Zusatzvereinbarung zur Auftragsverarbeitung

gem. Art. 28 EU-Datenschutz-Grundverordnung (DSGVO).

zwischen

Firma: _____
Name: _____
Straße: _____
PLZ/Ort: _____

- nachfolgend Auftraggeber/Kunde-

und

nettrix e.K.
Franz-Josef Drewer-Gutland
Staufenstr.40
48145 Münster

- nachfolgend Auftragnehmer -

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem Hauptvertrag (Angebot / Leistungsbeschreibung, AGB) 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 Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrags.

§ 1 Definitionen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

(2) Datenverarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers (Art. 4 Abs. 2 EU-DSGVO).

(3) Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Herausgabe, Anonymisierung, Sperrung oder Löschung) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst, abhängig vom gebuchten Produkt, Hostingleistungen für Webhosting, Management von Servern, Vermietung von virtuellen und dedizierten Servern, Bereitstellung von Storagespace, Speicherung von E-Mails, Bereitstellung von Datenbanken, Registrierung von Domains und Skripten sowie Dienstleistungen, die in einem individuellen Vertrag festgehalten werden. Der Auftrag umfasst alle notwendigen Arbeiten zur Erbringung dieser

Dienstleistungen. Dies umfasst Tätigkeiten, die in den Angeboten / Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses 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 (»Verantwortung des für die Verarbeitung Verantwortlichen« im Sinne des Art. 24 EU-DSGVO).

Die Art der personenbezogenen Daten und der Verarbeitungszweck werden in Anlage 1 näher beschrieben (vom Auftraggeber auszufüllen).

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

§ 3 Laufzeit, Beendigung, Löschung von Daten

(1) Die Laufzeit des Vertrages richtet sich nach der Dauer der Erbringung von Hosting-Leistungen des Auftragnehmers an den Auftraggeber. Der Auftrag endet, wenn der Auftraggeber keine Hosting- Leistungen des Auftragnehmers, entsprechend den Leistungsvereinbarungen/Angeboten der einzelnen Auftragsbestätigungen für Hosting-Leistungen des Auftragnehmers, mehr in Anspruch nimmt.

(2) Die Rechte der durch den Datenumgang bei dem Auftragnehmer betroffenen Personen, insbesondere auf Berichtigung, Löschung und Sperrung, sind gegenüber dem Auftraggeber geltend zu machen. Er ist allein verantwortlich für die Wahrung dieser Rechte.

(3) Nach Ende des Auftrags oder auf schriftliche Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche Daten des Auftraggebers vollständig datenschutzgerecht zu löschen (einschließlich der verfahrens- oder sicherheitstechnisch notwendigen Kopien) oder an den Auftraggeber zurückzugeben. Das gleiche gilt auch für Test- und Ausschussmaterial, das bis zur Löschung oder Rückgabe unter datenschutzgerechtem Verschluss zu halten ist. Dies gilt nicht für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen oder soweit z.B. rechtliche Regelungen, gesetzliche Pflichten oder gerichtliche Verfügungen dem entgegenstehen. Entstehen durch eine Löschung vor Vertragsbeendigung zusätzliche Kosten, so trägt diese der Auftraggeber.

(4) Der Auftragnehmer ist verpflichtet, im Rahmen seiner Tätigkeit für den Auftraggeber an ihn gerichtete Ersuchen Betroffener zur sachgerechten Bearbeitung unverzüglich an den Auftraggeber weiterzuleiten. Er ist nicht berechtigt, diese Ersuchen ohne Abstimmung mit dem Auftraggeber selbständig zu bescheiden.

(5) Der Auftragnehmer hat den Auftraggeber bei der Umsetzung der Rechte der Betroffenen nach Kapitel III der DSGVO, insbesondere im Hinblick auf Berichtigung, Sperrung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen der technischen Möglichkeiten, insbesondere hinsichtlich des Charakters der geschuldeten Dienstleistung, zu unterstützen. 2.6 Zu einem Datenträgeraustausch gemäß Art. 28 Abs. 3 lit. g DSGVO zwischen den Beteiligten dieser Auftragsverarbeitung kommt es nicht. Insoweit ist eine Rückgabe nicht zu regeln.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf die Daten des Auftraggebers (Anlage 1) nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten. Kosten für über den vertraglich vereinbarten Leistungsumfang hinausgehende Einzelweisungen des Auftraggebers, sind nach Rücksprache mit dem Auftragnehmer, unter Berücksichtigung des Aufwands, vom Auftraggeber zu tragen.

(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 gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO genügen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. Diese Maßnahmen sind in Anlage 2 näher beschrieben. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen per Verpflichtung untersagt ist, die Daten unbefugt zu verarbeiten (Datengeheimnis entsprechend § 53 BDSG-neu). Das Datengeheimnis besteht auch nach Beendigung des Auftrages fort.

(4) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden, bei schwerwiegenden Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder die im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten nach Art. 34 EU-DSGVO.

(5) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(6) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 34 EU-DSGVO und § 5 BDSG-neu nachzukommen, wie z.B. seiner Pflicht, einen Datenschutzbeauftragen zu bestellen, soweit vom Gesetz vorgeschrieben. Er gewährleistet weiterhin, seinen Pflichten nach Art. 32 Abs. 1 lit. d) EU-DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(7) Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung.

(8) Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Entstehen dabei durch Aufwand oder Gebühren dritter Kosten, trägt diese der Auftraggeber. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag bereits vereinbart. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

§ 5 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

(3) Dem Auftraggeber obliegen die aus Artt. 33, 34 EU-DSGVO resultierenden Informationspflichten.

(4) Die Daten werden nach dem Ende des jeweiligen Vertrages gelöscht. Es obliegt dem Auftraggeber, Sicherungskopien von seinen Daten anzufertigen und die Daten vor Vertragsende umzuziehen. Der Auftraggeber hat selbst Zugriff auf seine Daten. Eine Pflicht des Auftragnehmers zur Herausgabe besteht daher nicht.

§ 6 Anfragen Betroffener

(1) Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Verarbeitung von Daten dieser Person zu erteilen, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen. Dies setzt voraus, dass der Auftraggeber den Auftragnehmer hierzu schriftlich oder in Textform aufgefordert hat und der Auftraggeber dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten erstattet. Der Auftragnehmer wird keine Auskunftsverlangen beantworten und den Betroffenen insoweit an den Auftraggeber verweisen.

(2) Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung oder Sperrung an den Auftragnehmer, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen.

§ 7 Kontrollpflichten

(1) Der Auftraggeber kann sich auf seine Kosten vor der Aufnahme der Datenverarbeitung und sodann regelmäßig über die technischen und organisatorischen Maßnahmen des Auftragnehmers informieren und das Ergebnis dokumentieren. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich ein ggf. vorhandenes Testat eines Sachverständigen vorlegen lassen oder nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Bei der Prüfung muss mindestens ein Mitarbeiter des Auftragnehmers anwesend sein. Jeder Schritt ist mit diesem abzuklären. Entstandene Kosten für Anfahrt und Arbeitszeit des Auftragnehmers, trägt der Auftraggeber. Für die Unterstützung bei der Durchführung einer Prüfung darf der Auftragnehmer eine Vergütung verlangen, wenn dies im Vertrag vereinbart ist. Der Aufwand einer Prüfung ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle erforderlich sind. Dafür entstehende Kosten trägt der Auftraggeber.

§ 8 Subunternehmer

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungspflichten verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. dritte Unternehmen mit Leistungen unterbeauftragt.

(2) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages. Eine etwaige Prüfung durch den Auftraggeber beim Subunternehmer erfolgt nur in Abstimmung mit dem Auftragnehmer.

(3) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post- und Versanddienstleistungen oder Wartung. Der Auftragnehmer wird mit diesem Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

§ 9 Informationspflichten, Schriftformklausel, Annahmeerklärung, AGB

(1) 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. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »verantwortlicher Stelle« im Sinne des Bundesdatenschutzgesetzes liegen.

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

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Im Übrigen gelten die Allgemeinen Geschäftsbedingungen (kurz AGB) des Auftragnehmers.

§ 10. Salvatorische Klausel, Gerichtsstand

(1) Sollte eine Bestimmung dieses Vertrages ungültig oder undurchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieses Vertrages hiervon unberührt. Die Parteien vereinbaren, die ungültige oder undurchsetzbare Bestimmung durch eine gültige und durchsetzbare Bestimmung zu ersetzen, welche wirtschaftlich der Zielsetzung der Parteien am nächsten kommt. Das Gleiche gilt im Falle einer Regelungslücke.

(2) Es gilt deutsches Recht.

(3) Als Gerichtsstand wird Münster vereinbart

Datum _____

Unterschrift Auftraggeber _____

Datum _____

Unterschrift Auftragnehmer _____

Übermitteln Sie die vorliegende Vereinbarung per Email/PDF an F.J.Drewer-Gutland: info@nettrix.de

Die Vereinbarung wird mit Unterschrift von/durch F.J. Drewer-Gutland rechtskräftig.

Anlagen: Anhang 1 – Auflistung der personenbezogenen Daten und Zweck ihrer Verarbeitung
Anhang 2 – Allgemeine technisch-organisatorische Maßnahmen nach Art. 32 EU-DSGVO

Anhang 1 - Auflistung der personenbezogenen Daten und Zweck ihrer Verarbeitung

1. Umfang, Art und Zweck der Datenverarbeitung Datenverarbeitungszweck ist die Erbringung der technischen Leistungen für die Bereitstellung der Dienstleistungen von nettrix e.K., wie sie in den Angeboten / Leistungsbeschreibungen und den Allgemeinen Geschäftsbedingungen (kurz AGB) von nettrix e.K. beschrieben werden.

2. Art der Daten Daten, die der Auftraggeber oder von ihm autorisierte Nutzer in den bereit gestellten Paketen (Webhosting-Pakete, StorageSpace, dedizierte, virtuelle Server und Root Server, managed Server und vServer, E-Mail-Pakete, Groupware) speichern (Inhalt der Webseiten, des Online-Speichers, der Datenbanken etc.)

(durch den Auftraggeber vollständig und richtig auszufüllen/anzukreuzen!)

□ Abrechnungsdaten □ Adressdaten □ Angebotsdaten □ Authentifizierungsdaten □ Bankverbindungsdaten □ Bestelldaten □ Bilddaten □ E-Mails □ Finanzdaten	□ Mitarbeiterdaten □ Nutzungsdaten □ Passwortdateien □ Personaldaten □ Programmcode □ Profildaten □ Stammdaten □ Transaktionsdaten □ Vertragsdaten	□ Videodateien □ Weitere Betroffene:

Kategorien besonderer personenbezogener Daten:

□ Biometrische Daten □ Genetische Daten □ Gesundheitsdaten □ Daten von Kindern □ Daten zu politischen Meinungen	Daten über rassische und ethnische Herkunft □ Daten zu religiösen oder weltanschaulichen Überzeugungen □ Daten zur Gewerkschaftszugehörigkeit □ Daten zum Sexualleben oder sexuellen Orientierung □ Daten zur Bewertung der Persönlichkeit, der Fähigkeiten, der Leistung oder des Verhaltens

3. Kreis der von der Datenverarbeitung Betroffenen (durch den Auftraggeber vollständig und richtig auszufüllen/anzukreuzen!)

□ Angehörige □ Auszubildende □ Bewerber □ Berater □ Dienstleister □ Geschädigte □ Geschäftspartner □ Gesellschafter □ ehemalige Mitarbeiter	□ Interessenten □ Kunden □ Lieferanten □ Makler / Vermittler □ Mieter □ Mitarbeiter □ Mitglieder □ Nutzer □ Praktikanten	□ Unterhaltsberechtigte □ Presse □ Zeugen □ Weitere Betroffene:

Anhang 2 Allgemeine technisch-organisatorische Maßnahmen nach Art. 32 EU-DSGVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)

• Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:
• Zugänge zu den Büroräumen grundsätzlich verschlossen
• Schließsystem mit Sicherheitsschlössern
• Öffnen der Zugangstüren nur mit Schlüssel
• Besucherregelung: Abholung von Besuchern (nach Klingeln) am Eingang
• Spezielle Räume abschließbar
• Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

• Firewall, Intrusion Detection System
• Zugang zu DV-Geräten mit persönlicher Benutzer-ID und Kennwort
• Zusätzliches Login für spezielle Applikationen
• Kennwort: > 8 Zeichen, bestehend aus Sonderzeichen, Groß- und Kleinbuchstaben sowie Zahlen (3 aus 4)
• Bei Bedarf zeitgesteuerte Kennwort-Erneuerung
• Home Partition der Arbeitsplatzrechner verschlüsselt
• Verbindung zur Applikation im Rechenzentrum nur über SSL
• Für Kundensysteme bei Bedarf Zwei-Faktor-Authentifizierung
• Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

• Benutzerrollen-/Gruppenkonzept
• Erteilung und Verwaltung von Benutzerechten voneinander getrennt
• Überprüfung/Aktualisierung der Berechtigungen
• Zentrales Virenschutzprogramm mit automatischer Aktualisierung
• Zeitgesteuerte Bildschirmsperre mit Wiederanmeldung
• Bildschirme so aufgestellt, dass ein unbefugtes Lesen verhindert wird

• Trennungskontrolle Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:
• Firmendaten (Buchhaltung, Personalverwaltung etc.) physikalisch getrennt
• Trennung von Entwicklungs- und Produktionsumgebung

2. Integrität (Art. 32 Abs. 1 lit. b EU-DSGVO)

• Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Abhängig vom Projekt
• Zugang über VPN
• Verschlüsselte Übertragung
• Identifizierung / Authentifizierung
• Regelungen für Datenträgervernichtung
• Eine technisch notwendige Zugriffsmöglichkeit auf alle übertragenen Daten besteht im Rahmen der Verwaltung der Netzwerkhardware (Router, Switches). Dieser Zugriff ist auf die Mitarbeiter des Teams des Auftragnehmers beschränkt und dient ausschließlich zur Gewährleistung des technischen Betriebes. Eine Selektierung personenbezogener Daten ist dabei nicht möglich. Dem Kunden obliegt es durch eine Verschlüsselung, z.B. SSL dafür zu sorgen, dass die übertragenen Daten nicht lesbar sind.
• Der Auftragnehmer hat bei unmanaged Produkten keinen Zugriff auf durch den Kunden verarbeitete personenbezogene Daten – außer der Kunde beauftragt den Auftragnehmer mit administrativen Aufgaben auf seinen Systemen. Bei Änderungen durch den Auftragnehmer werden die Administrationszugriffe protokolliert. Der Zugriff erfolgt durch geschulte und auf das Datengeheimnis verpflichtete Administratoren. Sämtliche administrative Aufgaben finden über gesicherte Wege, wie bspw. SSL-verschlüsselt, statt.
• Bei managed-Produkten verfügt der Auftragnehmer über organisatorische Maßnahmen, welche den Zugriff auf die Systeme regelt um den Systembetrieb sicherzustellen. Sämtliche administrative Aufgaben finden über gesicherte Wege, wie bspw. SSL-verschlüsselt, statt. Der Zugriff erfolgt durch geschulte und auf das Datengeheimnis verpflichtete Administratoren. Die Anzahl der Mitarbeiter werden vom Auftragnehmer möglichst gering gehalten. Bei Änderungen durch den Auftragnehmer werden die Administrationszugriffe adäquat protokolliert.
• Eingabekontrolle Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
• Die Datenverarbeitung erfolgt durch den Kunden. Der Auftragnehmer hat keinen Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme, so dass die Eingabekontrolle der Daten ausschließlich durch den Kunden umgesetzt werden kann.
• Protokollierung bei Eingabe, Änderung und Löschung von Daten
• Regelungen zum Zugriff und zur Löschung der Protokolle

3. Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit

(Art. 32 Abs. 1 lit. b, c EU-DSGVO)
• Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind:

• Alle Server stehen in Rechenzentren in Deutschland
• Rechenzentren sind DIN ISO 27001-zertifiziert Schutzmaßnahmen
• Geeignete Zutrittskotrollsysteme
• Videoüberwachung
• Redundante unterbrechungsfreie Stromversorgung
• Überspannungsschutz o Schutz gegen Feuer und Wassereintritt
• Monitoring der Leitungskapazitäten ◦ Intrusion Detection System (DoS/DDoS-Angriffe)
• Redundante IT-Infrastruktur (z.B. durch Virtualisierung)
• Datensicherungskonzept vorhanden
• Prüfung der Rücksicherung/Wiederherstellung
• Virenscanner und Firewalls im Einsatz

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO)

• Auftragskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:
• Zwischen Auftragnehmer und evtl. Unterauftragnehmer werden bei Bedarf ein ADV-Verträge geschlossen.

Datenschutz-Management
• Es ist ein Datenschutzmanagementsystem implementiert, mit dessen Hilfe die Nachweispflichten der EUDSGVO und des BDSG-neu umgesetzt werden:
• Rechtsgrundlagen der Verarbeitung, Art.6 DSGVO
• Erteilung der Einwilligung, Art.7 DSGVO
• Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person, Art.12 DSGVO
• Einhaltung der Informationspflichten, Art.13 DSGVO
• Datenschutz durch Technik, Art.25 DSGVO
• Auskunftsrecht der betroffenen Person, Art.15 DSGVO
• Recht auf Berichtigung, Art.16 DSGVO
• Recht auf Löschung, Art.17 DSGVO
• Umsetzung der Speicherbegrenzung, Art.5 DSGVO
• Umsetzung der Sicherheit der Verarbeitung, Art.32 DSGVO
• Auflistung aller Auftragsverarbeiter, Art.30 Abs.2 DSGVO
• Umgang mit Datenschutzverletzungen, Art.33 DSGVO
• Darstellung der Meldepflicht an Aufsichtsbehörden, Art.33 DSGVO
• Verwendung von Werkzeug Zertifizierung, Art.42 DSGVO
• Risikobewertung / Datenschutzfolgenabschätzung, Art.35 DSGVO
• Dokumentation von Audits • Dokumentation von Awareness-Maßnahmen

Incident-Response-Management
• Ein organisatorischer und technischer Prozess zum Umgang mit Sicherheitsvorfällen (incidents) ist definiert und implementiert. Hierüber wird auch eine einheitliche Reaktion sowie ein prozessualisierter Umgang mit erkannten und vermuteten Sicherheitsvorfällen/Störungen sichergestellt. Ebenfalls erfolgt im Rahmen dessen, eine einheitliche Nachbereitung und Kontrolle im Sinne eines kontinuierlichen Verbesserungsprozesses.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DSGVO)
• Es sind technisch-organisatorische Maßnahmen getroffen, die sicherzustellen, dass die im Customer Control Panel (CCP) verarbeiteten Daten lt. den Vorgaben von Art. 25 Abs. 2 EU-DSGVO verarbeitet werden.

Ansprechpartner
Franz-Josef Drewer-Gutland
Staufenstr.40
48145 Münster
0171-9909729
info@nettrix.de