(V. 1.1-D1.D2.B1 - 2018/06)

VERTRAG ZUR AUFTRAGSVERARBEITUNG

gemäß Art. 28 DSGVO

zwischen

- [**Anne und Klaus Jensen**
  Unternehmensbezeichnung / Firma

  [**Westertilli 23**
  Straße, Hausnummer

  [**25849 Pellworm**
  PLZ, Stadt

  [**Deutschland**
  Land

- im Folgenden „ Auftraggeber “ genannt –

und der Firma

- **prohost networks GmbH**
  Wilhelm-Külz-Str. 69
  14532 Stahnsdorf (b. Berlin)
  DE

- im Folgenden „ Auftragnehmer “ genannt –

1. Allgemeine Bestimmungen und Vertragsgegenstand

1.1 Gegenstand des vorliegenden Vertrages ist die Bereitstellung von Webhosting-Dienstleistungen sowie der damit im Zusammenhang stehenden Leistungen wie Speicherplatz, Domains, DNS, E-Mail, SSL-Zertifikate, dedizierte Server, etc. Im Rahmen dieses Vertrages hat der Auftraggeber, abhängig von den Tarifmerkmalen und den individuellen Leistungsvereinbarungen, unter Nutzung eines Webservers, Datenbankservers, FTP- oder SSH-Zugangs die Möglichkeit, Daten zu verarbeiten (speichern, verändern, übertragen, löschen).

1.2 Vertragsgegenstand ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Im Zuge der Leistungserbringung des Auftragnehmers als Dienstleister im Bereich Webhosting, technischer Support sowie Administration von Serversystemen kann ein Zugriff auf personenbezogene Daten des Auftraggebers jedoch nicht ausgeschlossen werden.

1.3 Der Begriff „Daten“ beschreibt im Folgenden ausschließlich personenbezogene Daten im Sinne der DSGVO.

1.4 Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Abs. 7 DSGVO. Er allein ist für Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 DSGVO und die Wahrung der Betroffenenrechte verantwortlich.

1.5 Die Verarbeitung der Daten durch den Auftragnehmer findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers.

2. Art der Daten und Kreis der Betroffenen gemäß Art. 28 Abs. 3 S. 1 DSGVO

2.1 Gegenstand der Verarbeitung personenbezogener Daten sind sämtliche Datenarten/-kategorien, die der Auftraggeber zur Speicherung auf die im Rahmen der Leistungserbringung vom Auftragnehmer zur Verfügung gestellten Serversysteme überträgt. Gleiches gilt für die Kategorien der durch die Verarbeitung betroffenen Personen.

2.2 Der Auftraggeber entscheidet allein und ausschließlich darüber, welche personenbezogenen Daten in welcher Weise verarbeitet werden (Herr der Daten). Die hierfür erforderlichen Programme zur Datenverarbeitung werden durch den Auftraggeber erstellt und auf den Serversystemen des Auftragnehmers eingesetzt. Die Datenverarbeitung selbst erfolgt durch den Auftraggeber. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Auftraggeber durchgeführten Datenverarbeitungsvorgänge.

2.3 Für die Sicherheit und regelmäßige Wartung der vom Auftraggeber für die Verarbeitung personenbezogener Daten auf den Systemen des Auftragnehmers eingesetzte Software, beispielsweise dessen Content Management- oder Shop-System, ist der Auftraggeber selbst verantwortlich. Dies gilt ebenso, wenn der Auftraggeber beispielsweise veraltete PHP- oder MySQL-Versionen zum Betrieb der Software nutzt. Regelmäßige Aktualisierungen sowie Überprüfungen der Protokolle auf unübliche Aktivitäten sind für die Sicherheit von Web-Anwendungen jeglicher Art essentiell.

3. Vertragslaufzeit und Kündigung

3.1 Der Vertrag beginnt zum Zeitpunkt der durch den Auftraggeber erteilten Zustimmung, frühestens jedoch am 25.05.2018. Die Laufzeit des Vertrages richtet sich nach der Dauer der Erbringung von Hosting-Leistungen des Auftragnehmers an den Auftraggeber. Der Vertrag endet, wenn der Auftraggeber keine Leistungen des Auftragnehmers, entsprechend des gebuchten Tarifs bzw. des vereinbarten Leistungsumfangs, mehr in Anspruch nimmt. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

4. Allgemeine Pflichten des Auftragnehmers

4.1 Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragnehmer erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragnehmer dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4.2 Kopien der vertragsgegenständlichen Daten dürfen nur mit Zustimmung des Auftraggebers erstellt werden. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung der ordnungsgemäßen Datenverarbeitung oder Erfüllung vertraglicher oder gesetzlicher Verpflichtungen erforderlich sind.

4.3 Der Auftragnehmer stellt die Einhaltung aller für die Auftragsdurchführung notwendigen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO sicher.

4.4 Sofern der Auftragnehmer zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen in Einklang mit den gesetzlichen Vorschriften ausgewählt hat und sichert dem Auftraggeber zu, diesen unter Angabe seiner Kontaktdaten zu benennen (z.B. per E-Mail). Änderungen und die aktuellen Kontaktdaten des Datenschutzbeauftragten sind der Website des Auftragnehmers zu entnehmen.

4.5 Der Auftragnehmer hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

4.6 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei von ihm oder der bei ihm beschäftigten Personen begangenen Verstößen gegen Datenschutzvorschriften. Gleiches gilt im Falle schwerwiegender Störungen des Betriebsablaufs oder anderen Unregelmäßigkeiten im Umgang mit Daten des Auftraggebers. Soweit den Auftraggeber Pflichten nach Art. 32-36 DSGVO treffen, z.B. im Falle des Abhandenkommens oder der unrechtmäßigen Kenntniserlangung von personenbezogenen Daten durch Dritte, hat der Auftragnehmer ihn hierbei im Rahmen der erbrachten Dienstleistung zu unterstützen.

5. Technische und organisatorische Maßnahmen

5.1 Der Auftragnehmer hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 1 dieses Vertrages festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt und mit dem Auftraggeber abgestimmt.

5.2 Der Auftragnehmer wird die technischen und organisatorischen Maßnahmen bei Bedarf und/oder anlassbezogen überprüfen und anpassen. Wesentliche Änderungen werden vom Auftragnehmer dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt.

6. Unterstützungspflichten des Auftragnehmers

6.1 Der Auftragnehmer wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12-22 DSGVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.

6.2 Der Auftragnehmer wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32-36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen.

6.3 Der Auftragnehmer kann eine Vergütung für Mehraufwendungen verlangen, die ihm bei der Durchführung der in dieser Ziffer genannten Unterstützungspflichten entstehen.

6.4 Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

7. Einsatz von Unterauftragnehmern (Subunternehmer)

7.1 Der Auftragnehmer ist zum Einsatz von Unterauftragnehmern (Subunternehmern) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden Subunternehmerverhältnisse des Auftragnehmers sind diesem Vertrag abschließend in Anlage 2 beigefügt. Für die in Anlage 2 aufgezählten Subunternehmer gilt die Zustimmung mit Abschluss dieses Vertrages als erteilt.

7.2 Beabsichtigt der Auftragnehmer den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber rechtzeitig vor deren Einsatz in schriftlicher oder elektronischer Form anzeigen. Der Auftraggeber hat nach dieser Mitteilung zwei Wochen Zeit, der Hinzuziehung des/der Subunternehmer zu widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Hinzuziehung des/der Subunternehmer(s) als genehmigt. Im Falle eines Widerspruchs dürfen die betroffenen Subunternehmer nicht eingesetzt werden. Widersprüche sind nur zulässig, wenn der Auftraggeber begründete Anhaltspunkte dafür hat, dass durch den Einsatz des Unterauftragnehmers die Datensicherheit oder der Datenschutz eingeschränkt würde, die Einhaltung gesetzlicher oder vertraglicher Bestimmungen gefährdet wäre und/oder sonstige berechtigte Interessen des Auftraggebers entgegenstehen; die entsprechenden Verdachtsmomente sind dem Widerspruch beizufügen.

7.3 Subunternehmer werden vom Auftragnehmer unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Nebenleistungen, die der Auftragnehmer zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse im Sinne des Art. 28 DSGVO dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragnehmer wird jedoch auch bei

diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards (insbesondere durch entsprechende Vertraulichkeitsvereinbarungen) sicherstellen.

8. Pflichten des Auftraggebers

8.1 Der Auftraggeber hat die für ihn geltenden datenschutzrechtlichen Bestimmungen einzuhalten.

8.2 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollumfänglich zu informieren, wenn er einen Verstoß des Auftragnehmers gegen datenschutzrechtliche Regelungen feststellt.

8.3 Der Auftraggeber ist für die Einhaltung der sich aus Art. 13, 14 und Art. 24 DSGVO ergebenden Informationspflichten verantwortlich.

9. Weisungen des Auftraggebers

9.1 Der Auftraggeber hat selbst jederzeit umfassenden Zugriff auf die gespeicherten Daten, sodass es einer Mitwirkung des Auftragnehmers, insbesondere zur Sperrung, Löschung oder Berichtigung, nicht bedarf. Sofern eine Mitwirkung des Auftragnehmers erforderlich ist, ist der Auftragnehmer hierzu gegen angemessene Erstattung der anfallenden Kosten verpflichtet. Dem Auftraggeber steht in diesem Fall ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung gegenüber dem Auftragnehmer zu. Der Auftragnehmer ist verpflichtet, den Weisungen des Auftraggebers Folge leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.

9.2 Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragnehmer substantiiert anzweifelt, ist der Auftragnehmer berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert. Besteht die Möglichkeit, dass der Auftragnehmer durch das Befolgen der Weisung einem Haftungsrisiko ausgesetzt wird, kann die Durchführung der Weisung bis zur Klärung der Haftung im Innenverhältnis ausgesetzt werden.

9.3 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen.

9.4 Der Auftraggeber benennt auf Verlangen des Auftragnehmers eine oder mehrere weisungsberechtigte Personen. Personelle Änderungen sind dem Auftragnehmer unverzüglich mitzuteilen.

10. Nachweismöglichkeiten

10.1 Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach, stellt ihm alle hierfür erforderlichen Informationen zur Verfügung und ermöglicht und unterstützt eine Überprüfung durch den Auftraggeber oder einen von diesem beauftragten Prüfer. Dem Auftraggeber steht hierzu die den gesetzlichen Anforderungen entsprechende Dokumentation über die vorhandenen technischen und organisatorischen Maßnahmen zur Verfügung.

10.2 Sollten im Einzelfall im Rahmen der Überprüfung nach Ziffer 10.1 stichprobenartige Inspektionen durch den Auftraggeber oder einem von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung und mit einer angemessenen Vorlaufzeit durchgeführt. Die Maßnahme muss verhältnismäßig sein und der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich im Rahmen der Prüfung ggf. berührter Betriebs- und Geschäftsgeheimnisse des Auftragnehmers abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Sämtliche Maßnahmen sind vom Auftragnehmer zu begleiten, alle Schritte sind mit diesem abzustimmen. Sämtliche Kosten, die dem Auftragnehmer durch seine Unterstützungshandlung entstehen, sind ihm in angemessenem Umfang zu erstatten, auch die Kosten für die Anfahrt. Der Aufwand einer Inspektion ist grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

11. Vertragsbeendigung, Löschung und Rückgabe der Daten

11.1 Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrages hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers zu

löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen).

11.2 Zu einem Datenträgeraustausch zwischen den Vertragsparteien nach Art. 28 Abs. 3 lit. g DSGVO kommt es nicht, daher ist eine Rückgabe nicht zu regeln.

12. Haftung

12.1 Der Auftragnehmer haftet gegenüber dem Auftraggeber im Innenverhältnis nicht, wenn die haftungsauslösende Datenverarbeitung / Maßnahme in Folge einer Weisung des Auftraggebers durchgeführt wurde oder durch eine Sicherheitslücke in der genutzten Software des Auftraggebers (beispielsweise in dessen Content Management- oder Shop-System oder bei Nutzung veralteter PHP- oder MySQL-Versionen, etc.) ausgelöst wurde. Das gleiche gilt für Maßnahmen, die mit dem Auftraggeber abgestimmt wurden (z.B. TOMs nach Art. 32 DSGVO). Als Abstimmung gilt es auch, wenn eine Regelung in diesem Vertrag auf Verlangen des Auftraggebers eingefügt wurde. Im Übrigen bleiben die gesetzlichen Haftungsregelungen (insb. Art. 82 DSGVO) unberührt.

13. Schlussbestimmungen

13.1 Änderungen dieses Vertrages und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

13.2 Als Gerichtsstand wird Potsdam vereinbart.

13.3 Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

13.4 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

13.5 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

Für den Auftraggeber zugestimmt von:

- [**Klaus Jensen** _____
  Vorname / Nachname

am **29.06.2018** **um** **13:59** **Uhr MEZ**

von der IP-Adresse **37.201.226.69**

Für den Auftragnehmer:

- [_____
  Roger Mayer

prohost networks GmbH, Geschäftsführer

(V. 1.1-D1.D2.B1 - 2018/06)

Anlage 1 zum Vertrag zur Auftragsverarbeitung

DOKUMENTATION DER TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN (TOMs)

gemäß Art. 32 DSGVO

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Auftraggeber und der Auftragnehmer die nachfolgenden technischen und organisatorischen Maßnahmen (TOMs), um die vier Schutzziele gem. Art. 32 Abs. 1 lit. b DSGVO:
Vertraulichkeit: Die personenbezogenen Daten vor unbefugtem Zutritt, Zugang und Zugriff zu schützen;
Integrität: Die personenbezogenen Daten vor Veränderung oder Löschung durch Unbefugte zu schützen;
Verfügbarkeit: Dauernde und uneingeschränkte Verfügbarkeit der Systeme, mit denen die personenbezogenen Daten verarbeitet werden, zu gewährleisten;
Belastbarkeit: Gewährleisten, dass die Systeme, mit denen die personenbezogenen Daten verarbeitet werden, punktuellen und andauernden Belastungen standhalten können;
sicherzustellen. Eine rasche Wiederherstellung nach einem physischen oder technischen Zwischenfall ist gewährleistet. Die technischen und organisatorischen Maßnahmen werden regelmäßig auf Wirksamkeit geprüft. Die Maßnahmen gelten für die im Hauptvertrag definierten Leistungen, die vom Auftragnehmer an den unten genannten Standorten erbracht werden.

Stand Mai 2018 unterhält der Auftragnehmer die folgenden, voneinander unabhängigen Datenverarbeitungs-Standorte:

	Bezeichnung	Ort	Typ
•	**Data Center Colo #1**	**12277 Berlin-Süd/Mariendorf, DE**	**Rechenzentrum Colocation**
•	**Data Center Colo #2**	**10785 Berlin-Mitte/Tiergarten, DE**	**Rechenzentrum Colocation**
•	**Data Center Colo #3**	**66386 St. Ingbert, DE**	**Rechenzentrum Colocation**
•	**Data Center Colo #4**	**NY 10011 New York, USA**	**Rechenzentrum Colocation**
•	**Data Center Colo #5**	**CT 06651 Trumbull, USA**	**Rechenzentrum Colocation**
•	**Büroeinheit #1**	**14532 Stahnsdorf (b. Berlin), DE**	**Büros**

An allen Standorten betreibt der Auftragnehmer eigene, selbstverwaltete IT-Systeme (kein Reselling, kein Leasing/Miete/Finanzierung, keine Ansprüche Dritter, kein Zugriff durch Dritte).

Für die einzelnen Standorte werden unterschiedliche technische und organisatorische Maßnahmen (TOMs) getroffen, daher sind diese im Folgenden separat dokumentiert. Nicht alle Standorte sind für das bestehende Vertragsverhältnis mit dem Auftraggeber relevant, insbesondere nicht die Standorte in den USA. Die vertragsrelevanten Standorte ergeben sich aus der nachfolgenden Aufstellung.

TOMs für Standort: Data Center Colo #1, 12277 Berlin-Süd/Mariendorf, DE

An diesem Standort erbringt der Auftragnehmer ausschließlich Rechenzentrums-bezogene Dienstleistungen.

1. Zweckbindung und Trennbarkeit

[Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden]

- Der Auftragnehmer erhebt personenbezogene Daten nur in dem Rahmen, der zur Erbringung der jeweiligen Dienstleistung unbedingt erforderlich ist (Datenminimierung und Zweckbindung)
- Trennbarkeit wird durch physisch oder logisch separierte DV-Systeme, unterschiedliche Speicherorte und/oder separate Datenbanken mit individuellen Berechtigungskonzepten sichergestellt
- Produktiv- und Testsysteme sind getrennt

2. Vertraulichkeit und Integrität der Systeme

[Maßnahmen, die Vertraulichkeit und Integrität der Systeme des Auftragnehmers gewährleisten]

2.1 Zutrittskontrolle

[Maßnahmen, die unbefugte Dritte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, hindern]

- Zutrittsgeschützte Rechenzentrumsflächen
- Alarmsysteme und Kameraüberwachung, mit Aufschaltung bei Sicherheitsdienst
- Alle Türen werden überwacht und sind mit Alarmierungsmechanismen gegen unbefugtes Öffnen geschützt, gleiches gilt bis zum 2. OG auch für die Fenster
- Kameraüberwachung aller Rechenzentrumsflächen und Gänge
- Zusätzliche Überwachung aller Flächen mit Bewegungsmeldern
- Auslösung eines Alarms wird unmittelbar an den Sicherheitsdienst und die verantwortlichen Mitarbeiter des Betreibers übermittelt
- Zutritt aller Rechenzentrumsflächen ausschließlich für autorisierte Personen
- Digitale Zutrittskontrollsysteme mit personengebundenen Transpondern und individuellen Zutrittscodes (Wissen und Besitz)
- Individuelle, personengebundene Zutrittsfreigabe für zuvor definierte Zeitfenster
- Protokollierung von Zutrittsaktivitäten (An-/Abmeldungen, Verweigerungen, etc.)
- Zutritt zu den Rechenzentrumsflächen nur über kameraüberwachte Schleusen. Gleichzeitiges Öffnen beider Schleusentüren führt zu Alarmauslösung
- Automatische Schließung von Türen
- Als Serverschränke werden geschlossene Stahl-Racks eingesetzt, die jeweils front- und rückseitig separat verschlossen sind
- Gehäuse der einzelnen Rack-Server zusätzlich mit Chassis Intrusion Detection, Alarmierung des zuständigen Mitarbeiters des Auftragnehmers bei Öffnung des Gehäuses
- Rechenzentrum ist durch den Betreiber TÜV zertifiziert nach ISO 27001

2.2 Zugangskontrolle

[Maßnahmen, die die Nutzung der Systeme durch unbefugte Dritte verhindern]

- Einsatz von Hardware-Firewalls
- Einsatz von Software-Firewalls
- Sperrung aller nicht benötigten TCP- und UDP-Ports
- Zentraler Einsatz von Firewall-Blacklists zur Aussperrung von Netzen und IPs bekannter Angreifer, gesteuert in Echtzeit durch die vom Auftragnehmer eingesetzten Intrusion Detection Systeme (IDS) sowie durch automatischen Abgleich mit verschiedenen, etablierten Blacklist-Betreibern
- Dokumentation aller erfolgreichen Logins und Login-Fehlversuche
- Automatische Aussperrung von Client IP-Adressen nach zu vielen Login-Fehlversuchen
- Zugang zu den DV-Systemen des Auftragnehmers erfolgt ausschließlich über sichere Schlüsselauthentifizierung mit Passphrase bzw. durch eindeutige Benutzerkennungen und Passwörter

- Administration der Systeme erfolgt durch den Auftragnehmer über ein physisch getrenntes Out-of-Band Netzwerk, welches mit eigener Hard- und Software-Firewall ausgestattet und welches ausschließlich über VPN zugänglich ist
- Zugang zum VPN ist nur von autorisierten Workstations bzw. Clients ausgehend und auch nur mit gültiger, nutzerbezogener Authentifizierung möglich, Zugriffe werden protokolliert und überwacht
- Physisch separierte WAN-, LAN- und KVM-Management-Netzwerke für alle Server und Netzwerkkomponenten, jeweils über separate Ports, Switches und Zuleitungen
- Serverzugriff auf Administrationsebene erfolgt ausschließlich über die isolierten LAN- bzw. Management-Netze, mit sicherer Schlüsselauthentifizierung und Passphrase und ausgehend von einer sicheren Linux-basierenden Management-Instanz vor Ort im Data Center, kein direkter Remote-Zugriff auf Administrationsebene über WAN/Internet möglich
- Der Auftragnehmer verfügt über eigene, autarke, beim RIPE NCC registrierte IP-Netze
- Alle produktiv eingesetzten Server sind Linux-basierend (kein Einsatz von MS Windows als Server-OS)
- Regelmäßige Software-Updates und -Patches
- Software-Updates und -Patches werden vor Einspielung in die Produktivsysteme auf separaten Entwicklungssystemen getestet
- Verschlüsselung mobiler IT-Systeme und Datenträger

2.3 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]

- Zuordnung von Benutzerprofilen zu IT-Systemen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Bestehende Berechtigungen werden regelmäßig überprüft
- Passwort- und Schlüssellängen-Richtlinien (Mindestlänge, Komplexität, etc.)
- Physische Trennung der vom Auftragnehmer verarbeiteten personenbezogenen Daten des Auftraggebers auf separaten Serversystemen (z.B. Kundenstammdatenverwaltung, Buchhaltung, etc.)
- Trennung von Administrations- und Benutzerzugängen
- Physische Trennung von Entwicklungs- und Produktivsystemen

Für die Sicherheit und regelmäßige Wartung der vom Auftraggeber auf den Systemen des Auftragnehmers eingesetzten Software, beispielsweise dessen Content Management- oder Shop-System, ist der Auftraggeber selbst verantwortlich. Dies gilt ebenso, wenn der Auftraggeber beispielsweise veraltete PHP- oder MySQL-Versionen zum Betrieb der Software nutzt. Regelmäßige Aktualisierungen sowie Überprüfungen der Protokolle auf unübliche Aktivitäten sind für die Sicherheit von Web-Anwendungen jeglicher Art essentiell.

2.4 Eingabekontrolle

[Maßnahmen, mit denen nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind]

- Separate, dienstbezogene Protokollierung über Eingabe, Änderung und Löschung von Daten, z.B. bei FTP-Zugriff
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle, eindeutige Benutzernamen (nicht Benutzergruppen)
- Protokollierung der Aktivitäten, die über die Server-Verwaltungsoberfläche des Auftraggebers durchgeführt werden, Protokoll ist für den Auftraggeber jederzeit online abrufbar
- Protokollierung aller erfolgreichen Logins sowie aller Login-Fehlversuche für die vom Auftragnehmer bereitgestellten Dienste

2.5 Auftragskontrolle

[Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können]

- Siehe Maßnahmen unter Ziffer 2.2 (Zugangskontrolle) und 2.3 (Zugriffskontrolle)
- Schriftliche Verpflichtung der Mitarbeiter auf Wahrung der Vertraulichkeit (NDA)

- Schriftliche Verpflichtung der Mitarbeiter auf Anwendung grundlegender, anerkannter Sicherheitsstandards im Umgang mit IT-Systemen
- Schriftliche Verpflichtung der Mitarbeiter auf Einhaltung der geltenden Datenschutzbestimmungen im Umgang mit personenbezogen Daten
- Auswahl der Unterauftragnehmer erfolgt unter Sorgfaltsgesichtspunkten, insbesondere hinsichtlich Datensicherheit
- Vorherige Prüfung der beim Unterauftragnehmer getroffenen Sicherheitsmaßnahmen
- Schriftliche Weisungen an den Unterauftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)

2.6 Transport- bzw. Weitergabekontrolle

[Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der Übertragung oder Weitergabe, physisch und/oder digital, nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können]

- Personenbezogene Daten des Auftraggebers werden durch den Auftragnehmer nur an berechtigte Empfänger (z.B. Banken im Rahmen des Zahlungsverkehrs oder die zur Registrierung eines Domainnamens oder eines SSL-Zertifikats mindestens erforderlich sind) elektronisch übertragen. Dazu werden ausschließlich sicher verschlüsselte Verbindungen eingesetzt
- Die Serversysteme des Auftragnehmers unterstützen gängige Verschlüsselungsverfahren für alle verfügbaren Kommunikationswege (z.B. Verschlüsselung des Verwaltungszugangs, des E-Mail-Verkehrs, etc.). Sicherheit vor unbefugtem Zugriff auf die übertragenen Daten durch Dritte im Kommunikationsweg kann nur dann gewährleistet werden, wenn der Auftraggeber seinerseits sichere Programme mit geeigneter Verschlüsselung einsetzt und die Verschlüsselung in diesen Programmen auch korrekt aktiviert und konfiguriert
- Beim Versand von E-Mails kann eine Übertragung unverschlüsselt vorkommen, wenn der Empfänger oder die vom Auftraggeber zum Versand eingesetzten Programme keine Verschlüsselung unterstützen. Um dem vorzubeugen kann der Auftraggeber eine Ende-zu-Ende-Verschlüsselung wie bspw. PGP in sein E-Mail-Programm implementieren
- Physische Datenträger werden bei Transport verschlüsselt
- Sichere Datenträgerlöschung (2x full random fill + 1x full zero fill)
- Sichere, physische Vernichtung alter oder fehlerhafter Datenträger

2.7 Anonymisierung, Pseudonymisierung, Verschlüsselung

- Anonymisierung, Pseudonymisierung oder Verschlüsselung der durch den Auftraggeber auf den Systemen des Auftraggebers selbst verwalteten Daten sind grundsätzlich nicht Gegenstand der vom Auftragnehmer zu erbringenden Leistungen
- Der Auftragnehmer stellt jedoch die technische Möglichkeit bereit, IP-Adressen auf Wunsch direkt in der Webserver-Software anonymisieren (verkürzen) zu können sodass diese in den vom Auftraggeber eingesetzten Web-Anwendungen in der anonymisierten Form verarbeitet werden können

3. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

[Maßnahmen, die gewährleisten, dass die eingesetzten Systeme jederzeit einwandfrei funktionieren und dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind]

- Redundante Stromversorgung der Rechenzentrumsflächen über zwei voneinander unabhängige und separat abgesicherte Stromzuführungen (Feeds)
- Unabhängige, unterbrechungsfreie Stromversorgungen (USVs) für beide Feeds
- Filterung von Unregelmäßigkeiten, Störungen und Überspannungen des örtlichen Stromversorgungsnetzes durch die USVs
- Alle Server und kritischen Netzwerkkomponenten sind mit jeweils zwei redundanten Netzteilen ausgestattet, die über unabhängige Strom-Feeds gespeist werden
- Zusätzlich unterbrechungsfrei zuschaltbare Dieselaggregate für unbegrenzt autonomen Betrieb aller Systeme, Dieselvorrat für 24h, Verträge über kurzfristige Nachlieferung von Diesel vorhanden
- Redundante Klimasysteme
- Umgebungstemperaturzonen- und Feuchtigkeitsüberwachung
- Rauch/Brand-Frühesterkennung
- Hochdruck-Löschanlage mit Argon-Inertgas, flutet bei Rauch- oder Brandentwicklung die Räume in kürzester Zeit vollständig mit Löschgas

- Ausfallsichere, redundante Datenträger-Spiegelung für alle produktiv eingesetzten Server (Hardware RAID über separate Controller-Karten, keine Nutzung von on-Board Controllern)
- Fehlerhafte Datenträger, Netzteile, RAMs, Lüfter im laufenden Serverbetrieb austauschbar (Hot-Swap)
- Vorhaltung von Ersatz-Komponenten für sämtliche vor Ort produktiv eingesetzte Serversysteme (SSDs, HDDs, RAID-Controller, Mainboards, CPUs, RAMS, Netzteil-Einschübe, Rack-Switches, Kabel, etc.)
- Vorhaltung vorkonfigurierter, sofort betriebsbereiter Ersatz Rack-Server
- Permanente, automatische Überwachung des Gesundheitszustands der jeweiligen Serverhardware und der installierten Komponenten über autarke Management Controller, auch Temperatur-überwachung aller Sensor-Zonen, mit Alarmierung der zuständigen Mitarbeiter
- Zusätzlich regelmäßig manuelle Überprüfung der einzelnen Komponenten der Systeme sowie proaktiver Austausch
- Tägliche Voll-Sicherung aller Daten auf physisch getrennten Systemen über separates, isoliertes LAN
- Vorhaltezeit der Sicherheitsbackups bis zu 90 Tage
- Eine Wiederherstellung von Daten aus den Sicherheitsbackups ist kurzfristig möglich und vom Auftraggeber über die Verwaltungsoberfläche selbst initiierbar
- Zusätzlich zur täglichen vor-Ort-Sicherung erfolgt eine regelmäßige georedundante Voll-Sicherung aller Daten auf physisch getrennte Backup-Systeme in Data Center Colo #2 (Berlin-Mitte/Tiergarten)
- Es besteht eine Direktvernetzung zwischen den DC Colo‘s #1 (Berlin-Süd/Mariendorf) und #2 (Berlin-Mitte/Tiergarten) über ein isoliertes LAN
- Die Übermittlung der Backup-Daten zwischen den Standorten erfolgt sicher verschlüsselt über das isolierte LAN, nicht über das Internet
- Alle geschäftsrelevanten Daten des Auftragnehmers werden im Rahmen eines strukturierten Backup-Plans in regelmäßigen Abständen gesichert. Dies gilt auch und besonders für personenbezogene Daten. Der ordnungsgemäße Durchlauf der Backup-Tasks wird regelmäßig kontrolliert
- Der Auftragnehmer setzt wirksame, proprietäre und ständig weiterentwickelte IDS-Systeme zur permanenten Überwachung sämtlicher Dienste auf korrekte Verfügbarkeit sowie auf unübliche Aktivitäten ein, mit sofortiger Alarmierung der zuständigen Mitarbeiter
- Intelligentes Traffic-Monitoring aller Kunden-Websites und Server mit Alarmierung der zuständigen Mitarbeiter bei plötzlich erhöhtem übertragenen Datenvolumen oder anderen unüblichen Zugriffsmustern
- Zugriffe und Zugriffsversuche auf die administrativen Serverzugänge, die dem Auftraggeber zur Verfügung stehen, werden protokolliert, um missbräuchliche Aktivitäten und Zugriffsmuster automatisiert zu erkennen
- Der Auftragnehmer setzt proprietäre, eigenentwickelte Software zur Überwachung sämtlicher Systeme sowie für die Verwaltungs- und -Management-Zugänge ein, in deren Entwicklung über 20 Jahre Branchenerfahrung eingeflossen sind
- Permanente Überwachung aller auf den Servern laufenden Prozesse (Tasks) und Netzwerkaktivitäten auf unübliche Betriebszustände/Aktivitäten sowie auf Ausführung unbekannter Prozesse oder unüblicher Verarbeitungsketten. Die auslösenden Prozesse werden durch die IDS zwangsbeendet. Alle verdächtigen Aktivitäten lösen eine Alarmierung der zuständigen Mitarbeiter aus (Push Alarm, Konsolenmeldung und E-Mail Alarmierung) und werden automatisch protokolliert
- Zusätzlich minütlich lokale sowie externe Überwachung aller Systeme und Dienste auf korrekte Verfügbarkeit, mit sofortiger Alarmierung der zuständigen Mitarbeiter bei Unregelmäßigkeiten

Penetrationstests der eigenen Systeme, Dienste und Anwendungen des Auftraggebers sind grundsätzlich nicht Gegenstand der vom Auftragnehmer zu erbringenden Leistungen.

4. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragnehmer wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen regelmäßig prüfen, evaluieren und bei Bedarf anpassen.

TOMs für Standort: Data Center Colo #2, 10785 Berlin-Mitte/Tiergarten, DE

An diesem Standort erbringt der Auftragnehmer ausschließlich Rechenzentrums-bezogene Dienstleistungen.

1. Zweckbindung und Trennbarkeit

[Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden]

- Der Auftragnehmer erhebt personenbezogene Daten nur in dem Rahmen, der zur Erbringung der jeweiligen Dienstleistung unbedingt erforderlich ist (Datenminimierung und Zweckbindung)
- Trennbarkeit wird durch physisch oder logisch separierte DV-Systeme, unterschiedliche Speicherorte und/oder separate Datenbanken mit individuellen Berechtigungskonzepten sichergestellt
- Produktiv- und Testsysteme sind getrennt

2. Vertraulichkeit und Integrität der Systeme

[Maßnahmen, die Vertraulichkeit und Integrität der Systeme des Auftragnehmers gewährleisten]

2.1 Zutrittskontrolle

[Maßnahmen, die unbefugte Dritte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, hindern]

- Zutrittsgeschützte Rechenzentrumsflächen
- Alarmsysteme und Kameraüberwachung, mit Aufschaltung bei Sicherheitsdienst
- Alle Türen werden überwacht und sind mit Alarmierungsmechanismen gegen unbefugtes Öffnen geschützt, gleiches gilt bis zum 2. OG auch für die Fenster
- Kameraüberwachung aller Rechenzentrumsflächen und Gänge
- Zusätzliche Überwachung aller Flächen mit Bewegungsmeldern
- Auslösung eines Alarms wird unmittelbar an den Sicherheitsdienst und die verantwortlichen Mitarbeiter des Betreibers übermittelt
- Zutritt aller Rechenzentrumsflächen ausschließlich für autorisierte Personen
- Digitale Zutrittskontrollsysteme mit personengebundenen Transpondern und individuellen Zutrittscodes (Wissen und Besitz)
- Individuelle, personengebundene Zutrittsfreigabe für zuvor definierte Zeitfenster
- Protokollierung von Zutrittsaktivitäten (An-/Abmeldungen, Verweigerungen, etc.)
- Zutritt zu den Rechenzentrumsflächen nur über kameraüberwachte Schleusen. Gleichzeitiges Öffnen beider Schleusentüren führt zu Alarmauslösung
- Automatische Schließung von Türen
- Als Serverschränke werden geschlossene Stahl-Racks eingesetzt, die jeweils front- und rückseitig separat verschlossen sind
- Gehäuse der einzelnen Rack-Server zusätzlich mit Chassis Intrusion Detection, Alarmierung des zuständigen Mitarbeiters des Auftragnehmers bei Öffnung des Gehäuses
- Rechenzentrum ist durch den Betreiber TÜV zertifiziert nach ISO 27001

2.2 Zugangskontrolle

[Maßnahmen, die die Nutzung der Systeme durch unbefugte Dritte verhindern]

- Einsatz von Hardware-Firewalls
- Einsatz von Software-Firewalls
- Sperrung aller nicht benötigten TCP- und UDP-Ports
- Zentraler Einsatz von Firewall-Blacklists zur Aussperrung von Netzen und IPs bekannter Angreifer, gesteuert in Echtzeit durch die vom Auftragnehmer eingesetzten Intrusion Detection Systeme (IDS) sowie durch automatischen Abgleich mit verschiedenen, etablierten Blacklist-Betreibern
- Dokumentation aller erfolgreichen Logins und Login-Fehlversuche
- Automatische Aussperrung von Client IP-Adressen nach zu vielen Login-Fehlversuchen
- Zugang zu den DV-Systemen des Auftragnehmers erfolgt ausschließlich über sichere Schlüsselauthentifizierung mit Passphrase bzw. durch eindeutige Benutzerkennungen und Passwörter

- Administration der Systeme erfolgt durch den Auftragnehmer über ein physisch getrenntes Out-of-Band Netzwerk, welches mit eigener Hard- und Software-Firewall ausgestattet und welches ausschließlich über VPN zugänglich ist
- Zugang zum VPN ist nur von autorisierten Workstations bzw. Clients ausgehend und auch nur mit gültiger, nutzerbezogener Authentifizierung möglich, Zugriffe werden protokolliert und überwacht
- Physisch separierte WAN-, LAN- und KVM-Management-Netzwerke für alle Server und Netzwerkkomponenten, jeweils über separate Ports, Switches und Zuleitungen
- Serverzugriff auf Administrationsebene erfolgt ausschließlich über die isolierten LAN- bzw. Management-Netze, mit sicherer Schlüsselauthentifizierung und Passphrase und ausgehend von einer sicheren Linux-basierenden Management-Instanz vor Ort im Data Center, kein direkter Remote-Zugriff auf Administrationsebene über WAN/Internet möglich
- Der Auftragnehmer verfügt über eigene, autarke, beim RIPE NCC registrierte IP-Netze
- Alle produktiv eingesetzten Server sind Linux-basierend (kein Einsatz von MS Windows als Server-OS)
- Regelmäßige Software-Updates und -Patches
- Software-Updates und -Patches werden vor Einspielung in die Produktivsysteme auf separaten Entwicklungssystemen getestet
- Verschlüsselung mobiler IT-Systeme und Datenträger

2.3 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]

- Zuordnung von Benutzerprofilen zu IT-Systemen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Bestehende Berechtigungen werden regelmäßig überprüft
- Passwort- und Schlüssellängen-Richtlinien (Mindestlänge, Komplexität, etc.)
- Physische Trennung der vom Auftragnehmer verarbeiteten personenbezogenen Daten des Auftraggebers auf separaten Serversystemen (z.B. Kundenstammdatenverwaltung, Buchhaltung, etc.)
- Trennung von Administrations- und Benutzerzugängen
- Physische Trennung von Entwicklungs- und Produktivsystemen

Für die Sicherheit und regelmäßige Wartung der vom Auftraggeber auf den Systemen des Auftragnehmers eingesetzten Software, beispielsweise dessen Content Management- oder Shop-System, ist der Auftraggeber selbst verantwortlich. Dies gilt ebenso, wenn der Auftraggeber beispielsweise veraltete PHP- oder MySQL-Versionen zum Betrieb der Software nutzt. Regelmäßige Aktualisierungen sowie Überprüfungen der Protokolle auf unübliche Aktivitäten sind für die Sicherheit von Web-Anwendungen jeglicher Art essentiell.

2.4 Eingabekontrolle

[Maßnahmen, mit denen nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind]

- Separate, dienstbezogene Protokollierung über Eingabe, Änderung und Löschung von Daten, z.B. bei FTP-Zugriff
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle, eindeutige Benutzernamen (nicht Benutzergruppen)
- Protokollierung der Aktivitäten, die über die Server-Verwaltungsoberfläche des Auftraggebers durchgeführt werden, Protokoll ist für den Auftraggeber jederzeit online abrufbar
- Protokollierung aller erfolgreichen Logins sowie aller Login-Fehlversuche für die vom Auftragnehmer bereitgestellten Dienste

2.5 Auftragskontrolle

[Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können]

- Siehe Maßnahmen unter Ziffer 2.2 (Zugangskontrolle) und 2.3 (Zugriffskontrolle)
- Schriftliche Verpflichtung der Mitarbeiter auf Wahrung der Vertraulichkeit (NDA)

- Schriftliche Verpflichtung der Mitarbeiter auf Anwendung grundlegender, anerkannter Sicherheitsstandards im Umgang mit IT-Systemen
- Schriftliche Verpflichtung der Mitarbeiter auf Einhaltung der geltenden Datenschutzbestimmungen im Umgang mit personenbezogen Daten
- Auswahl der Unterauftragnehmer erfolgt unter Sorgfaltsgesichtspunkten, insbesondere hinsichtlich Datensicherheit
- Vorherige Prüfung der beim Unterauftragnehmer getroffenen Sicherheitsmaßnahmen
- Schriftliche Weisungen an den Unterauftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)

2.6 Transport- bzw. Weitergabekontrolle

[Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der Übertragung oder Weitergabe, physisch und/oder digital, nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können]

- Personenbezogene Daten des Auftraggebers werden durch den Auftragnehmer nur an berechtigte Empfänger (z.B. Banken im Rahmen des Zahlungsverkehrs oder die zur Registrierung eines Domainnamens oder eines SSL-Zertifikats mindestens erforderlich sind) elektronisch übertragen. Dazu werden ausschließlich sicher verschlüsselte Verbindungen eingesetzt
- Die Serversysteme des Auftragnehmers unterstützen gängige Verschlüsselungsverfahren für alle verfügbaren Kommunikationswege (z.B. Verschlüsselung des Verwaltungszugangs, des E-Mail-Verkehrs, etc.). Sicherheit vor unbefugtem Zugriff auf die übertragenen Daten durch Dritte im Kommunikationsweg kann nur dann gewährleistet werden, wenn der Auftraggeber seinerseits sichere Programme mit geeigneter Verschlüsselung einsetzt und die Verschlüsselung in diesen Programmen auch korrekt aktiviert und konfiguriert
- Beim Versand von E-Mails kann eine Übertragung unverschlüsselt vorkommen, wenn der Empfänger oder die vom Auftraggeber zum Versand eingesetzten Programme keine Verschlüsselung unterstützen. Um dem vorzubeugen kann der Auftraggeber eine Ende-zu-Ende-Verschlüsselung wie bspw. PGP in sein E-Mail-Programm implementieren
- Physische Datenträger werden bei Transport verschlüsselt
- Sichere Datenträgerlöschung (2x full random fill + 1x full zero fill)
- Sichere, physische Vernichtung alter oder fehlerhafter Datenträger

2.7 Anonymisierung, Pseudonymisierung, Verschlüsselung

- Anonymisierung, Pseudonymisierung oder Verschlüsselung der durch den Auftraggeber auf den Systemen des Auftraggebers selbst verwalteten Daten sind grundsätzlich nicht Gegenstand der vom Auftragnehmer zu erbringenden Leistungen
- Der Auftragnehmer stellt jedoch die technische Möglichkeit bereit, IP-Adressen auf Wunsch direkt in der Webserver-Software anonymisieren (verkürzen) zu können sodass diese in den vom Auftraggeber eingesetzten Web-Anwendungen in der anonymisierten Form verarbeitet werden können

3. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

[Maßnahmen, die gewährleisten, dass die eingesetzten Systeme jederzeit einwandfrei funktionieren und dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind]

- Redundante Stromversorgung der Rechenzentrumsflächen über zwei voneinander unabhängige und separat abgesicherte Stromzuführungen (Feeds)
- Unabhängige, unterbrechungsfreie Stromversorgungen (USVs) für beide Feeds
- Filterung von Unregelmäßigkeiten, Störungen und Überspannungen des örtlichen Stromversorgungsnetzes durch die USVs
- Alle Server und kritischen Netzwerkkomponenten sind mit jeweils zwei redundanten Netzteilen ausgestattet, die über unabhängige Strom-Feeds gespeist werden
- Zusätzlich unterbrechungsfrei zuschaltbare Dieselaggregate für unbegrenzt autonomen Betrieb aller Systeme, Dieselvorrat für 24h, Verträge über kurzfristige Nachlieferung von Diesel vorhanden
- Redundante Klimasysteme
- Umgebungstemperaturzonen- und Feuchtigkeitsüberwachung
- Rauch/Brand-Frühesterkennung
- Hochdruck-Löschanlage mit Argon-Inertgas, flutet bei Rauch- oder Brandentwicklung die Räume in kürzester Zeit vollständig mit Löschgas

- Ausfallsichere, redundante Datenträger-Spiegelung für alle produktiv eingesetzten Server (Hardware RAID über separate Controller-Karten, keine Nutzung von on-Board Controllern)
- Fehlerhafte Datenträger, Netzteile, RAMs, Lüfter im laufenden Serverbetrieb austauschbar (Hot-Swap)
- Vorhaltung von Ersatz-Komponenten für sämtliche vor Ort produktiv eingesetzte Serversysteme (SSDs, HDDs, RAID-Controller, Mainboards, CPUs, RAMS, Netzteil-Einschübe, Rack-Switches, Kabel, etc.)
- Vorhaltung vorkonfigurierter, sofort betriebsbereiter Ersatz Rack-Server
- Permanente, automatische Überwachung des Gesundheitszustands der jeweiligen Serverhardware und der installierten Komponenten über autarke Management Controller, auch Temperatur-überwachung aller Sensor-Zonen, mit Alarmierung der zuständigen Mitarbeiter
- Zusätzlich regelmäßig manuelle Überprüfung der einzelnen Komponenten der Systeme sowie proaktiver Austausch
- Tägliche Voll-Sicherung aller Daten auf physisch getrennten Systemen über separates, isoliertes LAN
- Vorhaltezeit der Sicherheitsbackups bis zu 90 Tage
- Eine Wiederherstellung von Daten aus den Sicherheitsbackups ist kurzfristig möglich und vom Auftraggeber über die Verwaltungsoberfläche selbst initiierbar
- Zusätzlich zur täglichen vor-Ort-Sicherung erfolgt eine regelmäßige georedundante Voll-Sicherung aller Daten auf physisch getrennte Backup-Systeme in Data Center Colo #1 (Berlin-Süd/Mariendorf)
- Es besteht eine Direktvernetzung zwischen den DC Colo‘s #2 (Berlin-Mitte/Tiergarten) und #1 (Berlin-Süd/Mariendorf) über ein isoliertes LAN
- Die Übermittlung der Backup-Daten zwischen den Standorten erfolgt sicher verschlüsselt über das isolierte LAN, nicht über das Internet
- Alle geschäftsrelevanten Daten des Auftragnehmers werden im Rahmen eines strukturierten Backup-Plans in regelmäßigen Abständen gesichert. Dies gilt auch und besonders für personenbezogene Daten. Der ordnungsgemäße Durchlauf der Backup-Tasks wird regelmäßig kontrolliert
- Der Auftragnehmer setzt wirksame, proprietäre und ständig weiterentwickelte IDS-Systeme zur permanenten Überwachung sämtlicher Dienste auf korrekte Verfügbarkeit sowie auf unübliche Aktivitäten ein, mit sofortiger Alarmierung der zuständigen Mitarbeiter
- Intelligentes Traffic-Monitoring aller Kunden-Websites und Server mit Alarmierung der zuständigen Mitarbeiter bei plötzlich erhöhtem übertragenen Datenvolumen oder anderen unüblichen Zugriffsmustern
- Zugriffe und Zugriffsversuche auf die administrativen Serverzugänge, die dem Auftraggeber zur Verfügung stehen, werden protokolliert, um missbräuchliche Aktivitäten und Zugriffsmuster automatisiert zu erkennen
- Der Auftragnehmer setzt proprietäre, eigenentwickelte Software zur Überwachung sämtlicher Systeme sowie für die Verwaltungs- und -Management-Zugänge ein, in deren Entwicklung über 20 Jahre Branchenerfahrung eingeflossen sind
- Permanente Überwachung aller auf den Servern laufenden Prozesse (Tasks) und Netzwerkaktivitäten auf unübliche Betriebszustände/Aktivitäten sowie auf Ausführung unbekannter Prozesse oder unüblicher Verarbeitungsketten. Die auslösenden Prozesse werden durch die IDS zwangsbeendet. Alle verdächtigen Aktivitäten lösen eine Alarmierung der zuständigen Mitarbeiter aus (Push Alarm, Konsolenmeldung und E-Mail Alarmierung) und werden automatisch protokolliert
- Zusätzlich minütlich lokale sowie externe Überwachung aller Systeme und Dienste auf korrekte Verfügbarkeit, mit sofortiger Alarmierung der zuständigen Mitarbeiter bei Unregelmäßigkeiten

Penetrationstests der eigenen Systeme, Dienste und Anwendungen des Auftraggebers sind grundsätzlich nicht Gegenstand der vom Auftragnehmer zu erbringenden Leistungen.

4. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragnehmer wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen regelmäßig prüfen, evaluieren und bei Bedarf anpassen.

TOMs für Standort: Büroeinheit #1, 14532 Stahnsdorf (b. Berlin), DE

An diesem Standort führt der Auftragnehmer Büro-bezogene Tätigkeiten durch, hier werden weder Hosting-Server noch andere produktiv eingesetzte Dienste für den Auftraggeber betrieben.

1. Zweckbindung und Trennbarkeit

[Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden]

- Der Auftragnehmer erhebt personenbezogene Daten nur in dem Rahmen, der zur Erbringung der jeweiligen Dienstleistung unbedingt erforderlich ist (Datenminimierung und Zweckbindung)
- Trennbarkeit wird durch physisch oder logisch separierte DV-Systeme, unterschiedliche Speicherorte und/oder separate Datenbanken mit individuellen Berechtigungskonzepten sichergestellt
- Produktiv- und Testsysteme sind getrennt

2. Vertraulichkeit und Integrität der Systeme

[Maßnahmen, die Vertraulichkeit und Integrität der Systeme des Auftragnehmers gewährleisten]

2.1 Zutrittskontrolle

[Maßnahmen, die unbefugte Dritte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, hindern]

- Abgeschlossene Büroeinheit, alleinige Nutzung
- Automatische Schließung der Zugangstüren, Öffnung von außen nur mit Schlüssel
- Restriktive Zutrittsregelung, kein Publikumsverkehr
- Alle Räume mit DV-Anlagen außerhalb der Arbeitszeiten separat mit Zylinderschlössern verschlossen
- Kameraüberwachung (PoE, kein WLAN) von Außenhaut, Eingangs- und Innenbereich bei Abwesenheit
- Bewegungserkennung
- Kameraaufzeichnung, verschlüsselt, lokal und auf externem System
- Direkt-Alarmierung der verantwortlichen Mitarbeiter über redundante Kommunikationswege (Push Alarm, E-Mail), auch bei Ausfall von Kameras (externe Verfügbarkeitsüberwachung)
- Workstations mit verschlossenen Metallgehäusen, Datenträger nicht von außen zugänglich
- Aktenschränke mit personenbezogenen Daten sind abschließbar und außerhalb der Arbeitszeiten verschlossen

2.2 Zugangskontrolle

[Maßnahmen, die die Nutzung der Systeme durch unbefugte Dritte verhindern]

- CAT.7 Festinstallation für alle Arbeitsplätze (kein WLAN), VLAN-Trennung
- Einsatz von Hardware-Firewalls
- Einsatz von Software-Firewalls
- Einsatz von Linux als Master-Betriebssystem für die produktiv eingesetzten Workstations
- Windows-Instanzen jeweils mit zusätzlicher Firewall und Virenschutz
- Regelmäßige Software-Updates
- Zugang zu den DV-Systemen des Auftragnehmers nur für autorisierte Mitarbeiter und ausschließlich durch eindeutige Benutzerkennungen und Passwörter
- Workstations werden bei Verlassen des Arbeitsplatzes gesperrt und bei Arbeitsende heruntergefahren
- Verschlüsselung mobiler IT-Systeme und Datenträger

2.3 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]

- Zuordnung von Benutzerprofilen zu IT-Systemen

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Bestehende Berechtigungen werden regelmäßig überprüft
- Mehrfache Passwort- und Sicherheitsschwellen
- Passwort- und Schlüssellängen-Richtlinien (Mindestlänge, Komplexität, etc.)
- Physische Trennung der vom Auftragnehmer verarbeiteten personenbezogenen Daten des Auftraggebers auf separaten Serversystemen (z.B. Kundenstammdatenverwaltung, Buchhaltung, etc.)
- Physische Trennung von Entwicklungs- und Produktivsystemen
- Clean Desk Prinzip

2.4 Eingabekontrolle

[Maßnahmen, mit denen nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind]

- Separate, dienstbezogene Protokollierung über Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle, eindeutige Benutzernamen (nicht Benutzergruppen)

2.5 Auftragskontrolle

[Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können]

- Siehe Maßnahmen unter Ziffer 2.2 (Zugangskontrolle) und 2.3 (Zugriffskontrolle)
- Schriftliche Verpflichtung der Mitarbeiter auf Wahrung der Vertraulichkeit (NDA)
- Schriftliche Verpflichtung der Mitarbeiter auf Anwendung grundlegender, anerkannter Sicherheitsstandards im Umgang mit IT-Systemen
- Schriftliche Verpflichtung der Mitarbeiter auf Einhaltung der geltenden Datenschutzbestimmungen im Umgang mit personenbezogen Daten
- Verbot privater Nutzung der Workstations sowie Nutzung privater Datenträger
- Auswahl der Unterauftragnehmer erfolgt unter Sorgfaltsgesichtspunkten, insbesondere hinsichtlich Datensicherheit
- Vorherige Prüfung der beim Unterauftragnehmer getroffenen Sicherheitsmaßnahmen
- Schriftliche Weisungen an den Unterauftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)

2.6 Transport- bzw. Weitergabekontrolle

[Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der Übertragung oder Weitergabe, physisch und/oder digital, nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können]

- Personenbezogene Daten des Auftraggebers werden durch den Auftragnehmer nur an berechtigte Empfänger (z.B. Banken im Rahmen des Zahlungsverkehrs oder die zur Registrierung eines Domainnamens oder eines SSL-Zertifikats mindestens erforderlich sind) elektronisch übertragen. Dazu werden ausschließlich sicher verschlüsselte Verbindungen eingesetzt
- Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des E-Mail-Verkehrs)
- Einsatz individueller VPN-Tunnelverbindungen zu den Data Center Standorten
- Zugang zum VPN ist nur von autorisierten Workstations bzw. Clients ausgehend und auch nur mit gültiger, nutzerbezogener Authentifizierung möglich, Zugriffe werden protokolliert und überwacht
- Aktenvernichter nach DIN 66399 mit Sicherheitsstufe 4
- Physische Datenträger werden bei Transport verschlüsselt
- Sichere Datenträgerlöschung (2x full random fill + 1x full zero fill)
- Sichere, physische Vernichtung alter oder fehlerhafter Datenträger

3. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

[Maßnahmen, die gewährleisten, dass die eingesetzten Systeme jederzeit einwandfrei funktionieren und dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind]

- Geschäftsrelevante DV-Systeme sind redundant vorhanden
- Blitz-/Überspannungsschutz
- Feuerlöscher

- Vorhaltung von Ersatz-Komponenten für sämtliche produktiv in den Data Centern eingesetzte Serversysteme (SSDs, HDDs, RAID-Controller, Mainboards, CPUs, RAMS, Netzteil-Einschübe, Switches, Kabel, etc.)
- Vorhaltung sofort einsatzfähiger Ersatz Rack-Server für den Einsatz im Data Center (ohne personenbezogene Daten)
- Alle geschäftsrelevanten Daten des Auftragnehmers werden im Rahmen eines strukturierten Backup-Plans in regelmäßigen Abständen gesichert. Dies gilt auch und besonders für personenbezogene Daten. Der ordnungsgemäße Durchlauf der Backup-Tasks wird regelmäßig kontrolliert

4. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragnehmer wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen regelmäßig prüfen, evaluieren und bei Bedarf anpassen.

TOMs für Standort: Data Center Colo #3, 66386 St. Ingbert, DE

An diesem Standort verarbeitet, speichert oder lagert der Auftragnehmer weder personenbezogene Daten des Auftraggebers noch Daten, die durch den Auftraggeber selbst verwaltetet werden. Die für diesen Standort getroffenen technischen und organisatorischen Maßnahmen sind daher für den vorliegenden AV-Vertrag irrelevant.

TOMs für Standort: Data Center Colo #4, NY 10011 New York, USA

An diesem Standort verarbeitet, speichert oder lagert der Auftragnehmer weder personenbezogene Daten des Auftraggebers noch Daten, die durch den Auftraggeber selbst verwaltetet werden. Die für diesen Standort getroffenen technischen und organisatorischen Maßnahmen sind daher für den vorliegenden AV-Vertrag irrelevant.

TOMs für Standort: Data Center Colo #5, CT 06651 Trumbull, USA

An diesem Standort verarbeitet, speichert oder lagert der Auftragnehmer weder personenbezogene Daten des Auftraggebers noch Daten, die durch den Auftraggeber selbst verwaltetet werden. Die für diesen Standort getroffenen technischen und organisatorischen Maßnahmen sind daher für den vorliegenden AV-Vertrag irrelevant.

Anlage 2 zum Vertrag zur Auftragsverarbeitung

Liste der bestehenden Unterauftragnehmer zum Zeitpunkt des Vertragsschlusses

Unternehmen:	**Dienstleistung:**
• CSL Computer Service Langenbach GmbH Hansaallee 191-193 40549 Düsseldorf DE	Domaindienstleistungen
• http.net Internet GmbH Franzstr. 51 52064 Aachen DE	Domaindienstleistungen
• 1blu business GmbH Stromstr. 1-5 10555 Berlin DE	Domaindienstleistungen
• Symantec Corporation 350 Ellis Street Mountain View, CA 94043 USA	SSL-Zertifikate
• IMPULS Steuerberatungs GmbH Waldfeuchter Str. 268 52525 Heinsberg DE	Lohnbuchhaltung, Buchführung, DATEV