Vertrag über die Auftragsdatenverarbeitung gemäß Art. 28 DSGVO

Zwischen
der

1blu AG
Stromstraße 1-5
10555 Berlin

nachstehend auch „Auftragnehmer" genannt

und

dem Kunden

Kundennummer:	
Firma /Organisation:	Diplom Psychologin und Psychologische Psychotherapeutin
Name:	Sigrun Voß
Straße, Hausnummer:	Schillerstraße 2/1
PLZ, Ort:	89077 Ulm

nachstehend auch „Auftraggeber" genannt

Präambel

Dieser Vertrag über die Auftragsdatenverarbeitung ergänzt und konkretisiert die datenschutzrechtlichen Verpflichtungen, die aus dem zwischen den Vertragsparteien geschlossenen Einzelvertrag resultieren. Das Bestehen eines solchen Individualvertrags ist zwingende Voraussetzung für das rechtlich bindende Zustandekommen dieses Vertrags.

§ 1 Gegenstand und Dauer der Auftragsdatenverarbeitung

Der Auftrag umfasst Folgendes:

Dienstleistungen für Webhosting, Domainregistrierung und -verwaltung, Rechenzentrumsarbeiten sowie alle damit im Zusammenhang stehenden Handlungen, wie zum Beispiel die Weitergabe der zur Domainregistrierung oder Zertifikatserstellung erforderlichen Daten an die jeweilige Registrierungsstelle oder den entsprechenden Dienstleister, die Administration der Server inklusive des Erstellens von Backupdateien. Die Dauer der Auftragsdatenverarbeitung richtet sich nach der Laufzeit des Individualvertrags.

§ 2 Anwendungsbereich

(1) Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.

(2) Die vertraglich vereinbarte Dienstleistung wird mit Ausnahme der Übertragung der zur Domainregistrierung erforderlichen Daten ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Die Übertragung von Daten an Organisationen, die Daten an internationale Organisationen in Drittländern übermitteln, findet nur und ausschließlich bei der entsprechenden ausdrücklichen Bestellung einer Domain der entsprechenden Organisation statt.

(3) Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 3 Dauer des Auftrags

(1) Der Vertrag beginnt mit Datum des Zugangs des durch den Auftraggeber unterzeichneten Vertrags beim Auftragnehmer und endet 14 Tage nach der wirksamen Beendigung des zugehörigen Individualvertrags.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers

gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 4 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

(1) Die Art und der Zweck der Verarbeitung richten sich jeweils nach der Leistungsbeschreibung des Individualvertrags.

(2) Der Auftraggeber verarbeitet die Daten des Auftragnehmers für den Auftragnehmer laut der Leistungsbeschreibung des Individualvertrags.

§ 5 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

(3) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

(4) Der Auftraggeber ist berechtigt, sich wie unter Ziffer 6 Nr. 9 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Die Durchführung einer solchen Kontrolle vor Ort kann durch den Auftragnehmer von einer

vorab zu zahlenden Aufwandsentschädigung die sich nach dem tatsächlichen Aufwand und dem Umfang der beabsichtigten Kontrolle richtet abhängig gemacht werden. Die Kontrolle ist regelmäßig auf eine Maßnahme pro Jahr begrenzt.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(6) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen. Als Ansprechpartner steht dem Auftraggeber der in Ziffer 6 Absatz 13 benannte Datenschutzbeauftragte zur Verfügung.

§ 6 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen zur Durchführung des Vertrags und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

(2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(4) Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber regelmäßige Kontrollen über die Einhaltung dieser Vereinbarung in seinem Bereich durchzuführen. Das Ergebnis der Kontrollen ist zu dokumentieren.

(5) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten, sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an den Auftraggeber weiterzuleiten.

(6) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

(7) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers oder gesetzliche Vorschriften dem nicht entgegenstehen.

(8) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

(9) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h

DSGVO). Die Durchführung einer solchen Kontrolle vor Ort kann durch den Auftragnehmer von einer vorab zu zahlenden Aufwandsentschädigung, die sich nach dem tatsächlichen Aufwand und dem Umfang der beabsichtigten Kontrolle richtet abhängig gemacht werden. Die Kontrolle ist regelmäßig auf eine Maßnahme pro Jahr begrenzt.

(10) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.

(11) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

(12) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

(13) Beim Auftragnehmer ist als Beauftragter für den Datenschutz

Herr Michael Reim, datenschutzbeauftragter@1blu.de

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

§ 7 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen

Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 5 dieses Vertrages durchführen.

§ 8 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

(1) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet (Art. 28 Abs. 2 DSGVO), welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

(2) Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(3) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt

dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

(4) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

(5) Zurzeit sind für den Auftragnehmer die in **Anlage 1** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Als weitere genehmigte Subunternehmer nach diesem Vertrag gelten alle verbundenen Unternehmen des Auftragnehmers im Sinne des AktG. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Sie sind in der im Anhang beigefügten Liste aufgeführt.

(6) Der Auftragnehmer informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

§ 9 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

(1) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

(2) Die angewandten Methoden zur Risikoberwertung und Überwachung

werden permanent aktualisiert und auf den aktuellen Stand der Technik überprüft.

(3) Die in **Anlage 2** beschriebenen TOM stellen die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT- Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

(4) Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO).

(5) Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

(6) Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

§ 10 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten zu löschen, beziehungsweise deren Löschung zu veranlassen und dies zu kontrollieren.

§ 11 Haftung

Hinsichtlich der Haftung wird auf Art. 82 DSGVO wird verwiesen.

§ 12 Sonstiges

(1) Alle Änderungen, Nebenabreden, die Kündigung und Aufhebung dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für die Aufhebung dieser Klausel. Nebenabreden wurden nicht getroffen. Streichungen in dieser Vereinbarung müssen von beiden Parteien gezeichnet werden.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise

unwirksam oder lückenhaft sein, so berührt dies die Gültigkeit der übrigen Bestimmungen nicht. Vielmehr tritt für den Fall, dass ein Verbraucher an dem Vertrag nicht beteiligt ist an die Stelle der unwirksamen Bestimmung eine Regelung, die dem gewollten Zweck am nächsten kommt. Im Fall einer Lücke gilt dann diejenige Bestimmung als vereinbart, die dem entspricht, was nach dem Zweck vereinbart worden wäre, hätten die Parteien die Angelegenheit von vornherein bedacht. Ist hiernach eine Lösung nicht möglich, finden die Parteien eine Regelung im Geist partnerschaftlicher Kooperation.

(3) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(4) Es gilt deutsches Recht.

Datum:

1blu AG
Stromstraße 1-5
10555 Berlin
Fon: 030 - 20 18 10 00
Fax: 030 - 20 18 10 01
www.1blu.de

_____	_____
Auftraggeber	Auftragnehmer
	Ulf Jeziorek
_____	Prokurist
Name in Druckbuchstaben	
_____	
Ggfs. Funktion	

Anlage 1 zum ADV

Genehmigte Subunternehmer(weitere Auftragsverarbeiter) der 1blu AG

Name	Adresse	Leistungsbeschreibung
1blu business GmbH	Stromstraße 1-5 10555 Berlin Deutschland	Server- und Netzwerkverwaltung, Kundensupport, IT Beratung, Domainregistrierung
Greatnet.de GmbH	Stromstraße 1-5 10555 Berlin Deutschland	Server- und Netzwerkverwaltung, Kundensupport, IT Beratung,
OMCnet Internet Service GmbH	Ernst-Abbe-Straße 10 25451 Quickborn Deutschland	Server- und Netzwerkverwaltung, Kundensupport, IT Beratung, Domainregistrierung

Anlage 2 zum ADV

Technische und organisatorische Maßnahmen der 1blu AG

1. Pseudonymisierung, Datenminimierung

(Art. 32 Abs. 1 lit. a DSGVO, Art. 25 Abs. 1 DSGVO)

Maßnahmen zur Verarbeitung personenbezogener Daten in einer Weise, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und den entsprechenden technischen und organisatischen Maßnahmen unterliegen:

- IP-Adressen werden in Logdateien nur vollständig erfasst, sofern dies zum ordnungsgemäßen Betrieb der Server erforderlich ist (d.h. zur Abwehr von Angriffen, zur Feststellung missbräuchlicher Verwendung von Diensten oder der Herausgabe bei Anfragen durch Strafverfolgungsbehörden, usw.).
- Logdateien, welche unverfremdete IP-Adressen enthalten, werden auf unseren Systemen automatisch rotiert.
- Über längere Zeit gespeicherte IP-Adressen (z.B. als Grundlage zur Erstellung von Statistiken für unsere Kunden) sind durch Unkenntlichmachung eines Oktetts (IPv4) bzw. eines Hextetts (IPv6) nicht mehr eindeutig einer bestimmten Person zuzuordnen.
- Es werden nur solche persönlichen Daten unserer Kunden erhoben, die für die Erbringung unserer Dienstleistung notwendig sind. Mitarbeiter sind zur Datensparsamkeit gehalten.

2. Vertraulichkeit

(Art. 32. Abs. 1 lit. b DSGVO)

2.1 Maßnahmen, die Unbefugten den physischen Zugriff auf Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren (Zutrittskontrolle):

- Das Rechenzentrum verfügt über einbruchshemmende Türen und Lüftungsklappen.
- Es besteht eine Schlüsselregelung samt dokumentierter Schlüsselvergabe.

- Das Rechenzentrum ist durch ein personalisiertes biometrisches Zutrittskontrollsystem abgesichert.
- Eine Richtlinie regelt den Zutritt und die Überwachung von Besuchern. Der Zutritt zu den Serverräumen ist gesondert geregelt.
- Besucher im Rechenzentrum werden protokolliert.
- Videoüberwachung ist im Rechenzentrum installiert.
- Es besteht eine Alarmanlage, deren Auslösung eine automatische Benachrichtigung des Bereitschaftsdienstes nach sich zieht.
- Das Rechenzentrum weist keine Fenster auf.

2.2 Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle):

- Alle DV-Systeme, die Zugang zu personenbezogenen Daten gewähren, erfordern mindestens eine Authentifikation mittels Benutzername und Kennwort.
- Benutzerzugänge sind personalisiert.
- Die Vergabe von Zugangsberechtigungen erfolgt rollenbasiert und wird dokumentiert.
- Es erfolgt ein Entzug von Berechtigungen, sofern diese nicht mehr benötigt werden. Dieser Vorgang wird dokumentiert.
- Die Authentifikation der Benutzer erfolgt durch Verwendung digitaler Zertifikate.
- Administrative Zugänge dürfen sich nur von bestimmten, festgelegten IPs aus anmelden.
- Bei wiederholten Authentifizierungsfehlern erfolgt eine automatische Sperrung von Zugängen.
- Es existiert eine Richtlinie zur datenschutzkonformen Konfiguration der Arbeitsplatzrechner.
- Vorgeschrieben ist für alle Arbeitsplatzrechner das Einrichten einer automatischen Bildschirmsperre mit Kennwortschutz bei Untätigkeit.
- Es erfolgt eine zentrale Speicherung von Protokolldateien auf einem dezidierten Logserver.

2.3 Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, sowie dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen,

kopiert, verändert oder entfernt werden können (Zugriffskontrolle):

- Es gelten rollenbasierte Zugriffsregelungen.
- Administrative Tätigkeiten werden protokolliert.
- Privilegierte Aktionen werden zusätzlich auf einem dedizierten Logserver protokolliert.
- Protokollierung von Kenntnisnahme, Veränderung und Löschung von personenbezogenen Daten auf den Kundenservern.

2.4 Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden (Trennungskontrolle):

- Auftragsdaten werden getrennt (auf anderen Maschinen) von den Daten aus laufenden Systemanwendungen der Kunden gespeichert.
- Personenbezogene Daten werden ausschließlich zweckgebunden verarbeitet.

3. Integrität

(Art. 32. Abs. 1 lit. b DSGVO)

3.1 Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektrischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Weitergabekontrolle):

- Entfernter Zugriff ist nur unter Verwendung verschlüsselter Verbindungen möglich (z.B. VPN / SSH).
- Wo dies möglich ist, wird Datenverschlüsselung eingesetzt (z.B. PGP für Email).
- Personenbezogene Daten werden standardmäßig nicht an Dritte übermittelt.
- Es besteht ein dokumentierter Prozess zur Vernichtung von Daten und Datenträgern.
- Die physische Vernichtung der Datenträger erfolgt durch einen zertifizierten Dienstleister.

- Transport der Datenträger zur Vernichtung erfolgt in eigens dafür vorgesehenen abschließbaren Behältern.

3.2 Maßnahmen, die eine nachträgliche Überprüfung ermöglichen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle):

- Eine Protokollierung aller Vorgänge im Bereich der eingesetzten Verwaltungssoftware wird durchgeführt.
- Für essentielle Systeme kommen Versionsverwaltungssysteme zum Einsatz.

4. Verfügbarkeit und Belastbarkeit

(Art. 32 Abs. 1 lit. b und c DSGVO)

Maßnahmen, welche gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und verfügbar bleiben (Verfügbarkeitskontrolle):

- Um die Daten nach einem Ausfall wiederherstellen zu können, existiert ein vollständiges Backup- & Recovery-Konzept.
- Es wird eine tägliche Datensicherung automatisch durchgeführt.
- Um größtmögliche Verfügbarkeit der Daten zu erzielen, werden in den Servern RAID-Systeme eingesetzt.
- Auf Wunsch werden Hochverfügbarkeitslösungen umgesetzt.
- Im Rechenzentrum wird Gebrauch von unterbrechungsfreier Stromversorgung gemacht.
- Das Rechenzentrum verfügt über einen automatisch anlaufenden Dieselgenerator, um Stromausfälle überbrücken zu können, welche über die Batteriekapazität der eingesetzten USV-Anlagen gehen.
- Der Dieselgenerator wird regelmäßig mittels durchgeführter Testläufe auf Betriebsbereitschaft hin überprüft.
- Es besteht eine mehrfach-redundante Anbindung an Backboneprovider.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

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

Maßnahmen zur Sicherstellung eines technisch und organisatorisch angemessenen Standes bei der Erbringung der vertraglich vereinbarten Leistungen:

- Die TOM werden nach einem definierten Prozess regelmäßig auf Wirksamkeit und Einhaltung eines angemessenen technischen Standes überprüft.
- Der sichere Betrieb des Rechenzentrums und die sachgemäße Dokumentation der diesbezüglichen Prozesse werden mittels eines durch einen anerkannten externen Dienstleister ausgestellten Zertifikates nachgewiesen.

6. Datenschutzbeauftragter und Auftragsdatenverarbeitung

(Art. 32. Abs. 4 DSGVO; Art. 29 DSGVO; Art. 37 Abs. 4 DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle):

- Die 1blu AG hat einen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten Prozesse.
- Verpflichtung der Beschäftigten auf das Datengeheimnis (vormals § 5 BDSG).
- Abschluss von Verträgen zur Verarbeitung von personenbezogenen Daten im Auftrag unter Berücksichtigung der jeweiligen Anforderungen, wenn diese vom Auftraggeber mitgeteilt werden.
- Serverstandorte sind – sofern nicht anderweitig vereinbart – Rechenzentren in Deutschland.