte Zugriffe statt.

5. Eingabekontrolle

5.1. Der manuelle Datenaustausch für den Zweck der internen Verwaltung und Buchhaltung (Rechnungsstellung) zwischen den Diensten und der PAGENTUS SYSTEMS, wird zum einen in den Diensten,,selbst (siehe TOMs der Dienste), als auch über die zentrale UTM und auf dem Zielsystem der lokalen internen Verwaltung und Buchhaltung protokolliert.

6. Auftragskontrolle

6.1. Die **Auftragskontrolle** bedeutet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden dürfen.

6.2. Dies wird bei der **PAGENTUS SYSTEMS** dadurch gewährleistet, dass nur Berechtigte zugreifen können.

6.3. Ausschließlichkeit: Es erhalten nur ausdrücklich Berechtigte Zugriff zu den Daten. Durch diese strikte Trennung wird sichergestellt, dass auf die Daten nicht zugegriffen werden kann um sie weiterzuverarbeiten.

6.4. Weisungen werden grundsätzlich schriftlich erteilt. In Ausnahmefällen können die bevollmächtigten Personen Weisungen auch mündlich erteilen, wobei eine schriftliche Bestätigung erfolgen muss.

6.5. Gewährleistung, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

7. Verfügbarkeitskontrolle / Datensicherung

7.1. Alle Daten werden in einem einheitlich festgelegten Konzept gesichert. Es ist schriftlich fixiert. Für die Datensicherung steht ein dedizierter Sicherungsserver zur Verfügung.

7.2. Alle Daten werden täglich über eine spezielle Schnittstelle für ein Online-Backup komplett gesichert.

7.3. Alle Backups sind mit dem AES-Verfahren verschlüsselt.

7.4. Nur die Systemadministratoren sind befugt, aus den Sicherungen zerstörte Dateiinhalte wiederherzustellen. Die Rekonstruktion kann nur in den Administrationskennungen ausgeführt werden. In dieser Kennung wird die Recovery-Funktion der Sicherungssoftware benutzt, in der auch die richtigen Datenträger benannt werden. Zur späteren Kontrolle wird ein Zwangsprotokoll durch die Sicherungssoftware erstellt und archiviert.

7.5. Die Systemadministratoren führen solche Arbeiten in Eigenverantwortung aus.

7.6. Die Sicherungsdatenträger werden intern und zur weiteren Absicherung zusätzlich extern verschlossen aufbewahrt. Die Schlüssel werden durch die Administratoren verwahrt.

8. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden

8.1. Die verschiedenen Datenbereiche sind logisch voneinander getrennt

8.2. Die Benutzerverwaltung (Stammdaten) ist von der Prozessdatenverwaltung getrennt. Zum einen ist die Benutzerverwaltung in Ihrer Struktur so aufgebaut, dass hierarchisch unterschieden wird zwischen Kunden-, Auftrags- und Nutzerverwaltung. Dabei sind die verschiedenen Datensätze strikt voneinander getrennt.

8.3. Es findet keine Weitergabe an Dritte oder sonstige Datenverarbeitung statt. Die **PAGENTUS SYSTEMS** speichert die Daten ausschließlich zur Erfüllung ihrer vertraglichen Verpflichtungen gegenüber dem Verantwortlichen.

III. Technische und organisatorische Maßnahmen der Amazon Web Services

- Die technischen und organisatorischen Maßnahmen zur Absicherung der Cloud-Laufzeitumgebung der Amazon Web Services werden ständig verbessert. Nachfolgend sind die technischen und organisatorischen Maßnahmen von Amazon Web Services abgebildet. Die nachfolgende Beschreibung ist ein Auszug aus dem Auftragsdatenverarbeitungsvertrag zwischen der PAGENTUS SYSTEMS und Amazon Web Services, Inc:

AWS Security Standards

1. **Information Security Program.** AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the AWS Network, and (c) minimize security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

   1.1 **Network Security.** The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

   1.2 **Physical Security**

      1.2.1 **Physical Access Controls.** Physical components of the AWS Network are housed in nondescript facilities (the "**Facilities**"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

      1.2.2 **Limited Employee and Contractor Access.** AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

      1.2.3 **Physical Security Protections.** All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. **Continued Evaluation.** AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.