Auftragsverarbeitungsvertrag

zwischen

Relias Learning GmbH, Luisenstr. 46, 10117 Berlin

Auftragnehmer –

und

der auf app.pflegeclever.de registrierten Einrichtung

Auftraggeber –

1. Präambel

(1) Der Auftraggeber hat sich auf der Website des Auftragnehmers online für die Nutzung dessen Online-Schulungsangebotes „Relias Care“ registriert (im Folgenden die „**Vereinbarung**“ genannt). Relias Care ist eine intuitive Lernplattform zur Administration, Durchführung und Dokumentation von Online-Kursen. Die Kursbibliothek von Relias Care enthält eine Vielzahl an Pflichtfortbildungen, Expertenstandards und weiteren Fachfortbildungen und kann nach Registrierung durch den Auftraggeber eigenständig betrieben werden.

(2) Über „Relias Care“ ermöglicht der Auftragnehmer Dritten wie dem Auftraggeber, Online-Schulungskurse im Bereich der Pflege zu buchen, zu absolvieren und im Falle des erfolgreichen Abschlusses Zertifikate zu erhalten.

(3) Mit Abschluss der Vereinbarung beauftragt der Auftraggeber den Auftragnehmer als Auftragsverarbeiter mit der Verarbeitung von personenbezogenen Daten des Auftraggebers. Dieser Auftragsverarbeitungsvertrag (im Folgenden „**AV-Vertrag**“) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien unter Berücksichtigung der Anforderungen nach Art. 28 der DS-GVO. Er findet Anwendung auf alle Tätigkeiten, die mit der Vereinbarung im Zusammenhang stehen und bei denen durch den Auftragnehmer eingesetzte Personen personenbezogene Daten des Auftraggebers verarbeiten.

2. Begriffsbestimmungen

Die in diesem AV-Vertrag verwendeten Begriffe wie z.B. „**personenbezogene Daten**“, „**Verarbeitung“,** „**Verantwortlicher**“, „**Auftragsverarbeiter**“ oder „**betroffene Person**“ entsprechen den Begriffsbestimmungen der DS-GVO, soweit in diesem AV-Vertrag keine anderweitigen Definitionen enthalten sind. Mit „**Daten des Auftraggebers**“ sind ausschließlich solche personenbezogenen Daten gemeint, die im Zusammenhang mit der Vereinbarung entweder dem Auftragnehmer vom Auftraggeber überlassen oder vom Auftragnehmer ausschließlich für den Auftraggeber in dessen Auftrag erhoben wurden.

3. Gegenstand und Dauer der Verarbeitung; Art, Zweck und Mittel der Verarbeitung; Art der personenbezogenen Daten sowie Kategorien betroffener Personen

(1) Der Gegenstand und die Dauer der Verarbeitung, die Art, der Zweck und die Mittel der Verarbeitung sowie die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen sind in **Anhang 1** dieses AV-Vertrags niedergelegt.

(2) Der Auftragnehmer ist im Rahmen der Erfüllung des Auftragsgegenstandes unter Einhaltung der Bestimmungen dieses AV-Vertrags zur Durchführung aller erforderlichen Verarbeitungsschritte hinsichtlich der Daten des Auftraggebers (z.B. Duplizieren von Beständen für die Verlustsicherung, Anlegen von Logfiles, Zwischendateien und Arbeitsbereichen) berechtigt, soweit dies nicht zu einer inhaltlichen Umgestaltung der Daten des Auftraggebers führt.

4. Weisungsgebundenheit des Auftragnehmers

(1) Der Auftragnehmer darf die Daten des Auftraggebers nur im Rahmen dieses AV-Vertrags und der Weisungen des Auftraggebers – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation - verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen schriftlich oder per E-Mail (Textform) mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Weisungen sind die auf eine bestimmte Verarbeitung der Daten des Auftraggebers durch den Auftragnehmer gerichteten, dokumentierten Anordnungen des Auftraggebers. Sie werden anfänglich durch diesen AV-Vertrag festgelegt und können vom Auftraggeber danach durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden (Einzelweisung).

(3) Die Weisungen des Auftraggebers sind grundsätzlich in Textform zu erteilen; im Ausnahmefall erforderliche mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen. Weisungsberechtigte Personen auf Seiten des Auftraggebers und empfangsberechtigte Personen auf Seiten des Auftragnehmers werden der jeweils anderen Partei mitgeteilt. Die jeweilige Partei wird die andere Partei unverzüglich über einen Wechsel dieser Person informieren.

(4) Es besteht keine materiell-rechtliche Prüfpflicht seitens des Auftragnehmers in Hinblick auf vom Auftraggeber erteilte Weisungen. Ist der Auftragnehmer jedoch der Auffassung, dass eine Weisung des Auftraggebers gegen die DS-GVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt, informiert er den Auftraggeber unverzüglich. Der Auftragnehmer ist berechtigt, die Durchführung der vereinbarten Tätigkeit so lange auszusetzen, bis der Auftraggeber über das weitere Vorgehen entschieden hat. Der Auftraggeber trägt die alleinige Verantwortung für die vom ihm getroffene Entscheidung. Hält der Auftraggeber an der erteilten Weisung fest und verlangt deren Umsetzung aus Sicht des Auftragnehmers ihm ein rechtswidriges Handeln ab, ist der Auftragnehmer berechtigt, (i) die entsprechende Verarbeitung von der Stellung einer Sicherheit durch den Auftraggeber (z.B. Bürgschaft) abhängig zu machen, (ii) eine Entscheidung der zuständigen Aufsichtsbehörde einzuholen oder (iii) die Verarbeitung nicht durchzuführen.

5. Pflichten des Auftragnehmers

(1) Der Auftragnehmer wird in seinem Verantwortungsbereich technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit dieser Auftragsverarbeitung auf Dauer sicherstellen sowie die Fähigkeit haben, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Die

vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sind in **Anhang 2** niedergelegt (im Folgenden „**technische und organisatorische Maßnahmen**"). Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt. Er trägt die alleinige Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden personenbezogenen Daten ein angemessenes Schutzniveau bieten.

(2) Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das im **Anhang 2** niedergelegte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer hat ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung etabliert.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, diese außerhalb der vereinbarten Weisungen zu verarbeiten. Der Auftragnehmer gewährleistet ferner, dass sich die von ihm zur Verarbeitung der Daten des Auftraggebers eingesetzten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Verpflichtung besteht auch nach Beendigung des Auftrags fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der Daten des Auftraggebers bekannt werden. Der Auftragnehmer kann nach eigenem Ermessen in seinem Verantwortungsbereich angemessene Maßnahmen zur Sicherung der Daten des Auftraggebers und zur Minderung möglicher nachteiliger Folgen treffen. Der Auftragnehmer informiert den Auftraggeber über etwaige von ihm getroffene Maßnahmen.

(6) Der Ansprechpartner beim Auftragnehmer für im Rahmen des AV-Vertrags anfallende Datenschutzfragen ist in **Anhang 1** benannt. Der Auftragnehmer wird den Auftraggeber über einen Wechsel des Ansprechpartners unverzüglich in Textform informieren.

(7) Sofern der Auftragnehmer gemäß **Anhang 1** ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DS-GVO führt, ist er befugt, dass diesen AV-Vertrag betreffende Verzeichnis einer Aufsichtsbehörde auf deren Anfrage zur Verfügung zu stellen bzw. kann der Auftraggeber dieses Verzeichnis beim Auftragnehmer anfordern, sofern eine Aufsichtsbehörde dies von ihm verlangt.

(8) Der Auftraggeber ist für die Erfüllung der in den Artikeln 32 bis 36 DS-GVO geregelten Pflichten verantwortlich. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der dort genannten Pflichten.

(9) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten allein beim Auftraggeber liegen.

6. Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO und damit Herr der Daten. Er ist im Rahmen dieses AV-Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Der Ansprechpartner beim Auftraggeber für im Rahmen des AV-Vertrags anfallende Datenschutzfragen ist in **Anhang 1** benannt. Der Auftraggeber wird den Auftragnehmer über einen Wechsel des Ansprechpartners unverzüglich in Textform informieren.

(4) Der Auftraggeber wird dem Auftragnehmer alle Informationen zur Verfügung stellen, die der Auftragnehmer zum Führen des Verzeichnisses nach Art. 30 Abs. 2 DS-GVO benötigt.

(5) Dem Auftraggeber obliegen die Evaluierung und Bewertung der Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(6) Im Fall einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO verpflichtet sich der Auftraggeber, den Auftragnehmer bei der Abwehr der Ansprüche zu unterstützen. Der Auftragnehmer ist in diesem Zusammenhang berechtigt, Details des AV-Vertrages, der Datenverarbeitung und von Weisungen des Auftraggebers zum Zwecke der Abwehr dieser Ansprüche oder zur Exkulpation nach Art. 82 Abs. 3 DS-GVO gegenüber Dritten offenzulegen.

(7) Über die Aufbewahrung, Herausgabe oder Löschung der Daten des Auftraggebers nach Beendigung der Vereinbarung (vgl. Ziffer 10 dieses AV-Vertrages) muss der Auftraggeber innerhalb einer vom Auftragnehmer gesetzten angemessenen Frist entscheiden. Geht dem Auftragnehmer innerhalb dieser Frist keine Entscheidung zu, ist der Auftragnehmer zur Löschung dieser Daten berechtigt, soweit keine rechtlichen Verpflichtungen des Auftragnehmers zur Aufbewahrung dieser Daten bestehen.

7. Wahrung von Betroffenenrechten

(1) Hinsichtlich dieses AV-Vertrags ist der Auftraggeber für die Wahrung der nach Kapitel III der DS-GVO vorgesehenen Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber im Rahmen seiner Möglichkeiten mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner diesbezüglichen Verpflichtungen unterstützen.

(2) Wendet sich ein Betroffener mit der Geltendmachung von in der DS-GVO geregelten datenschutzrechtlichen Betroffenenrechten (beispielsweise Forderungen zur Datenportabilität, Berichtigung, Löschung oder Auskunft) an den Auftragnehmer, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen, sofern eine Zuordnung der Betroffenenanfrage an den Auftraggeber nach den Angaben des Betroffenen möglich ist.

8. Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Auftragnehmer ist nach Maßgabe, der in **Anhang 1** getroffenen Regelungen berechtigt, Subunternehmer als weitere Auftragsverarbeiter einzusetzen. Der Auftragnehmer wird die vertraglichen Vereinbarungen mit dem Subunternehmer so gestalten, dass dem Subunternehmer dieselben datenschutzrechtlichen Verpflichtungen auferlegt werden, die in diesem AV-Vertrag in Bezug auf den Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und

Datensicherheit. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten.

(2) Subunternehmer des Auftragnehmers sind zum Zeitpunkt des Abschlusses dieses AV-Vertrages die folgenden Unternehmen:

a) Mailjet GmbH, Alt-Moabit 2, 10557 Berlin, Deutschland (Versendung systeminterner Emails und Erbringung sonstiger E-Mail-Dienstleistungen);

b) IONOS SE, Elgendorfer Str. 57, 56410 Montabaur, Deutschland (Hosting der Applikation)

c) PAYONE GmbH Lyoner Straße 9, 60528 Frankfurt am Main, Deutschland (Zahlungsabwicklung und Handhabung von Zahlungen)

Zwischen den in diesem Absatz 2 genannten Unternehmen und dem Auftragnehmer besteht jeweils ein Auftragsverarbeitungsvertrag, aufgrund dessen sich der jeweilige Subunternehmer zur Einhaltung der Bestimmungen der DS-GVO und insbesondere dazu verpflichtet, personenbezogene Daten ausschließlich zur Erfüllung seiner Verpflichtungen gegenüber dem Auftragnehmer zu verwenden.

(3) Der Auftragnehmer ist berechtigt, die in Absatz 2 genannte Liste der Subunternehmer von Zeit zu Zeit anzupassen und wird etwaige Änderungen auf seiner Website bekanntgeben.

(4) Kommt ein Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Subunternehmers wie für eigenes Verschulden.

9. Nachweise des Auftragnehmers, Inspektionen

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem AV-Vertrag niedergelegten Pflichten wie in **Anhang 1** beschrieben nach und stellt dem Auftraggeber die hierfür erforderlichen Informationen zur Verfügung.

(2) Sollten im Einzelfall datenschutzrechtlich gebotene Inspektionen oder Überprüfungen durch den Auftraggeber oder einen von diesem beauftragten unabhängigen externen Prüfer, dessen Namen dem Auftragnehmer rechtzeitig im Voraus mitgeteilt wird, erforderlich sein (z.B. wenn der Auftraggeber begründete Zweifel an einem vom Auftragnehmer vorgelegten Selbstaudit hat), werden diese zu den üblichen Geschäftszeiten sowie ohne Störung des Betriebsablaufs in der Betriebsstätte des Auftragnehmers nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zum Auftragnehmer oder dessen Subunternehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(3) Der Auftraggeber stellt dem Auftragnehmer eine Kopie des Auditberichts zur weiteren Verwendung zur Verfügung.

(4) Der Auftragnehmer hat hinsichtlich schriftlicher Anfragen des Auftraggebers im gewöhnlichen Geschäftsverkehr keinen Anspruch auf Zahlung einer Vergütung. Das Recht des Auftraggebers zur Inspektion bzw. Überprüfung gemäß vorstehenden Absatz 2 ist auf einen Tag pro Kalenderjahr begrenzt; Abweichungen sind mit dem Auftragnehmer in Textform zu vereinbaren.

10. Rückgabe und Löschung von Daten bei Vertragsbeendigung

(1) Nach Beendigung der Vereinbarung wird der Auftragnehmer, sofern technisch möglich und vom Auftraggeber gemäß Ziffer 6 Abs. 7 gewünscht, die Daten des Auftraggebers herausgeben. Elektronisch gespeicherte Daten sind auf Wunsch und auf Kosten des Auftraggebers entweder in einem marktüblichen Format auf Datenträgern herauszugeben, wobei der Auftraggeber das Versandrisiko trägt, oder verschlüsselt online zu übertragen, wobei der Auftraggeber das Übermittlungsrisiko trägt.

(2) Der Auftragnehmer wird sämtliche elektronisch gespeicherten Daten des Auftraggebers gemäß der in **Anhang 1** definierten Prozesse löschen oder im Fall von Backups oder Logfiles eine Beschränkung der Datenverarbeitung bis zum Zeitpunkt der Löschung sicherstellen. Der Auftragnehmer wird dem Auftraggeber die Löschung in Textform bestätigen.

(3) Daten des Auftraggebers, die nicht in elektronischer Form gespeichert sind (z.B. Daten auf CDs, papierhafte Unterlagen) und von denen der Auftraggeber keine Herausgabe gemäß Absatz 1 wünscht, werden durch den Auftragnehmer datenschutzkonform vernichtet.

(4) Die Verpflichtung zur Herausgabe oder Löschung gemäß dieser Ziffer 10 besteht nicht, wenn der Auftragnehmer nach dem Unionsrecht oder dem Recht des Mitgliedstaates, dem der Auftragnehmer unterliegt, zur Aufbewahrung oder sonst zur Speicherung dieser Daten verpflichtet ist.

(5) Sofern der Auftraggeber eine Aufbewahrung seiner Daten über das Vertragsende hinaus wünscht, bedarf dies einer gesonderten Vereinbarung zwischen den Parteien.

11. Kontrollrechte von Aufsichtsbehörden oder sonstiger hoheitlicher Aufsichtsbehörden des Auftraggebers; Kooperation mit Aufsichtsbehörden

(1) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion bei dem Auftragnehmer vornehmen, gelten grundsätzlich Ziffer 9 Abs. 2 und Abs. 4 Satz 1 des AV-Vertrags entsprechend. Eine Unterzeichnung der Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

(2) Die Vertragsparteien werden sich wechselseitig über sämtliche behördliche Anfragen/Anordnungen und Verfahren sowie sämtliche drohenden oder laufenden gerichtlichen Verfahren, die die in diesem AV-Vertrag geregelte Zusammenarbeit zum Gegenstand haben, unverzüglich informieren, im Zusammenhang mit diesen Anfragen, Anordnungen oder Verfahren eng zusammenarbeiten und sich wechselseitig alle erforderlichen Unterlagen und Angaben zur Verfügung stellen. Jede Partei ist berechtigt, sämtliche diesen AV-Vertrag, einschließlich der Details der Datenverarbeitung, betreffende Informationen und Unterlagen gegenüber der für sie zuständigen Aufsichtsbehörde offenzulegen, soweit dies aus Sicht der Partei erforderlich ist.

12. Schlussbestimmungen

(1) Im Fall eines Widerspruchs zwischen der Vereinbarung und dem AV-Vertrag gehen die Regelungen dieses AV-Vertrags vor. Sofern in diesem AV-Vertrag keine abweichenden Abreden getroffen worden sind, gelten die zwischen den Parteien in der -Vereinbarung getroffenen Vereinbarungen. Dies gilt insbesondere für die in der -Vereinbarung getroffenen Kündigungs- und Haftungsregelungen. Sollten einzelne Teile dieses AV-Vertrags unwirksam sein, so berührt dies die Wirksamkeit des AV-Vertrag im Übrigen nicht.

(2) Änderungen und Ergänzungen dieses AV-Vertrags und seiner Bestandteile bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Die Parteien vereinbaren für diesen AV-Vertrag die Geltung deutschen Rechts unter Ausschluss der Regelungen des internationalen Privatrechts. Der ausschließliche Gerichtstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit diesem AV-Vertrag ist im **Anhang 1** niedergelegt

Auftraggeber

Der Auftraggeber bestätigt durch den Abschluss seiner Registrierung für die Nutzung von Relias Care und den Abschluss dieses AV-Vertrages, dass er über sämtliche für die Nutzung von Relias Care durch seine Mitarbeiterinnen und Mitarbeiter und die Erbringung der dem Auftragnehmer nach diesem AV-Vertrag obliegenden Aufgaben und Verpflichtungen erforderlichen Einwilligungen seiner Mitarbeiterinnen und Mitarbeiter, die Relias Care nutzen, verfügt oder die Verarbeitung deren personenbezogener Daten aus anderen Gründen, insbesondere den in Art. 6 DS-GVO genannten, rechtmäßig ist.

Auftragnehmer

Relias Learning GmbH

Berlin,

DocuSigned by:
Adrian Thiessen
C7E650F290BC488...

Adrian Thiessen, Geschäftsführer

DocuSigned by:
Anne Frühauf
556B6B0F833F409...

Anne Frühauf, Prokuristin

ANHANG 1

1. Auftraggeber

Auftraggeber ist die sich auf der Plattform Relias Care registrierende Person.

2. Auftragnehmer

Auftragnehmer ist die Relias Learning GmbH, Luisenstr. 46, 10117 Berlin.

3. Vereinbarung

Vereinbarung bezeichnet die zwischen den vorgenannten Parteien elektronisch abgeschlossene Vereinbarung.

4. Gegenstand der Verarbeitung

Gegenstand der Auftragsverarbeitung sind das Hosting von Online-Kursen im Rahmen der vom Auftragnehmer betriebenen Plattform „Relias Care“ und der hiervon umfassten Daten des Auftraggebers und seiner Mitarbeiterinnen und Mitarbeiter.

5. Dauer der Verarbeitung

Dieser AV-Vertrag tritt zeitgleich mit dem Abschluss der Vereinbarung in Kraft und endet mit Beendigung der Vereinbarung, sofern sich aus den Bestimmungen dieses AV-Vertrages keine zeitlich darüberhinausgehenden Verpflichtungen ergeben. In Ansehung dieser Verpflichtungen besteht dieser AV-Vertrag so lange fort, bis diese erloschen sind. Durch diese Regelung erfolgt keine Modifizierung der in der Vereinbarung vereinbarten Kündigungsrechte.

6. Art, Zweck und Mittel der Verarbeitung

Art der Verarbeitung:

Nachdem der Auftragnehmer die Personenbezogenen Daten erhalten hat, werden die Daten genutzt, um die Zuordnung von über die Plattform „Relias Care“ des Auftragnehmers angebotenen Online-Kursen zu organisieren und Berichte über den Abschluss von Online-Kursen zu erstellen.

Zweck der Verarbeitung:

Speicherung, Übermittlung und ggf. Löschung von seitens des Auftraggebers erhobenen Personenbezogenen Daten der Mitarbeiter des Auftraggebers. Nutzung dieser Daten für Zwecke der Durchführung der über die Plattform „Relias Care“ des Auftragnehmers angebotenen Online-Kurse und der Report-Erstellung.

Mittel der Verarbeitung:

Die Daten werden auf einem von weiteren Auftragsverarbeitern (vgl. Ziffer 8 Abs. 2 und 3 des AV-Vertrages) betriebenen Server gespeichert und auf nach Maßgabe der Bestimmungen von zwischen dem Auftragnehmer und den bestehenden weiteren Auftragsverarbeitern betriebenen Servern verarbeitet.

7. Art der personenbezogenen Daten

Im Rahmen dieses AV-Vertrags werden folgende personenbezogene Daten verarbeitet:

Vertragsdaten für Online-Kurse: Name, Funktion, Abteilung, Standort, E-Mail-Adresse und Berufsbezeichnung des Lerners / Teilnehmers. Dies ist keine abschließende Aufzählung.

8. Kategorien betroffener Personen

Es sind folgende natürliche Personen von dieser Auftragsverarbeitung betroffen:

Diejenigen Mitarbeiter des Auftraggebers und dessen Subunternehmer, die an Online-Kursen teilnehmen

9. Anweisungs-, empfangs- und kontrollberechtigten Personen des Auftraggebers

Soweit vom Auftraggeber nicht ausdrücklich anders angegeben, ist anweisungs-, empfangs- und kontrollberechtigte Person des Auftraggebers diejenige Person, die über die Plattform „Pflegeclever“ die Vereinbarung namens des Auftraggebers in elektronischer Form abgeschlossen hat und deren E-Mail-Adresse hierfür genutzt wurde.

10. Weisungsempfangsberechtigte Personen auf Seiten des Auftragnehmers

Name	Vorname	Anschrift	E-Mail
Frühauf	Anne	Relias Learning GmbH, Luisenstr. 46, 10117 Berlin	afruehauf@relias.de
Dinkler	Maik	Relias Learning GmbH, Bleicherufer 25, 19053 Schwerin	mdinkler@relias.de

11. Ansprechpartner für im Rahmen des Vertrags anfallende Datenschutzfragen auf Seiten des Auftraggebers

Soweit vom Auftraggeber nicht ausdrücklich anders angegeben, ist Ansprechpartner für Datenschutzfragen des Auftraggebers diejenige Person, die über die Plattform „Pflegeclever“ die Vereinbarung namens des Auftraggebers in elektronischer Form abgeschlossen hat und deren E-Mail-Adresse hierfür genutzt wurde.

12. Ansprechpartner für im Rahmen des Vertrags anfallende Datenschutzfragen auf Seiten des Auftragnehmers

Name	Vorname	Telefon	E-Mail
Dannhoff	Martin	05241 807 5562	Martin.Dannhoff@Bertelsmann.de

13. Etwaige Mitteilung des Auftragnehmers in Bezug auf Art. 28 Abs. 3 Nr. a DS-GVO

Keine.

14. Frist nach Ziffer 6 Abs. 7 des AV-Vertrags

Der Auftraggeber muss nach schriftlicher Aufforderung durch den Auftragnehmer innerhalb einer 30-tägigen Frist über die Herausgabe oder Löschung der Daten nach Beendigung der Vereinbarung entscheiden.

15. Verarbeitungsverzeichnis gemäß Art. 30 DS-GVO

Der Auftragnehmer hat ein Verarbeitungsverzeichnis gemäß Art. 30 DS-GVO: ☒ JA ☐ NEIN

16. Beauftragung von Subunternehmern

(1) Der Auftraggeber erteilt mit Unterzeichnung dieses AV-Vertrags seine Einwilligung, dass der Auftragnehmer berechtigt ist, die Ausführungen dieses AV-Vertrags ganz oder teilweise auf Subunternehmer als weitere / Unter-Auftragsverarbeiter zu übertragen; diese Einwilligung umfasst insbesondere die in Absatz 4 genannten Subunternehmer. Vor Hinzuziehung anderer als der in Absatz 4 genannten Subunternehmer oder deren Ersetzung informiert der Auftragnehmer den Auftraggeber, indem er nach seiner Wahl (a) eine unter Punkt 9 genannte Person informiert oder (b) unter der Adresse www.reliaslearning.de eine Liste mit allen jeweils eingesetzten und neu hinzukommenden Subunternehmern veröffentlicht.

(2) Der Auftraggeber kann der Änderung innerhalb einer Frist von 7 Tagen – aus wichtigem datenschutzrechtlichem Grund – gegenüber den vom Auftragnehmer in Ziffer 10 in Anhang 1 benannten Personen widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als erteilt.

(3) Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich, wird beiden Seiten ein außerordentliches Sonderkündigungsrecht eingeräumt.

(4) Rein nachrichtlich informiert der Auftragnehmer den Auftraggeber, dass er zum Zeitpunkt des Vertragsabschlusses folgende Subunternehmer eingeschaltet hat:

Name des Subdienstleisters	Anschrift	Beschreibung der Teilleistung
PAYONE GmbH	Lyoner Straße 9, 60528 Frankfurt am Main	Zahlungsabwicklung und Handhabung von Zahlungen
Mailjet GmbH	Alt-Moabit 2, 10557 Berlin	Erbringung von E-Mail-Dienstleistungen, insbesondere Versand systeminterner Mails
Ionos SE	Elgendorfer Str. 57, 56410 Montabaur	Hosting der Applikation

17. Nachweise des Auftragnehmers gem. Ziffer 9 des AV-Vertrags

Der Auftragnehmer führt in regelmäßigen Abständen ein Selbstaudit oder Self-Assessment bezüglich der Einhaltung der in diesem AV-Vertrag niedergelegten Pflichten durch.

18. Löschung

Gemäß Ziffer 10 Abs. 2 des AV-Vertrags gestaltet sich der Prozess der Löschung elektronisch gespeicherter Daten wie folgt: Sollten Sie sich entschließen, das Abonnement mit Relias-Care nach Ablauf der 30-tägigen Testphase oder zu einem späteren Zeitpunkt zu kündigen, werden Ihre Daten nach Ablauf Ihre Abonnements automatisiert und mit einer Frist von 90 Tagen von den Systemen des Auftraggebers und denen der beauftragten Subunternehmer vollständig gelöscht.

Alle Speicheroperationen einschließlich Löschen sind so konzipiert, dass sie sofort konsistent sind. Die erfolgreiche Ausführung eines Löschvorgangs entfernt alle Verweise auf das zugehörige Datenelement.

Die physikalischen Bits werden überschrieben, wenn der zugehörige Speicherblock zur Speicherung anderer Daten wiederverwendet wird, wie es bei Standard-Computer-Festplatten typisch ist.

ANHANG 2

Beschreibung der zwischen den Parteien vereinbarten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers nach Art. 32 DS-GVO.

Durch die technischen und organisatorischen Maßnahmen werden die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit diesem AV-Vertrag sichergestellt.

I. Technische und organisatorische Maßnahmen des Auftragnehmers

1. Zugangskontrolle: Physische Sicherheit

Der Auftragnehmer hat in Kooperation mit den weiteren Auftragsverarbeitern folgende Maßnahmen ergriffen, um eine angemessene Zugangskontrolle zu den physischen Servern, auf denen personenbezogene Daten der Kunden des Auftragnehmers gespeichert werden, zu gewährleisten:

- Alle Datencenter verfügen über Sicherheitssysteme, die sich auf dem aktuellen Stand der Technik befinden einschließlich einer 24x7x365 Überwachung, Umweltschutzmaßnahmen und ausführlichen Vorschriften, die einen sicheren Datenzugang sicherstellen.
- Das technische Personal der Datacenter, das für die Bedienung und Wartung der Datenverarbeitungsanlagen verantwortlich ist, hat keinen Zugang zu Anwendung des Auftragnehmers, Nutzer-Zugängen / Log-Ins und auch in sonstiger Weise keinen Zugriff auf Nutzerdaten oder Kursinhalte.
- Der Zugang zu den Datencentern in Europa und weitere Sicherheitsmaßnahmen unterliegen strengen Vorschriften.
- Zutrittskontrolle an den Relias Standorten durch manuelles Sicherheitsschließsystem in Verbindung mit Schlüsselregelung / Schlüsselbuch, bzw. 24/7 Personenkontrolle beim Empfang / Pförtner in Verbindung mit Tragepflicht von Gästeausweisen.

2. Zugangskontrolle: Datensicherheit

Der Auftragnehmer hat folgende Maßnahmen umgesetzt, um den Zugang zu Datenverarbeitungsanlagen durch Nichtberechtigte zu verhindern:

- Der Zugang zu Server-Systemen ist nur Personen mit Administratoren-Rechten gestattet und nur durch Passwort-geschützte, verschlüsselte Verbindungen.
- Die Datenübertragung des RLMS erfolgt verschlüsselt.
- Auf Systeme von Kunden des Auftragnehmers kann nur nach einer positive Passwort-geschützten Netzwerk-Autorisierung zugegriffen werden.
- Eingaben und Änderungen im System von Mitarbeitern des Auftragnehmers werden standardmäßig per Logfiles dokumentiert.
- Vorschriften zur Datensicherheit verlangen, dass Mitarbeiter des Auftragnehmers ihre Computer-Bildschirme jedes Mal sperren, wenn sie nicht an ihrem Arbeitsplatz sind, so dass es der Eingabe eines Passwortes bedarf, um das System wieder hochzufahren.
- Sämtliche Mitarbeiter des Auftragnehmers werden im sicheren und angemessenen Umgang mit Passwörtern und deren Änderung geschult. Hierzu gehört auch die Anweisung, Passwörter nicht aufzuschreiben.

- Alle Relias-Einheiten nutzen Firewalls, um den unautorisierten Zugang zu verhindern; hierzu zählt auch der Schutz gegen das Einschleusen von Computerviren und sog. Trojanern in das Relias-Netzwerk bzw. die Relias-Infrastruktur.
- Der Auftragnehmer hat eine Reihe von selbst entwickelten und vertraulichen Maßnahmen umgesetzt, um die Datensicherheit weiter zu erhöhen, darunter, dass Webservern die Kommunikation mit Relias' Database-Servern nur über einen zwischengeschalteten Middle-Tier Server möglich ist.
- Der Auftragnehmer trennt Database-Server strikt von Webservern, um einen unautorisierten Zugang zu verhindern.

3. Zugangskontrolle: Erlaubnisse

Der Auftragnehmer hat folgende Maßnahmen ergriffen, um sicherzustellen, dass der Zugriff auf Daten durch Personen, die Datenzugang haben, nur im Umfang, der ihnen jeweils zugewiesenen Zugangsberechtigung erfolgt:

- Daten werden innerhalb Europas gegen Datenverlust gesichert und können auf Wunsch vom Auftragnehmer wiederhergestellt werden.
- Mitarbeiter des Auftragnehmers erhalten erst dann Zugriff auf Site1 (die Master-Site, über die alle Kundenportale kontrolliert werden), nachdem sie in angemessenem Umfange im Zugriff auf und im Umgang mit Daten geschult worden sind, um auf diese Weise das unberechtigte Kopieren, die Manipulation oder das Löschen von Daten zu unterbinden.
- Die für die Vergabe von Zugangsberechtigungen maßgeblichen Verfahren werden in Organisationsprotokollen des Auftragnehmers festgelegt. Mitarbeiter des Auftragnehmers, die Administratorenrechte für den Zugriff auf die Site1 (Site1-Zugangsrechte) benötigen, umfassen folgende (hier nur unvollständig und exemplarisch genannten) Abteilungen:
    - Erstellung und Umsetzung neuer Auftragnehmer-Kunden-Seiten;
    - Hilfestellung für Kunden des Auftragnehmers bei der Behebung von Service-Problemen (Service Troubleshooting);
    - Inhalte für den Upload von Kursen; und
    - Entwicklung von Lösungen für technische Probleme (technisches Troubleshooting).
- Zugangsrechte für Anwendungen (Application Login-Rechte) erhalten nur solche Nutzer, die über ein aktives und bestehendes Kundenkonto verfügen und deren Passworte von demjenigen Kunden des Auftragnehmers, der das Konto des jeweiligen Nutzers verwaltet und überwacht, freigegeben worden sind.
- Die Zugangsrechte auf die Anwendung werden durch ein passwortgeschütztes Berechtigungskonzept geregelt und überwacht, das Zugriffe außerhalb gewährter Rechte verhindert.
- Ausschließlich der Kunde des Auftragnehmers ist innerhalb seiner jeweiligen Organisation für die Autorisierung bzw. die Sperrung des Zuganges zum LMS und die Festlegung der verschiedenen Stufen von Zugangsberechtigungen (d.h. genereller Nutzer-Zugriff, Zugang zum Reporting, Zugang zum Nutzer-Management etc.) zuständig und verantwortlich.
- Im Rahmen von Projekten temporär erforderliche Unterlagen oder Datenträger werden ordnungsgemäß vernichtet.
- Auf Wunsch des Auftraggebers können eine Überprüfung von Nutzer-Zugängen (User-Logins) und Änderungen im Record Level erfolgen.

4. Kontrolle der Datenweitergabe

Der Auftragnehmer hat folgende Maßnahmen ergriffen, um sicherzustellen, dass personenbezogene Daten nicht gelesen, kopiert, geändert oder entfernt werden können, wenn sie auf elektronischem Wege übertragen oder transportiert werden oder auf einem Datenträger gespeichert sind:

- Daten werden beim Transport verschlüsselt.
- Der Zugriff auf personenbezogene Daten ist nur durch Nutzung freigegebener Kanäle zulässig.
- Zur Verhinderung von Angriffen setzt der Auftragnehmer Firewalls ein.
- Auf Wunsch des Auftraggebers können eine Überprüfung von Nutzer-Zugängen (User-Logins) und Änderungen im Record Level erfolgen, um so Eingaben, Änderungen oder Zerstörungen nachvollziehen zu können.
- Der Auftragnehmer bietet seinen Kunden zudem kundenspezifische sichere FTP-Seiten (File Transfer Protocol) an, falls ein Kunde des Auftragnehmers dies wünscht. Sichere FTP-Ordner bieten einen vertraulichen Mechanismus, um Mitarbeiterdaten an den Auftragnehmer zu übertragen.

5. Kontrolle von Kundenvorgaben

Der Auftragnehmer hat folgende Maßnahmen umgesetzt, um sicherzustellen, dass personenbezogene Daten nur gemäß den vertraglichen Vereinbarungen oder den Vorgaben des Kunden des Auftragnehmers verarbeitet werden:

- Nutzerdaten werden in einem transaktionalen Datenspeicher aufbewahrt. Ein Abruf von Informationen aus diesem Datenspeicher erfolgt nur an einen bestimmten Kunden des Auftragnehmers und ausschließlich zur Verwendung und Nutzung durch diesen Kunden.
- Die Nutzung von Nutzerinformationen umfasst auch Berichte, die Nutzerdaten enthalten. Der Auftragnehmer stellt jedem seiner Kunden eine Vielzahl von Berichten zur Verfügung, die Nutzerinformationen enthalten. Es liegt ausschließlich in der Verantwortung des jeweiligen Kunden des Auftragnehmers, für eine ordnungsgemäße Nutzung und Vernichtung gedruckter oder gespeicherter Berichte, die sensible Daten enthalten, Sorge zu tragen. Das umfasst Emails, Spreadsheets, PDF-Dokumente oder sonstige Berichtsformate.
- Der Auftragnehmer erlaubt Dritten Zugriff auf Daten ausschließlich für Zwecke der Verarbeitung und Speicherung dieser Daten. Unter keinen Umständen wird der Auftragnehmer gesammelte Daten Dritten für kommerzielle Zwecke zur Verfügung stellen.
- Die Muttergesellschaft des Auftragnehmers hat einen Corporate Privacy-Beauftragten ernannt.

6. Kontrolle der Verfügbarkeit

Der Auftragnehmer hat folgende Maßnahmen ergriffen, um personenbezogene Daten gegen die unbeabsichtigte Zerstörung oder gegen Verlust zu sichern:

- Täglicher Daten-Back-up und eine gegen Unglücksfälle / Katastrophen geschützte Aufbewahrung von Datenträgern.
- Sicherstellung einer sicheren und geeigneten Archivierung in physisch geschützten Archiven mit Zugangskontrolle.

- Einsatz von Schutzprogrammen (Virenscannern, Firewalls, Verschlüsselungssoftware, SPAM-Filter).
- Verwendung von Speicherprogrammen mit redundanter RAID.
- Nutzung einer nicht unterbrechbaren Stromversorgung und Verfügbarkeit von Notstromversorgungsaggregaten.
- Leitlinien für die Handhabung und Umsetzung von Updates.
- Automatisierte Standard-Routinen für das regelmäßige Updaten von Schutzsoftware (wie zum Beispiel Virenscannern).
- Automatischer Support und ständige Überwachung, um Fehler aufzuspüren und zu entdecken.
- Automatische Benachrichtigung über die Weiterleitung und Behandlung von Fehlermeldungen.

7. Sicherheit: System Sicherheit

Der Auftragnehmer hat folgende Maßnahmen umgesetzt, um die Systemsicherheit zu gewährleisten:

- System-Installation unter Verwendung von einem gehärteten patched OS.
- Das System patching ist so konfiguriert, dass es einen laufenden Schutz gegen Exploits bietet.
- Schutz von Daten durch gemanagte Back-Up-Lösungen.

Distributed Denial of Service (DDoS) Mitigation Services basierend auf einem proprietären System.

8. Datentrennung

Die Kundensysteme werden auf der Lernplattform softwareseitig in Form jeweils eigener logischer Mandanten getrennt, so dass ein Systemübergreifender Zugriff ausgeschlossen ist.

Ein Berechtigungskonzept regelt und überwacht die Zugriffsrechte innerhalb der Kundensystem sowie der Administration der Lernplattform.

II. Technische und organisatorische Maßnahmen des Unterauftragnehmers Mailjet GmbH / Mailgun

Durch die interne Organisation von Mailgun wird gewährleistet, dass die spezifischen Anforderungen des Datenschutzes durch die Anwendung optimaler Sicherheitsverfahren erfüllt werden, ganz gleich wo personenbezogene Daten automatisch verarbeitet oder verwendet werden. Insbesondere sorgt Mailgun durch die folgenden Maßnahmen für den Schutz personenbezogener Daten oder anderer sensibler Datenkategorien.

Physische Zugangskontrolle:

Um unbefugten Personen den Zugang zu den Datenverarbeitungssystemen zu verweigern, mit denen personenbezogene Daten verarbeitet oder genutzt werden:

- Nutzt Mailgun Rechenzentren und Cloud-Infrastrukturen branchenführender Anbieter. Der Zugang zu sämtlichen Rechenzentren wird strengstens kontrolliert. Alle Rechenzentren sind mit Überwachungs- und biometrischen Zugangskontrollsystemen ausgestattet, für eine kontinuierliche Überwachung rund um die Uhr, 7 Tage die Woche, 365 Tage im Jahr. Darüber hinaus sind alle Anbieter nach SOC Typ II und ISO 27001 zertifiziert.

- Sind die Rechenzentren mit einer N+1-Redundanz für Strom, Netzwerk und Kühlungsinfrastruktur ausgestattet.
- Erfolgt innerhalb einer Region die Datenverarbeitung über mindestens drei verschiedene Verfügbarkeitszonen. Die Dienste sind so konzipiert, dass sie den Ausfall einer Verfügbarkeitszone ohne Unterbrechung für die Kunden überstehen.

Systemzugangskontrolle:

Um zu verhindern, dass die Datenverarbeitungssysteme unbefugt benutzt werden:

- Folgt der Administratorzugriff zu Mailgun-Systemen und -Diensten dem Prinzip der geringsten Rechte. Der Zugang zu den Systemen richtet sich nach dem Aufgabengebiet und den Zuständigkeiten am Arbeitsplatz. Mailgun verwendet eindeutige Benutzernamen/Bezeichner, die nicht weitergegeben oder auf andere Personen übertragen werden dürfen.
- Erfolgt der Zugriff auf interne Kundensupport-Tools und die Produktinfrastruktur über VPN und eine mehrstufige Authentifizierung.
- Wird der ein- und ausgehende Datenverkehr der Produktionsinfrastruktur über Zugriffssteuerungslisten (ACLs) und Sicherheitsgruppen begrenzt.
- Anhand von Intrusion Detection-Systemen (IDS) können potenziell unbefugte Zugriffe erkannt werden.
- Maßnahmen zum Schutz des Netzwerks wurden eingeführt, um die Auswirkungen von Distributed-Denial-of-Service (DDoS)-Angriffen abzumildern.
- On- und Offboarding-Prozesse werden dokumentiert und konsequent eingehalten und so sichergestellt, dass der Zugang zu internen und extern gehosteten Tools und Systemen ordnungsgemäß verwaltet wird. Wenn möglich, benutzen Dienste von Drittanbietern die Single-Sign-On-Funktionalität (SSO), die eine zentralisierte Verwaltung ermöglicht und eine mehrstufige Authentifizierung erzwingt.

Datenzugangskontrolle:

Um zu gewährleisten, dass zur Nutzung von Datenverarbeitungssystemen autorisierte Benutzer lediglich Zugriff auf die Daten haben, für die sie ein Zugriffsrecht haben, und, dass personenbezogene Daten ohne Erlaubnis während der Verarbeitung oder Nutzung und nach der Aufbewahrung nicht gelesen, kopiert, geändert oder entfernt werden können:

- Verwendet Mailgun ein Passwortverwaltungssystem, das eine Mindestlänge von Passwörtern, deren Komplexität, Ablaufzeit und die Mindestanzahl der zuletzt verwendeten Passwörter erzwingt.
- Werden Mitarbeiter-Arbeitsstationen nach längerer Inaktivität automatisch gesperrt. Benutzer werden von den Systemen nach längerer Inaktivität abgemeldet.
- Werden Protokolle zentral gespeichert und indiziert. Kritische Protokolle, wie z. B. Sicherheitsprotokolle, werden mindestens ein Jahr lang aufbewahrt.
- Gewährleistet die Patchverwaltung von Mailgun, dass die Systeme mindestens einmal pro Monat gepatcht werden. Überwachung, Warnungen und das routinemäßige Überprüfen auf Schwachstellen sollen sicherstellen, dass die gesamte Produktinfrastruktur konsistent gepatcht wird.
- Wird anhand der Antivirensoftware nach Branchenstandard sichergestellt, dass interne Anlagen, die auf personenbezogene Daten zugreifen, vor bekannten Viren geschützt sind. Die Antivirensoftware wird regelmäßig aktualisiert.
- Verwendet Mailgun Firewalls, um unerwünschten Datenverkehr am Eindringen in das Netzwerk zu hindern. Eine DMZ ist mit Firewalls ausgestattet, um interne Systeme zum Schutz sensibler Daten zusätzlich zu schützen.

Datenübertragungskontrolle:

Um sicherzustellen, dass personenbezogene Daten während der elektronischen Übertragung oder des Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Werden die ruhenden Kundendaten durch die Verwendung der AES-256-Verschlüsselung auf Blockgeräten verschlüsselt gespeichert.
- Werden die Kunden-Backups sowohl bei der Übertragung als auch im Ruhezustand stark verschlüsselt.
- Unterstützt Mailgun TLS 1.2 zur Verschlüsselung des Netzwerkverkehrs zwischen der Client-Anwendung und der Mailgun-Infrastruktur. Kunden können die Verschlüsselungseinstellungen für Nachrichten, die von Mailgun verarbeitet und an die E-Mail-Service Provider gesendet werden, kontrollieren und verwalten, um so die Compliance-Anforderungen zu erfüllen, die über den Rahmen der externen Zertifizierungen von Mailgun hinausgehen.
- Wird Mailgun durch regelmäßige Risikoeinschätzungen und Penetrationstests Dritter auf Probleme bei der Verschlüsselung aufmerksam gemacht. Mailgun führt jährlich oder bei Bedarf bei Veränderungen im Unternehmen Penetrationstests durch Dritte durch.
- Betreibt Mailgun ein Bug-Bounty-Programm, das die verantwortungsvolle Offenlegung von Schwachstellen durch Community-Recherchen unterstützt.

Eingabekontrolle:

Um zu gewährleisten, dass die Überprüfung und Feststellung möglich ist, ob und von wem die personenbezogenen Daten in Datenverarbeitungssysteme eingegeben bzw. dort geändert oder entfernt wurden:

- Werden die Systeme auf Sicherheitsereignisse hin überwacht, um eine schnelle Lösung zu gewährleisten.
- Werden die Protokolle zentral gespeichert und indiziert. Kritische Protokolle, wie z. B. Sicherheitsprotokolle, werden mindestens ein Jahr lang aufbewahrt. Zur Untersuchung von Abweichungen oder Sicherheitsereignissen können die Protokolle mit Zeitstempeln zu einzelnen eindeutigen Benutzernamen zurückverfolgt werden.
-

Verfügbarkeitskontrolle:

Um zu gewährleisten, dass die personenbezogenen Daten vor unbeabsichtigter Zerstörung oder unbeabsichtigtem Verlust geschützt sind:

- Werden die Kontodaten mindestens täglich gesichert. Für alle primären Datenbanken ist eine inkrementelle/Point-in-Time-Wiederherstellung verfügbar. Die Backups werden sowohl bei der Übertragung als auch im Ruhezustand mit starker Verschlüsselung verschlüsselt.
- Wird durch die Patchverwaltung von Mailgun sichergestellt, dass die Systeme mindestens einmal pro Monat gepatcht werden. Überwachung, Warnungen und das routinemäßige Überprüfen auf Schwachstellen sollen sicherstellen, dass die gesamte Produktinfrastruktur konsistent gepatcht wird.
- Wenn nötig, patcht Mailgun als Reaktion auf die Offenlegung kritischer Schwachstellen die Infrastruktur im Eilverfahren, um so den Systembetrieb zu gewährleisten.
- Kundenumgebungen zu jeder Zeit logisch getrennt. Kunden haben keinen Zugriff auf andere Konten als die, für die sie Anmeldeinformationen für die Autorisierung erhalten haben.

III. Technische und organisatorische Maßnahmen des Unterauftragnehmers Payone GmbH

Vertraulichkeit

Art. 32 Abs. 1 lit. b) DSGVO

1. Zutrittskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- Zutrittskontrollsystem, Ausweisleser (z.B. Magnet-/Chipkarte)
- Türsicherungen (elektrische Türöffner, Zahlenschloss etc.)
- Sicherheitstüren • Gitter vor Fenstern/Türen in den Data Centern
- Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- Werkschutz, Pförtner
- Videoüberwachung in den Data Centern
- Spezielle Schutzvorkehrungen des Serverraums
- Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern
- Nicht-reversible Vernichtung von Datenträgern
- Sicherheitsbereiche/Sperrbereiche
- Besucherregelung (z.B. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang).

2. Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben:

- Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- Autorisierungsprozess für Zugangsberechtigungen
- Restriktive Rechtvergabe (need-to-know-Prinzip) mittels Rechte- und Rollenkonzept zur Begrenzung der befugten Benutzer
- Single Sign-On im Backoffice
- BIOS Passwörter
- Passwort zur Entschlüsselung von Festplatten
- Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
- Biometrische Identifikation bei Zutritt zu Rechenzentren
- Personalisierte Chipkarten, Token, PIN/TAN, etc. für den Remote-Zugang
- Einsatz sicherer Passwortsafes
- Protokollierung des Zugangs
- Zusätzlicher System-Log-In für bestimmte Anwendungen von privilegierten Benutzern
- Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
- Firewalls

3. Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:

• Verwaltung und Dokumentation von differenzierten Berechtigungen

• Abschluss von Verträgen zur Auftragsverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von personenbezogenen Daten, also der Umgang mit personenbezogenen Daten, Gegenstand der Dienstleistung ist.

- Auswertungen/Protokollierungen von Datenverarbeitungen
- Autorisierungsprozess für Berechtigungen • Genehmigungsroutinen
- Profile/Rollen
- Verschlüsselung von CD/DVD, externen Festplatten und Laptops
- Verschlüsselung von E-Mails
- Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger (Sperrung oder Verschlüsselung von Datenträgern an USB-Ports)
- „Mobile Device Management-System“
- Vier-Augen-Prinzip • Funktionstrennung - „Segregation of Duties“
- Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
- Nicht-reversible Löschung von Datenträgern
- Sichtschutzfolien für mobile Datenverarbeitungssysteme (Laptops)
- Einsatz eines SIEM-Systems

4 Trennungskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- Speicherung der Datensätze in physikalisch getrennten Datenbanken
- Zugriffsberechtigungen nach funktioneller Zuständigkeit
- Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- Mandantenfähigkeit von IT-Systemen
- Verwendung von Testdaten
- Trennung von Entwicklungs- und Produktionsumgebung

5. Verschlüsselung und Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt – soweit möglich und sinnvoll - in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Die zusätzlichen Informationen werden nach Möglichkeit gesondert aufbewahrt und unterliegen entsprechenden technischen und organisatorischen Maßnahmen.

Es werden, sofern möglich, die personenbezogenen Daten außerhalb des Stammdatensystems durch IDs ersetzt. Dadurch wird der Datenbestand von personenbezogenen Daten auf nachfolgenden Verabeitungssystemen auf das nötige Minimum reduziert.

Folgende Maßnahmen sind umgesetzt:

- Maskierung von Daten (z.B. Kreditkartennummern)
- Verschlüsselung von sensiblen Daten (z.B. Kreditkartennummern)

Integrität

Art. 32 Abs. 1 lit. B) DSGVO

6.Weitergabekontrolle

Folgende implementierte Maßnahmen stellen sicher, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben:

- Verschlüsselung von E-Mail bzw. E-Mail-Anhängen (z.B. WinZip)
- Verschlüsselung des Speichermediums von Laptops
- Gesicherter File Transfer (z.B. sftp)
- Gesicherter Datentransport (z.B. VPN, TLS)
- Verschlüsselung von externen Festplatten oder USB-Sticks
- Verpackungs- und Versandvorschriften
- Elektronische Signatur • Gesichertes WLAN
- Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort)
- Regelung zum Umgang mit mobilen Speichermedien (z.B. Laptop, USB-Stick, Mobiltelefon)
- Protokollierung von Datenübertragung oder Datentransport
- Protokollierung von lesenden Zugriffen (z.B. bei Kreditkartendaten)
- Nachvollziehbare Protokollierung (Kopieren, Verändern oder Entfernen von Daten)
- Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)

7. Eingabekontrolle

Folgende implementierte Maßnahmen stellen sicher, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- Zugriffsrechte
- Systemseitige Protokollierungen
- Dokumenten Management System (DMS) mit Änderungshistorie
- Sicherheits-/Protokollierungssoftware
- Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- Mehraugenprinzip

Verfügbarkeit und Belastbarkeit

Art. 32 Abs. 1 lit. B) DSGVO

8.Verfügbarkeitskontrolle und Belastbarkeitskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

- Sicherheitskonzept für Software- und IT-Anwendungen
- Back-Up-Verfahren
- Rasche Wiederherstellbarkeit
- Aufbewahrungsprozess für Back-Ups (z.B. getrennter Brandabschnitt)
- Gewährleistung der Datenspeicherung im gesicherten Netzwerk
- Bedarfsgerechtes Einspielen von Sicherheits-Updates
- Spiegeln von Festplatten zwischen Rechenzentren
- Einrichtung einer unterbrechungsfreien Stromversorgung (USV)

- Geeignete Archivierungsräumlichkeiten für Papierdokumente
- Brand- und/oder Löschwasserschutz des Serverraums und der Archivierungsräumlichkeiten
- Klimatisierter Serverraum
- Virenschutz
- Firewalls
- Notfallplan
- Notfallübungen
- Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)
- Redundante, örtlich getrennt betriebene IT-Systeme

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO

9 Datenschutz-Management

Folgende implementierte Maßnahmen stellen sicher, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Datenschutz-Managementsystem der PAYONE GmbH
- Informationssicherheits-Managementsystem der PAYONE GmbH
- Datenschutzrichtlinie, Sicherheitsrichtlinie
- Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
- Bestellung eines Datenschutzbeauftragten
- Verpflichtung der Mitarbeiter auf die Vertraulichkeit
- Regelmäßige Schulungen der Mitarbeiter zum Datenschutz und zur Informationssicherheit
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Durchführung von Datenschutz-Folgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)
- Externe Prüfung/Auditierung des Datenschutzes und der Informationssicherheit (z.B. Datenschutzaudit, PCI DSS, KRITIS)

10. Incident Response Management

Folgende implementierte Maßnahmen stellen sicher, dass im Falle von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Nr. 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Nr. 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)

11. Datenschutzfreundliche Voreinstellungen

Gemäß Art. 25 Abs. 2 DSGVO sind die Default-Einstellungen sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Datenverarbeitungsverfahren zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben bzw. von Eingabemöglichkeiten (z. B. von Freitexten) festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden (z. B. hinsichtlich des Umfangs der Verarbeitung). Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und

Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden können) oder die Verfügbarkeit von bestimmten Verarbeitungsfunktionen, Protokollierungen etc. festgelegt:

- Beachtung des Datenschutzgrundsatzes zur Datenvermeidung
- Beachtung des Datenschutzgrundsatzes zur Datensparsamkeit
- Zugriffsberechtigungen, die sich am Business-Need orientieren
- Einschränkung von Daten-Exporten
- Passwortwechsel beim ersten Login
- Beachtung der Speicherfristen von Daten

12. Auftragskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können:

- Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
- Prozess zur Erteilung und/oder Befolgung von Weisungen
- Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
- Prüf- und Kontrollrechte des datenschutzrechtlich Verantwortlichen einer Datenverarbeitung
- Unabhängige Auditierung der Weisungsgebundenheit
- Verpflichtung der Mitarbeiter auf die Verschwiegenheit
- Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen
- Formalisiertes Auftragsmanagement
- Dokumentiertes Verfahren zur Auswahl des Dienstleisters
- Standardisiertes Vertragsmanagement zur Vor- und Nachkontrolle der Dienstleister

IV Technische und organisatorische Maßnahmen des Unterauftragnehmers IONOS GmbH

1. Allgemeines

Der Auftraggeber und der Auftragnehmer haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Auftraggeber hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen. Sowohl der Auftragnehmer als auch die einzelnen von diesen beauftragten Rechenzentren haben insbesondere die folgenden Maßnahmen getroffen. Grundsätzlich ist eine Nutzung der Datenverarbeitungssysteme durch den Rechenzentrumsbetreiber nicht vorgesehen. Der Auftragnehmer nutzt insofern in den Sicherheitsbereichen befindliche eigene Hardware, so dass weder Zugriffsrechte, Zugänge, Weitergaben, Eingaben der Daten des Auftraggebers durch die Rechenzentren stattfinden.

2. Technische organisatorische Maßnahmen nach Art. 32 DSGVO

Der Auftragnehmer hat geeignete Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert. (1) Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle) Die Räumlichkeiten der 1&1 IONOS Cloud GmbH in der Greifswalder Str. 207 in 10405 Berlin befinden sich in einem ausschließlich geschäftlich genutzten Hinterhaus in den Etagen EG bis 2. OG und 5 OG.

Sämtliche Zugänge sind ausreichend gegen den unbefugten Zutritt abgesichert, das bedeutet, dass:

• jedwede Außentüren mit einem manuellen und technischen Schließsystem (Sicherheitsschlösser) versehen und grundsätzlich verschlossen sind;

• die den Mitarbeitern zur Verfügung gestellten Schlüssel personengebunden registriert sowie die Schlüsselausgabe quittiert wird;

• der Zugang zu Serverräumen nur einer begrenzten Anzahl von Personen gestattet wird (restricted area);

• Mitarbeiter ausschließlich mit den personalisiert angelegten Benutzerprofilen arbeiten, welche die Eingabe eines spätestens alle drei Monate zu ändernden und mindestens 8 Stellen umfassenden alphanumerischen Passwort erfordern;

• Bildschirme automatisiert spätestens nach 5 Minuten sowie Zugänge bei mehr als fünf Fehlversuchen für 30 Minuten gesperrt werden; • VPN-Technologie (SSL/TLS) eingesetzt wird;

• Datenträger (soweit möglich) verschlüsselt sind;

• Besucher nur in Begleitung eines Mitarbeiters sich in den Räumlichkeiten bewegen können;
• Personal von Dritten, insbesondere für Reinigungs- und Wartungsaufgaben sorgfältig ausgewählt wird;

• es Festlegungen zur Zugangsberechtigung und Besucherregelung gibt.

Unter anderem im Rahmen des Rechenzentrumsbetriebes wird darauf geachtet, dass:

• der Zutritt zum Rechenzentrum nur autorisierten Personen gestattet ist;

• der Zutritt durch ein materielles (RFID-Chip) und ein geistiges (PIN) Identifikationsmerkmal gesichert ist. Es wird zwischen fest zugewiesenen und beim Sicherheitsdienst zur Abholung hinterlegten Zutrittsberechtigungen unterschieden. Bei Zutrittsberechtigungen, die zur Abholung hinterlegt sind, wird die Autorisierung durch Kontrolle des Personalausweises sichergestellt. Die Daten werden bei einem Sicherheitsdienst hinterlegt (Whitelist), so wird gewährleistet, dass nur berechtigte Personen das Rechenzentrum betreten können;

• der Zutritt zu den einzelnen Kundenschränken oder -flächen ausschließlich durch den Kunden und durch das zuständige Personal möglich ist;

• die Zutrittskontrollsysteme sowie die Alarmanlagen über USV und Netzersatzanlage gegen Stromausfall gesichert sind; das Rechenzentrum, insbesondere der Zutritt zu Sicherheitsbereichen mit Videoüberwachung ausgestattet ist;

• das Rechenzentrum regelmäßig innerhalb vorgegebener Zeitfenster durch einen Wachdienst begangen wird. Die zu überprüfenden Punkte, welche der Wachdienst in den Rechenzentren zu kontrollieren hat, sind festgelegt. Auffälligkeiten werden berichtet. Die vorgegebenen Laufwege des Wachdienstpersonals werden protokolliert.

(2) Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle)

Der Auftragnehmer gewährleistet, dass

• Datenträger (soweit möglich) restriktiv einzusetzen sowie verschlüsselt sind;

• Hardware von der IT des Auftragnehmers geprüft und herausgegeben wird; • die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren;

• ausgesonderte Datenträger datenschutzkonform gelöscht oder physikalisch gelöscht werden;

• der Zugriff auf Anwendungen (Eingabe, Veränderung und Löschung) protokolliert wird und ausgewertet werden kann (mindestens für 14 Tage) sowie

• Schutz gegen unberechtigte interne und externe Zugriffe durch Verschlüsselung und Firewalls besteht.

Es erfolgt eine authentifizierte Benutzeridentifikation, insbesondere dadurch, dass:• alle technischen Systeme (zentral und dezentral), sowohl Hard-, als auch Software durch eine Firewall geschützt sind,

• der vorhandene Virenschutz (Anti-Virensoftware) gepflegt und aktualisiert wird.

Die Kontrolle von Eingaben, erfolgt durch:

• Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles) bzw., dass • sich die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren.

(3) Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle)

Im Rahmen der Speicherkontrolle gilt das Nachfolgende:

• die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen (Berechtigungskonzept nach dem Need-to-Know-Prinzip),

• der Zugriff auf Anwendungen und Dateibenutzungen (Eingabe, Veränderung und Löschung) wird protokolliert und kann ausgewertet werden,

• Schutz gegen unberechtigte interne und externe Zugriffe durch Verschlüsselung und Firewalls besteht,

• die vom Kunden zu administrierenden Systeme datenschutzfreundliche Voreinstellungen enthalten (z. B. ist eine jederzeitige transparente Löschung möglich),

• freigegebene Speicherbereiche werden vor Neuzuweisung überschrieben (genullt).

Es erfolgt eine authentifizierte Benutzeridentifikation, insbesondere dadurch, dass:

• alle technischen Systeme (zentral und dezentral), sowohl Hard-, als auch Software durch eine Firewall geschützt sind sowie

• der vorhandene Virenschutz (Anti-Virensoftware) gepflegt und aktualisiert wird.

Die Kontrolle von Eingaben, erfolgt durch:

• Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles) sowie dass sich,

• die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren.

(4) Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle)

Die Benutzerkontrolle bedingt, dass die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren (Berechtigungskonzept nach dem need-to-know-Prinzip),

• der Zugriff auf Anwendungen (Eingabe, Veränderung und Löschung) protokolliert wird und ausgewertet werden kann (mindestens für 14 Tage) sowie,

• Remote-Access auf Infrastruktursysteme über dedizierte Managementnetzwerke und verschlüsselte, Passphrase- und Zertifikatgesicherte Services erfolgen.

Es erfolgt eine authentifizierte Benutzeridentifikation, insbesondere dadurch, dass:

• alle technischen Systeme (zentral und dezentral), sowohl Hard-, als auch Software durch eine Firewall geschützt sind und

• der vorhandene Virenschutz (Anti-Virensoftware) gepflegt und aktualisiert wird.

(5) Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle)

Die unerlaubte Tätigkeit in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen wird im Besonderen verhindert, dadurch dass:

• die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren (Berechtigungskonzept nach dem need-to-know-Prinzip),

• Passwortrichtlinien inkl. Passwortlänge und Passwortwechsel vorgegeben werden,

• der Zugriff auf Anwendungen (Eingabe, Veränderung und Löschung) protokolliert wird und ausgewertet werden kann (mindestens für 14 Tage),

• Schutz gegen unberechtigte interne und externe Zugriffe durch Verschlüsselung und Firewalls besteht,

• eine IT-Security Policy für das ITSM existiert und

• dedizierte Aufbewahrungspflichten bestehen.

(6) Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle)

Die Aspekte der Weitergabe personenbezogener Daten wird hierdurch umgesetzt, dass: • VPN-Technologie (SSL/TLS) zur Datenkommunikation eingesetzt wird,

• E-Mail-Nachrichten bzw. sonstige Informationen grundsätzlich verschlüsselt bzw. pseudonymisiert versendet werden können und

• beim physischen Transport, geeignete Transportpersonen sorgfältig ausgewählt werden.

(7) Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle)

Die Kontrolle von Eingaben, erfolgt durch:

• Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles) und, dass

• die Zugriffsrechte sich (sowohl für Anwender, wie auch für Administratoren) an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren (Berechtigungskonzept nach dem need-to-know-Prinzip).

(8) Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird (Transportkontrolle)

Die Transportkontrolle erfordert, dass

• die Auswahl von Dritten sorgfältig erfolgt (insb. wegen Datensicherheit) in Zusammenarbeit mit dem Datenschutzbeauftragten (soweit möglich nur ISO/IEC- 27001:2005 zertifizierte Unternehmen/ Rechenzentren),

• detaillierte vertragliche Regelungen zum Auftragsverhältnis existieren,

• wirksame Kontroll- und oder Zugriffs- bzw. Löschungsrechte (ggf. Vertragsstrafen) vereinbart werden und

• eine regelmäßige Kontrolle durch den Datenschutzbeauftragten erfolgt. Die Aspekte der Weitergabe personenbezogener Daten wird hierdurch umgesetzt, dass:

• VPN-Technologie (SSL/TLS) zur Datenkommunikation eingesetzt wird,

• E-Mail-Nachrichten bzw. sonstige Informationen grundsätzlich verschlüsselt bzw. anonymisiert versendet werden können und

• beim physischen Transport, geeignete Transportpersonen und -fahrzeuge sorgfältig ausgewählt werden und eine Festlegung der Wege stattfindet.

Die Kontrolle von Eingaben, erfolgt durch:

• Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles) sowie • die Zugriffsrechte, welche sich (sowohl für Anwender, wie auch für Administratoren) an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren.

(9) Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit)

Zur Wiederherstellbarkeit verpflichtet sich der Auftragnehmer

• zur Erstellung eines Backup- & Recoverykonzepts,

• die Datenwiederherstellbarkeit zu testen,

• Raid-Controller (Redundant Array of Independent Disks),

• zur Unterstützung der Datenportablität und

• Protokollierung und Auswertung von Störungsvorfällen.

(10) Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit)

Die Zuverlässigkeit erfordert, dass

• Eskalationsfälle prozessual gemeldet werden (Anzeige von Fehler- und Störmeldungen in den IT-Systemen),

• externe/interne technische Sicherheitsanalysen durchgeführt werden,

• Test- und Freigabeverfahren z. B. bei Einführung neuer Soft- oder Hardware bestehen und • Sensibilisierungen der Mitarbeiter zum Datenschutz und/oder -sicherheit vorgenommen werden.

(11) Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)

Im Rahmen der Datenintegrität orientiert sich der Auftragnehmer

• an einem Managementsystem für Informationssicherheit (ISMS) bzw. kann

• die Verarbeitung personenbezogener Daten im Einzelfall in Abstimmung mit dem Auftraggeber in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

Es erfolgt eine authentifizierte Benutzeridentifikation, insbesondere dadurch, dass:

• alle technischen Systeme (zentral und dezentral), sowohl Hard-, als auch Software durch eine Firewall geschützt sind und

• der vorhandene Virenschutz (Anti-Virensoftware) gepflegt und aktualisiert wird. Die Kontrolle von Eingaben, erfolgt durch:

• Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles) als auch,

• die Zugriffsrechte, welche sich (sowohl für Anwender, wie auch für Administratoren) an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren.

(12) Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

Die Vergabe und die Überwachung von Auftragsverarbeitungen insbesondere der externen Rechenzentren ergeben sich aus dem Folgenden:

• sorgfältige Auswahl von Dritten (insb. wegen Datensicherheit) in Zusammenarbeit mit dem Datenschutzbeauftragten (soweit möglich nur ISO/IEC- 27001:2005 zertifizierte Unternehmen/ Rechenzentren),

• detaillierte vertragliche Regelungen zum Auftragsverhältnis,

• Vereinbarung wirksamer Kontroll- und oder Zugriffs- bzw. Löschungsrechte (ggf. Vertragsstrafen),

• regelmäßige Kontrolle durch den Datenschutzbeauftragten.

(13) Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)

Zur Durchsetzung der Verfügbarkeit, hat der Auftragnehmer veranlasst, dass: • eine Backup Strategie existiert,

• eine unterbrechungsfreie Stromversorgung besteht (USV),

• Räumlichkeiten in Brandabschnitten versehen mit einzelnen Brandschutzeinrichtungen (Feuer- und Rauchmeldeanlagen, Feuerlöscher) eingeteilt sind,

• Klimaanlagen vorhanden sind,

• eine Notfallmatrix besteht.

Im Rahmen des Rechenzentrumsbetriebes wird insbesondere darauf geachtet, dass:

• die Stromversorgung durch Redundanzen sichergestellt wird (Notstromaggregate sowie USV-Anlagen mit n+1 Redundanz; Überbrückungszeit mindestens 15 min. bis die Notstromaggregate die Stromversorgung wieder sicherstellen - Anlaufzeit inkl. Lastübernahme 1-2 min.);

• das Rechenzentrum mit einer Raumklimatisierung ausgestattet ist (mittlere Temperatur 22° C +/- 4°, redundant ausgelegt (n+1), die installierten Luftfilter entsprechen DIN EN 779 G4); • das Rechenzentrum über baulich getrennte Brandabschnitte verfügt.

In den Räumlichkeiten ist eine Brandmeldeanlage und eine Brandfrühersterkennung installiert;

• die Hochwasser- und Erdbebenkritikalität DIN-gerecht geprüft wurde.

(14) Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit) Die getrennte Datenverarbeitung wird gewährleistet durch:

• fehlende Möglichkeit eines physikalischen Zugriffs durch dedizierte Rechte und Pflichten,

• klare Trennung und Nachvollziehbarkeit von Kundenzugriffen (logische Trennung durch individuelle Benutzerprofile mit Passwortschutz/ Trennung von Produktiv- und Testinfrastruktur),

• getrennte Verarbeitung zweckgebundener Daten.

(15) Anpassung der innerbetrieblichen Organisation an die besonderen Anforderungen des Datenschutzes

Der Auftragnehmer hat sich den folgenden datenschutzrechtlichen Standards unterworfen:

• Erarbeitung eines IT-Sicherheits- und Datenschutzkonzepts,

• Fertigung von internen Datenschutz- und Sicherheitsrichtlinien (Policies) sowie Arbeitsanweisungen,

• Bestellung eines externen Datenschutzbeauftragten,

• Regelmäßige Kontrolle durch den Datenschutzbeauftragten,

• Regelmäßige Hinweise und Ermahnungen, um das Problembewusstsein zu fördern,

• Gelegentliche unvermutete Kontrolle der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen.

Der Auftragnehmer gewährleistet, dass die Leistungserbringung grundsätzlich in deutschen Rechenzentren und unter Beachtung des deutschen Datenschutzrechts erfolgt.

Die Leistungen der 1&1 IONOS Cloud GmbH orientieren sich zudem soweit möglich an den Vorgaben der Normen der ISO-27001 Zertifizierung. Der Workflow zur Annäherung und Erfüllung der Normen richtet sich nach dem im ITIL Framework.

Zudem verfolgt der Auftragnehmer die Prozesse, um die Anforderungen der ISO 20000 zu erfüllen (Vorbereitung einer Zertifizierung; insbesondere Incident & Service Request Management; Problem management; Business Relationship Management; Budgeting and Accounting for Services; Service Level Management; Capacity Management; Design and Transition of new or changed Services; Change Management; Release and Deployment; Configuration Management; Information Security Management; Service Continuity and Availability; Supplier Management; Durchführung interner Audits). Der Auftragnehmer hat zudem nach den allgemein anerkannten Regeln von Wissenschaft und Technik die operativen Leistungskomponenten (Storage Systeme/ Infinibandswitche und Uplink Router/ Switche) doppelt redundant ausgelegt.