Auftrag gemäß Art. 28 DSGVO

Vereinbarung

zwischen

Nutzer*innen

- nachstehend „Auftraggeber“ genannt -

und

Negotiation Academy Potsdam Consulting GbR
Karl-Marx-Str. 12
14482 Potsdam

- nachstehend „Auftragnehmer“ oder „Auftragsverarbeiter“ genannt -

1. Gegenstand und Dauer der Verarbeitung

Diese Vereinbarung ist Bestandteil einer Vereinbarung über die Bereitstellung der Web-Applikation NEMA durch den Auftragnehmer für den Auftraggeber im Rahmen eines Software as a Service Angebots (nachfolgend „Hauptvertrag“) und konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus der im Hauptvertrag vereinbarten Auftragsdatenverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogenen Daten des Auftraggebers im Auftrag verarbeiten.

Die vertraglich vereinbarten Leistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht.

2. Konkretisierung des Auftragsinhalts

Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien betroffener Personen:

Gegenstand des Auftrags sowie Art und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag.

Die Kategorien der betroffenen Personen und die Art der Daten sind in ***Anlage 1*** zu dieser Vereinbarung näher spezifiziert.

Dauer der Verarbeitung:

Die Laufzeit dieser Vereinbarung und die Dauer der Verarbeitung richten sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

3. Anwendungsbereich und Verantwortlichkeit

3.1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag und in einer etwaigen Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Vertragsbeziehung für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzes, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

3.2. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in Textform (z.B. E-Mail, Fax, Brief) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). In dringenden Fällen kann der Auftraggeber Weisungen auch mündlich erteilen. Der Auftraggeber bestätigt mündliche Weisungen unverzüglich in Textform. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

3.3. Die Inhalte dieser Vereinbarung gelten entsprechend, wenn durch den Auftragnehmer für den Auftraggeber die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

4. Pflichten des Auftragnehmers

4.1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung des Auftraggebers gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Europäischen Union oder der Mitgliedsstaaten verstößt. Der Auftragnehmer darf die Umsetzung einer solchen Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

4.2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der der DSGVO genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Die zu treffenden Maßnahmen umfassen insbesondere die in ***Anlage 2*** zu dieser Vereinbarung aufgeführten Maßnahmen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Diese Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer darf alternative Maßnahmen einsetzen, wenn diese mindestens das Sicherheitsniveau der gemäß ***Anlage 2*** vereinbarten Maßnahmen erreichen.

4.3. Der Auftragnehmer unterstützt den Auftraggeber auf Anfrage im Rahmen seiner Möglichkeiten mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner (des Auftraggebers) Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Personen nachzukommen. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der

Verarbeitung und der ihm zur Verfügung stehenden Informationen auf Anfrage ferner bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten.

4.4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

4.5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft in solchen Fällen die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

4.6. Der Auftragnehmer gewährleistet, seiner Pflicht nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

4.7. Der Auftragnehmer ist verpflichtet, nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten des Auftraggebers, die er im Rahmen der Auftragsverarbeitung erhalten hat, nach dessen Wahl entweder zu löschen oder zurück zu geben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

5. Pflichten des Auftraggebers

5.1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen oder bei der Auftragsdatenverarbeitung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

5.2. Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftraggeber den Auftragnehmer bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

5.3. Wenn der Auftragnehmer wegen der Ausführung einer vom Auftraggeber erteilten Weisung von einem Dritten, der nicht Partei dieses Auftrags ist, insbesondere von einer betroffenen Person in Anspruch genommen wird, ist der Auftraggeber verpflichtet, dem Auftragnehmer die diesem in diesem Zusammenhang entstehenden Schäden zu ersetzen.

5.4. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

6. Ansprechpartner

Die zuständigen Ansprechpartner sind in ***Anlage 3*** benannt.

7. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

8. Nachweismöglichkeiten

8.1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

8.2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und 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 zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

8.3. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses, insbesondere im Zusammenhang mit durchgeführten Kontrollen erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers streng vertraulich zu behandeln.

9. Unterauftragsverhältnisse

9.1. Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt, insoweit erklärt der Auftraggeber seine Zustimmung:

- Hetzner Online GmbH
  - Speicherung der Anwendungsdaten in persistenten Datenbanken
  - Betrieb der Anwendung und primäre Datenverarbeitung
  - Vertragsgrundlage: Data Processing Agreement vom 04.03.2024
  - Garantien: EU-Standardvertragsklauseln, ISO 27001 zert. Serverstandort garantiert in der EU
- Functional Software, Inc. d/b/a Sentry
  - Erfassung und Speicherung von Fehlern innerhalb der Anwendung in persistenten Datenbanken
  - Vertragsgrundlage: Data Processing Agreement vom 04.03.2024
  - Garantien: ISO 27001 Zertifizierung

Vor der Hinzuziehung weiterer oder der Ersetzung vorstehend aufgeführter Subunternehmer ist der Auftragnehmer verpflichtet, den Auftraggeber in Textform zu informieren. Der Auftraggeber kann der Hinzuziehung weiterer oder der Ersetzung eingesetzter Subunternehmer innerhalb einer Frist von vier Wochen ab Zugang der Mitteilung seitens des Auftragnehmers aus wichtigem datenschutzrechtlichen Grund gegenüber der vom Auftragnehmer bezeichneten Stelle in Textform widersprechen. Erfolgt kein formgerechter Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als erteilt; hierauf und auf die Form und Frist für den Widerspruch wird der Auftragnehmer ausdrücklich in der Mitteilung über die Änderung hinweisen.

9.2. Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Der Auftragnehmer ist auf schriftliche Anforderung des Auftraggebers verpflichtet, Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erteilen.

9.3. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Leistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der

Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Reinigungskräfte, Prüfer. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

10. Kostenerstattung

10.1. Soweit die Verpflichtungen aus dieser Vereinbarung lediglich Pflichten des Auftragnehmers aus dem Hauptvertrag konkretisieren (z.B. Bereitstellung bestimmter technischer und organisatorischer Maßnahmen), erbringt der Auftragnehmer diese Leistungen kostenlos.

10.2. Sämtliche weitergehenden Aufwände, die dem Auftragnehmer auf Grundlage dieser Vereinbarung entstehen, werden vom Auftraggeber nach tatsächlichem Aufwand unter Zugrundelegung eines Stundensatzes in Höhe von 150,00 EUR erstattet, dies gilt insbesondere für sämtliche Aufwände, die dem Auftragnehmer im Zusammenhang mit der Erfüllung seiner Pflichten nach Ziff. 7. dieser Vereinbarung entstehen.

10.3. Für die Abrechnung und Rechnungsstellung gelten die Bestimmungen des Hauptvertrages entsprechend.

11. Allgemeine Bestimmungen

11.1. Änderungen und Ergänzungen sowie die Aufhebung der Vereinbarung zur Auftragsdatenverarbeitung oder dieser Bedingungen bedürfen zu ihrer Wirksamkeit der Textform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für die Aufhebung des Textformerfordernisses selbst.

11.2. Sollte eine Bestimmung des Vertrags oder dieser Bedingungen ganz oder teilweise unwirksam sein oder werden oder der Vertrag eine Lücke enthalten, bleibt die Rechtswirksamkeit der übrigen Bestimmungen hiervon unberührt. Anstelle der unwirksamen Bestimmungen werden die Vertragsparteien eine Regelung vereinbaren, die dem von den Vertragsparteien Gewollten wirtschaftlich am nächsten kommt.

11.3. Erfüllungsort der Sitz des Auftragnehmers.

11.4. Sofern der Auftraggeber Vollkaufmann, juristische Person des öffentlichen Rechts oder öffentlich rechtliches Sondervermögen ist oder der Vertrag Auslandsbezug aufweist, wird für alle Streitigkeiten, die sich aus oder im Zusammenhang mit der zwischen den Parteien vereinbarten Auftragsdatenverarbeitung ergeben, der Sitz des Auftragnehmers als Gerichtsstand vereinbart.

Anlage 1: Kategorien der betroffenen Personen und Art der Daten

Kategorien der betroffenen Personen	• Angestellte und freie Mitarbeiter des Auftraggebers • Interessenten • Kunden • Lieferanten • sonstige Geschäftspartner • angestellte und freie Mitarbeiter bei den vorstehend genannten Geschäftspartnern des Auftraggebers
Art der Daten	• Name, Vorname • Anrede • Adressdaten • E-Mail und ggf. weitere Kontaktdaten (z. B. Telefonnummer) • IP-Adressen • Berufsstand • Arbeitszeiten • Tätigkeiten • Fotos • Angaben zu unterschiedlichen Verhandlungskonstellationen

Anlage 2: Technische und organisatorische Maßnahmen

1. ZUTRITTSKONTROLLE ZU RÄUMLICHKEITEN UND EINRICHTUNGEN, IN DENEN DATEN VERARBEITET WERDEN

a) Zutritt zu den Räumlichkeiten des Auftragnehmers, die zur Durchführung des Auftrags verwendet werden, ist auf die zur Durchführung des Auftrags erforderlichen Personen beschränkt.

b) Die Eingänge zu den Räumlichkeiten des Auftragnehmers, in denen Personenbezogene Daten verarbeitet werden, sind mit Sicherheits- oder Magnetkartenschlössern gegen Zutritt Unbefugter gesichert.

c) Die Ausgabe von Schlüsseln und Zugangskarten ist protokolliert.

d) Türen, Tore und Fenster der Räumlichkeiten des Auftragnehmers, in denen Personenbezogene Daten verarbeitet werden, sind außerhalb der Betriebszeiten fest verschlossen; Türen, Tore und Fenster in Keller und Erdgeschoss sowie alle weiteren leicht zu erreichenden Zugänge zu diesen Räumen sind derart ausgeführt, dass diese Unbefugten nur erheblich erschwert zugänglich sind, etwa durch einbruchhemmende Türen, Tore, Fenster und Schlösser und/oder den Einsatz einer Einbruchmeldeanlage, sowie die in VdS 2333 beschriebenen Sicherungsmaßnahmen der Sicherungsklasse SG1.

e) Zur Durchführung des Auftrags vom Auftragnehmer verwendete Server sind in einem separat abgesicherten Serverraum oder Rechenzentrum untergebracht, welche durch eine Zutrittskontrollanlage entsprechend Klasse B nach VdS 2367 gegen den Zutritt Unbefugter gesondert gesichert sind. Diese Räume sind einbruchhemmend geschützt und mindestens gemäß den Vorgaben der Sicherungsklasse SG1 nach VdS 2333 ausgeführt. Der Zutritt zu diesen Räumlichkeiten ist auf das zur Wartung und Instandsetzung sowie auf die im Übrigen konkret erforderlichen Rollen und Personen beschränkt.

2. ZUGANGSKONTROLLE

a) Die zur Durchführung des Auftrags vom Auftragsverarbeiter eingesetzten informationsverarbeitenden Systeme (Client- und Serversysteme) sind durch Authentifikations- und Autorisationssysteme geschützt.

b) Identifikations- und Authentifikationsinformationen (insbesondere in Form von Benutzernamen und Passwörtern), welche mit der Zugangsberechtigung zu den zur Durchführung des Auftrags eingesetzten informationsverarbeitenden Systemen verbunden sind, werden nur an die mit der Durchführung des Auftrags beauftragten Personen und lediglich in dem für die jeweilige Aufgabe erforderlichen Umfang vergeben.

c) Jede Vergabe von Zugangsberechtigungen wird für die Laufzeit des Auftrags dokumentiert.

d) Alle Zugänge und Kennungen („Accounts“) werden ausschließlich personenspezifisch vergeben. Die Benutzung von Accounts durch mehrere Personen (Gruppen-Accounts) unterbleibt grundsätzlich.

e) Identifikations- und Authentifikationsinformationen werden ausschließlich persönlich verwendet, ein in solchen Informationen enthaltenes Passwort wird als Initialpasswort vergeben und wird unverzüglich nach dem Erhalt durch die berechtigte Person entsprechend den in diesem Anhang festgelegten Bestimmungen auf ein nur der berechtigten Person bekanntes Passwort umgesetzt; jegliche Weitergabe unterbleibt. Sofern Unbefugte Kenntnis von Zugangsdaten erhalten, zeigt der Auftragsverarbeiter dies dem Verantwortlichen unverzüglich an.

f) Die Wahl der Passwörter erfolgt in ausreichender Komplexität und Güte. Ausreichende Komplexität und Güte bedeutet mindestens eine Länge von zehn (10) Zeichen bei Nutzung von drei der folgenden 4 Kategorien (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen), keine Verwendung generischer Begriffe oder von Eigennamen sowie die Unzulässigkeit mindestens der letzten drei (3) verwendeten Passwörter.

g) Der Auftragsverarbeiter hält Authentifikationsdaten (insbesondere Passwörter und kryptographische Schlüssel) gegenüber Unbefugten streng geheim, bewahrt diese nicht im Klartext auf und verwendet diese ausschließlich unter Einsatz einer dieses Anhangs entsprechenden Verschlüsselung oder als unumkehrbare kryptographische Prüfsumme (insbesondere bei der Speicherung und der Übertragung im Netzwerk).
h) Für die Verschlüsselung wird der AES Algorithmus mit 256 Bit und für Password Hashes der HMAC Algorithmus mit 512 Bit verwendet.
i) Jede Herausgabe von Hardware an Mitarbeiter des Auftragnehmers wird für die Dauer des Auftrags dokumentiert.

3. ZUGRIFFSKONTROLLE

a) Sofern Personenbezogene Daten zur Durchführung des Auftrags auf informationsverarbeitenden Systemen des Auftragsverarbeiters gespeichert sind, ist für sämtliche Zugriffe auf personenbezogene Daten ein abgestuftes und geeignet granulares Rechtesystem eingerichtet und technisch implementiert. Dadurch ist sichergestellt, dass die Zugriffsrechte so gestaltet sind, dass sie nur den für die Leistungserbringung eingesetzten Mitarbeiter jeweils für die Erfüllung der konkreten Aufgaben im notwendigen Umfang Zugriff auf die personenbezogenen Daten erlauben. Dabei ist die Vergabe von Administratorenrechte auf das zwingend erforderliche Maß an Mitarbeitern des Auftragsverarbeiters begrenzt.
b) Alle verarbeiteten Daten werden verschlüsselt übertragen. Alle personenbezogenen Daten werden verschlüsselt in unseren Datenbanksystemen abgelegt. Jeder Zugriff erfolgt ebenfalls über verschlüsselte Datenkanäle.
c) Sofern personenbezogene Daten auf informationsverarbeitenden Systemen des Auftragsverarbeiters gespeichert sind, werden sämtliche Zugriffe auf personenbezogene Daten (einschließlich des lesenden, verändernden und löschenden Zugriffs) nach Benutzer, Datum, Uhrzeit und den jeweils betroffenen Personenbezogene Daten mindestens für die Dauer von 90 Tagen protokolliert.
d) Alle im Rahmen der Auftragsverarbeitung verwendeten Endgeräte (Laptops, Telefone usw.) sind mit automatischer Bildschirmsperre bei Inaktivität versehen.
e) In den Räumen des Auftragnehmers herrscht eine Clean-Desk-Policy, Schreibtische und sonstige Oberflächen sind frei von jeglichen Unterlagen zu hinterlassen.

4. EINGABEKONTROLLE

a) Die Eingabe, Änderung und Löschung von Daten in den verwendeten Server-Systemen wird automatisiert protokolliert.
b) Die Eingabe, Änderung und Löschung von Daten in den verwendeten Server-Systemen ist durch das Verwenden individueller Benutzernamen nachvollziehbar.
c) Die Vergabe von Rechten zu Eingabe, Änderung und Löschung von Daten in den verwendeten Server-Systemen erfolgt auf Basis eines Berechtigungskonzepts.
d) Dateien und Dokumente werden in Dokumentenmanagement-Systemen gespeichert, die Eingaben und Änderungen automatisch mit Datum und Benutzerkennung protokollieren.
e) Vor der Installation neuer Programme und Updates auf den verwendeten Serversystemen wird deren Integrität durch Funktionstests sichergestellt.

5. AUFTRAGSKONTROLLE

a) Über die allgemeinen Grundsätze sowie über die sich aus dieser AVV ergebenden spezifischen Anforderungen des Datenschutzes, einschließlich der Datensicherheit, werden die beim Auftragsverarbeiter zur Durchführung des Auftrags beschäftigten Personen vor dem Einsatz beim Auftragsverarbeiter zur Durchführung des Auftrags und sodann regelmäßig umfassend geschult.
b) Am Ende und auf Grundlage des in a) dieses Abschnitts festgelegten Schulungsprozesses werden die beim Auftragsverarbeiter zur Durchführung des Auftrags beschäftigten Personen auf die Vertraulichkeit und den Schutz personenbezogener Daten verpflichtet. Diese Verpflichtung erstreckt sich auf das

Fernmeldegeheimnis und die damit verbundenen Grundsätze und Anforderungen an die Vertraulichkeit der Telekommunikation, wenn dies nach Maßgabe des konkreten Auftrags erforderlich ist, insbesondere wenn der Auftrag den Zugriff auf Verkehrsdaten umfasst.

c) Die Vergabe von Aufträgen an Unterauftragnehmer erfolgt ausschließlich schriftlich, nach Abschluss eines Auftragsverarbeitungsvertrages und eingehender Prüfung der beim Unterauftragnehmer etablierten Technischen und organisatorischen Maßnahmen.

d) Es wird ein zentrales Verzeichnis aller abgeschlossenen Auftragsverarbeitungsverträge der beauftragten Subunternehmer geführt.

e) Nach Beendigung der Zusammenarbeit mit Unterauftragnehmern werden diese angewiesen, sämtliche verarbeiteten personenbezogenen Daten ordnungsgemäß zu löschen.

6. GETRENNTE VERARBEITUNG VON DATEN/TRENNUNGSKONTROLLE

a) Sofern personenbezogene Daten auf informationsverarbeitenden Systemen des Auftragsverarbeiters gespeichert sind, wird eine vollständige Trennung der Personenbezogene Daten von personenbezogenen Daten anderer Auftraggeber realisiert und dadurch die jederzeitige und vollständige Identifizier- und Löschbarkeit von personenbezogene Daten sichergestellt, z.B., durch Speicherung der personenbezogenen Daten in einem eigenen Mandanten, in einer eigenen Partition oder unter eindeutigen Identifier getrennt abrufbar.

b) Eine entsprechende Trennung wird auch für personenbezogene Daten selbst realisiert, wenn sie zu verschiedenen Zwecken gespeichert werden.

7. WEITERGABEKONTROLLE

a) Personenbezogene Daten können nicht unbefugt kopiert (insbesondere auf externe Datenträger gespeichert), weitergegeben und/oder gelöscht werden.

b) Datenträger sowie sämtliche Dokumente, sofern sie Personenbezogene Daten enthalten (einschließlich sämtlicher gegebenenfalls vorhandener Sicherungskopien von personenbezogenen Daten und Kopien von Originaldokumenten) werden in ordnungsgemäß verschlossenen, und ausschließlich für die Durchführung des Auftrags genutzten Datensicherungsschränken verwahrt, wenn und solange sie nicht nach Maßgabe dieses Anhangs in der Bearbeitung sind.

c) Originaldokumente, die personenbezogene Daten enthalten, werden durch die den Prozess verantwortlich leitenden Personen an die zur Leistungserbringung eingesetzten Personen herauszugeben und von diesen nach Arbeitsschluss wieder entgegengenommen.

d) Den bei der Durchführung des Auftrags beschäftigten Personen ist die Anfertigung von handschriftlichen Aufzeichnungen nur in dem zur Leistungserbringung erforderlichen Umfang und auf besonders gekennzeichneten Arbeitsmitteln (z.B. paginiertes oder farbiges Papier) gestattet.

e) Nach Maßgabe dieses Anhangs herausgegebene Originaldokumente oder nach Maßgabe dieses Anhangs erstellte handschriftliche Aufzeichnungen werden, auch bei auch nur kurzzeitigem Verlassen des Arbeitsplatzes, vor unberechtigtem Zugriff geschützt (“Clean Desk Policy“).

f) Die den bei der Durchführung des Auftrags beim Auftragsverarbeiter beschäftigten Personen nutzen Client-Systeme die ausreichend gesichert sind. Alle Client Systeme sind mit Firewall und Virenschutz versehen und werden regelmäßig auf gängige Sicherheitsstandards überprüft.

g) Auf Durchführung des Auftrags vom Auftragsverarbeiter verwendeten Server-Systemen mit nicht-flüchtigem Speicher, z.B. Netzwerkdrucker oder Scanner, werden personenbezogene Daten nicht über den unmittelbar zur Vertragsdurchführung erforderlichen Umfang hinaus gespeichert. Sofern Dritte mit der Wartung solcher Systeme betreut sind, gilt Ziffer 5.3 dieses Anhangs entsprechend.

h) In den Räumlichkeiten des Auftraggebers bereitgestellte WLAN-Zugänge für den Netzwerkzugriff sind verschlüsselt.

i) Besteht nach Maßgabe des Auftrags für den Auftragsverarbeiter eine Pflicht zur Löschung von personenbezogenen Daten, wird der Auftragsverarbeiter
   i. die datenschutzgerechte nicht wieder herstellbare Löschung sämtlicher, personenbezogene Daten enthaltender, löschbaren elektronischen Datenträger (insbesondere Festplatten, USB-Sticks, Disketten, Bänder) durchführen; ii. die nachhaltige und irreversible Entfernung von personenbezogenen Daten aus Datenbank- oder File-Systemen sowie aus allen anderen löschbaren Speichermedien realisieren;
   ii. sämtliche, personenbezogene Daten enthaltende Papierdokumente und sonstige nichtgemäß (i) oder (ii) dieser Ziffer löschbaren Datenträger (einschließlich sämtlicher personenbezogene Daten enthaltener Fehldrucke, Speicherkarten, USB-Sticks, etc.) mit einem handelsüblichen Dokumentenvernichter gemäß der Sicherheitsstufe 3 gemäß DIN-Norm 32757 oder einem mindestens gleichwertigen Verfahren vernichten, wobei defekte magnetische Datenträger, die nicht wie oben angegeben mechanisch vernichtet werden können (z.B. defekte Festplatten), sind mittels eines zugelassenen Löschgerätes nach DIN 33858 zu löschen;
   iii. die Löschung für die Dauer des Auftrages protokollieren.

8. VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B DSGVO)

a) Vom Auftragsverarbeiter zur Durchführung des Auftrags verwendete Server-Systeme werden durch Firewalls geschützt, welche diese Server-Systeme gegen nicht betriebsnotwendige Zugriffe sichern.
b) Sämtliche gegebenenfalls vom Auftragnehmer zur Durchführung des Auftrags verwendete Software wird aktualisiert gehalten und sicherheitsrelevante Aktualisierungen (insbesondere Updates, Patches, Fixes) werden unverzüglich eingespielt, nachdem diese vom Hersteller der Software allgemein verfügbar gemacht und vom Auftragsverarbeiter im Rahmen eines dem Stand der Technik entsprechenden Verfahren getestet werden. Bei als „kritisch“ oder sinngemäß qualifizierten Aktualisierungen beträgt die Frist nach Satz 1 höchstens zwei (2) Tage.
c) Originaldokumente, die personenbezogene Daten enthalten, sowie beim Auftragsverarbeiter rechtmäßig auf informationsverarbeitenden Systemen gespeicherte Personenbezogene Daten werden durch technische und organisatorische Maßnahmen vor Verlust durch zufällige, fahrlässige oder vorsätzliche Löschung oder Veränderung geschützt.
d) Sicherungskopien von beim Auftragnehmer rechtmäßig auf informationsverarbeitenden Systemen gespeicherten personenbezogene Daten werden nach denselben Maßgaben wie Originaldaten behandelt, insbesondere gegen unbefugten Zugriff gesichert.
e) Sämtliche verwendeten Server-Systeme verfügen über Feuer- und Rauchmeldeanlagen, Feuerlöschsysteme, klimatisierte Serverräume, Schutzmaßnahmen gegen Überspannung, Videoüberwachung sowie Alarmmeldungssysteme bei unberechtigten Zutritten zum Serverraum.
f) Sämtliche Speichersysteme verfügen über redundante Speichermedien (z.B. RAID-Systeme, Spiegelungen oder vergleichbar).
g) Der Auftragnehmer verfügt über ein Backup- und Recovery-Konzept, das die Wiederherstellung von Backups der letzten 30 Tage ermöglicht.
h) Die Datenspeicherung erfolgt getrennt von der Speicherung von Betriebs- und Anwendungssystemen.
i) Die Speicherung von Daten und Backups erfolgt in mindestens zwei getrennten Brandschutzzonen.
j) Die Datenwiederherstellung wird regelmäßig getestet und das Testergebnis protokolliert.

9. DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN, PRIVACY BY DEFAULT

a) Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

b) Durch geeignete technische Maßnahmen (Selbstständiges Anstoßen und Bestätigen des Löschvorgangs) wird die einfache Ausübung des Widerrufsrechts der Betroffenen gewährleistet.

10. ORGANISATIONSKONTROLLE

a) Es wird ein externer Datenschutzbeauftragter durch den Auftragnehmer bestellt.

b) Der bestellte Datenschutzbeauftragte wird durch einen internen Mitarbeiter („Lead-Function Datenschutz“) in seiner Arbeit unterstützt.

c) Sämtliche Mitarbeiter des Auftragnehmers werden mindestens einmal pro Jahr in Datenschutzfragen und vorliegenden Datenschutzkonzepten geschult.

d) Für Mitarbeiter des Auftragnehmers gelten interne Richtlinien und Arbeitsanweisungen zu
   a. Umgang mit personenbezogenen Daten im Home-Office / Mobile-Office,
   b. Nutzung des betrieblichen Internetzugangs und des betrieblichen E-Mail-Accounts,
   c. Nutzung privater Geräte für betriebliche Tätigkeiten (Bring your own device).

e) Alle Mitarbeiter des Auftragnehmers werden schriftlich auf die datenschutzrechtliche Vertraulichkeit verpflichtet.

11. REGELMÄßIGE ÜBERPRÜFUNG UND WIRKSAMKEITSKONTROLLE

a) Die in diesem Anhang aufgeführten Maßnahmen werden mindestens einmal jährlich durch die Geschäftsführung und die IT-Leitung in Zusammenarbeit mit dem Datenschutzbeauftragten überprüft.

b) Für den Fall, dass bei der Überprüfung festgestellt wird, dass sich technologische Standards oder organisatorische Prozesse geändert haben und solche Änderungen eine Anpassung der hier aufgelisteten Maßnahmen erforderlich machen, werden die dadurch erforderlich werdenden Anpassung unverzüglich umgesetzt. Dabei wird der Grundsatz der Angemessenheit beachtet.

c) Änderungen werden zudem auf ad hoc Basis durchgeführt, sofern dies aus Gründen der Sicherheit erforderlich ist.

d) Die Überprüfung sowie daraus resultierende Änderungen werden dokumentiert und abgelegt.

Anlage 3: Ansprechpartner

Ansprechpartner für datenschutzrechtliche Belange, insbesondere berechtigt und zuständig für die Erteilung bzw. den Empfang auf Seiten des Auftragnehmers sind:

Auftragnehmer:

Name: Katja Goericke
Funktion: Rechtsabteilung
Kommunikationskanal für Weisungen:
E-Mail: info@nap-digital.de
Telefon: 0331-2016 9258

Vertreter:
Name: Dr. Maximilian Ortmann
Funktion: Datenschutzbeauftragter
Kommunikationskanal für Weisungen:
E-Mail: info@nap-digital.de
Telefon: 0331-2016 9258

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich in Textform die Nachfolger bzw. die Vertreter mitzuteilen.