Vertrag über die Auftragsverarbeitung gemäß Art. 28 DSGVO

Zwischen
der

1blu AG
Riedemannweg 60
13627 Berlin

nachstehend auch "Auftragnehmer" genannt

und

dem Kunden

Kundennummer:	2739130
Firma /Organisation:	Wolfgang Flemming
Name:	Wolfgang Flemming
Straße, Hausnummer:	Römerstr. 175
PLZ, Ort:	Leonberg

Präambel

Dieser Vertrag über die Auftragsverarbeitung definiert die datenschutzrechtlichen Verpflichtungen, die aus den zwischen den Vertragsparteien geschlossenen Individualverträgen resultieren und gilt für alle zwischen den Parteien über die in Anlage 1 genannten Dienstleistungen bestehenden oder künftig geschlossenen Individualverträge.

§ 1 Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

§ 2 Anwendungsbereich

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

(2) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht.

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

§ 3 Dauer des Auftrags

(1) Der Vertrag über die Auftragsverarbeitung beginnt mit Abschluss dieses Vertrages und dauert an, solange der Auftragnehmer für den Auftraggeber Daten verarbeitet.

(2) Die Dauer der Verarbeitung entspricht der Laufzeit des jeweiligen Individualvertrages.

§ 4 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. Der Auftragnehmer wird den Auftraggeber nach Maßgabe des § 6 Nr. 5 dieses Vertrags unterstützen.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen. Weisungen des Auftraggebers, die über die vertraglichen Vereinbarungen hinausgehen und auch nicht erforderlich sind, um Rechtsverstöße im Zuständigkeitsbereich des Auftragnehmers zu verhindern bzw. abzustellen, sind kostenpflichtig und vom Auftraggeber zu vergüten, wobei beim Auftragnehmer entstehende Arbeitskosten mit 165,- EUR zzgl. USt. pro Stunde berechnet werden und entstehende Kosten durch die Beauftragung Dritter dem Auftraggeber weiterberechnet werden.

(3) Die Dokumentation der vom Auftraggeber erteilten Weisungen erfolgt durch den Auftragnehmer.

(4) Der Auftraggeber ist berechtigt, sich wie unter § 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.

(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. Die Verpflichtung dazu bleibt auch nach Beendigung dieses Vertrages bestehen. Eine Pflicht zur Vertraulichkeit besteht nicht, wenn und soweit der Auftraggeber aufgrund eines Gesetzes oder der Entscheidung eines Gerichts oder einer Verwaltungsbehörde dazu verpflichtet ist, Geschäftsgeheimnisse oder Datensicherheitsmaßnahmen des Auftragnehmers mitzuteilen und/oder darüber zu informieren. Als Ansprechpartner steht dem Auftraggeber der in § 5 Nr. 13 benannte Datenschutzbeauftragte zur Verfügung.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich nach dokumentierten Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der

Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, 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). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(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 (zur Vermeidung von Missverständnissen: Dies schließt Subunternehmer des Auftragnehmers ein) durchzuführen. Das Ergebnis der Kontrollen ist zu dokumentieren.

(5) Der Auftragnehmer wird den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen (DSGVO) und wird unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO).

(6) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten 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.

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

(9) Der Auftragnehmer verpflichtet sich, dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 DSGVO niedergelegten Pflichten zur Verfügung zu stellen und ermöglicht und trägt aktiv dazu bei, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung, sofern nicht eine Kontrolle ohne vorherige Anmeldung erforderlich erscheint, weil andernfalls der Kontrollzweck gefährdet wäre - die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst bzw. durch einen sachkundigen Dritten, sofern dieser nicht in einem unmittelbaren Wettbewerbsverhältnis zum Auftragnehmer steht, kontrolliert, 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). Mit Ausnahme von solchen Fällen, in denen diese Kontrollen wegen eines Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer erforderlich wurde, ist der Auftragnehmer berechtigt, vom Auftraggeber Ersatz der ihm durch solche Kontrollen entstandenen, angemessenen Kosten zu verlangen.

(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) Der Datenschutzbeauftragte des Auftragnehmers ist unter der Adresse 1blu AG Datenschutzbeauftragter Riedemannweg 60 13627 Berlin erreichbar.

§ 6 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 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. Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gern. § 5 dieses Vertrages durchführen.

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

(1) Der Auftragnehmer besitzt die allgemeine Genehmigung des Auftraggebers für die Beauftragung von Unterauftragsverarbeitern nach Maßgabe dieses § 8. Der Auftragnehmer muss dafür Sorge tragen, dass er die 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 nach vorheriger Weisung und dann

erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(3) Der Auftragnehmer hat dem Subunternehmer vertraglich sinngemäß dieselben Datenschutzpflichten aufzuerlegen, die in diesem Vertrag für den Auftragnehmer festgelegt sind. Der Auftragnehmer stellt sicher, dass der Subunternehmer die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesem Vertrag und gemäß der Verordnung (EU) 2016/679 unterliegt. 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. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. 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 seinen Datenschutzpflichten nachkommt.

(5) Zurzeit sind für den Auftragnehmer die in **Anlage 2** mit Namen, Rechtsform, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und werden vom Auftraggeber genehmigt.

(6) Der Auftragnehmer informiert den Verantwortlichen in einer angemessenen Zeit, die jedoch 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer unter Angabe von Namen, Rechtsform und Anschrift sowie der vorgesehenen Tätigkeit des neuen oder ersetzenden Subunternehmers sowie gegebenenfalls unter Abgrenzung der Aufgaben mehrerer Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO), wobei ein Einspruch gegen einen Subunternehmer nur aus einem sachlichem Grund zulässig ist. Eine solche Information kann insbesondere durch Übermittlung angepassten Liste gemäß Anlage 2 und des Datums der beabsichtigten Änderung oder Hinzuziehung erfolgen. Im Falle eines Einspruches gegen einen Subunternehmer, unterbleibt eine Verarbeitung durch diesen für den Auftraggeber, in diesem Fall ist der Auftragnehmer berechtigt, den Individualvertrag bzw. die Individualverträge, der bzw. die von der beabsichtigten Änderung betroffen ist bzw. sind, innerhalb eines Zeitraumes von drei Monaten nach Zugang des Einspruchs mit einer Frist von einem Monat zu kündigen.

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

(1) Der Auftragnehmer ergreift alle gemäß Artikel 32 erforderlichen Maßnahmen.

(2) Der Auftragsnehmer ergreift darüber hinaus mindestens die in Anlage 3 aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten.

(3) Die angewandten Methoden zur Risikobewertung und Überwachung werden permanent aktualisiert und auf den aktuellen Stand der Technik überprüft.

(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).

§ 9 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags (Art. 28 Abs. 3 Satz 2 lit. g DSGVO)

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben und die vorhandenen Kopien zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

§ 10 Haftung

Hinsichtlich der Haftung wird auf Art. 82 DSGVO verwiesen.

§ 11 Sonstiges

(1) Klarstellend wird festgehalten, dass dieser Vertrag über die Auftragsverarbeitung dann auch Anwendung findet, wenn ein zwischen den Parteien geschlossener Individualvertrag sich als unwirksam oder nichtig herausstellt oder wenn der Auftragnehmer im Rahmen eines nur vermeintlich geschlossenen Individualvertrages für den Auftraggeber personenbezogene Daten verarbeitet.

(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) Es gilt deutsches Recht.

Anlage 1 zum AVV

Gegenstand des Auftrags

1. Gegenstand, Art und Zweck der Verarbeitung
Gegenstand der Verarbeitung sind je nach den geschlossenen Individualverträgen zu erbringende Dienstleistungen und die damit im Zusammenhang stehende Verarbeitung der Daten auf den Systemen des Auftragnehmers. Zweck der Verarbeitung ist beim Webhosting und bei der Nutzung von Servern des Auftragnehmers der Betrieb einer Webseite oder sonstiger, über das Internet erreichbarer Anwendungen sowie die Nutzung von E-Mail-Kommunikation, beim Online-Speicher die bloße Speicherung von Daten. Die Arten der Verarbeitung sind die damit im Zusammenhang stehenden Vorgänge oder Vorgangsreihen, d.h. das Erheben, Ordnen, Speichern, Übermitteln, Löschen, Anonymisieren, oder Pseudonymisieren.

2. Art(en) der personenbezogenen Daten
Die Art(en) der personenbezogenen Daten sind alle sind die Nutzungs- und Contentdaten, die im Rahmen der jeweiligen Dienstleistungen der einzelnen Individualverträge vom Auftraggeber in den für ihn beim Auftraggeber gehosteten Websites, Servern, Datenbanken und E-Mail-Postfächern gespeichert oder verarbeitet werden, die vom Auftraggeber selbst, oder von Nutzern der Websites des Auftraggebers auf dessen Websites eingegeben werden, die per E-Mail an ihn gesendet oder vom Auftraggeber per E-Mail versendet werden. Es handelt sich dabei um folgende Daten:

- Daten, die technisch erforderlich sind, um eine Webseite anzuzeigen
- Vertragsdaten von Lieferanten und Kunden des Auftraggebers
- Kontaktdaten von Mitarbeitern, Lieferanten, Kunden und Interessenten des Auftraggebers
- Abrechnungsdaten von Kunden des Auftraggebers
- Bank- und Kontodaten von Kunden des Auftraggebers
- Inhaltsdaten, insbesondere aus E-Mailkommunikation

3. Kategorien betroffener Personen
Es werden die personenbezogenen Daten von Personen verarbeitet, deren Daten im Rahmen der gehosteten Services verarbeitet werden. Es handelt sich dabei um folgende Daten:

- Kunden
- Nutzer
- Lieferanten und Dienstleister
- Beschäftigte
- Interessenten

Anlage 2 zum AVV

Genehmigte Subunternehmer (weitere Auftragsverarbeiter) der 1blu AG

Name	Adresse	Leistungsbeschreibung
1blu business GmbH	Riedemannweg 60 13627 Berlin Deutschland	Server- und Netzwerkverwaltung, Kundensupport, IT-Beratung, Domainregistrierung
Greatnet.de GmbH	Riedemannweg 60 13627 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 3 zum AVV

Technische und organisatorische Maßnahmen der 1blu AG

1. Pseudonymisierunq. Datenminimierung (Art. 32 Abs. 11it. 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 organisatorischen Maßnahmen unterliegen:

(1) IP-Adressen werden in Logdateien nur vollständig erfasst, sofern dies zum ordnungsgemäßen Betrieb der Server erforderlich ist (d.h. zur Abwehr von Angriffen, zur Feststel-lung missbräuchlicher Verwendung von Diensten oder der Herausgabe bei Anfragen durch Strafverfolgungsbehörden, usw.).

(2) Logdateien, welche unverfremdete IP-Adressen enthalten, werden auf unseren Systemen automatisch rotiert.

(3) 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.

(4) 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. Mit. b 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 organisatorischen Maßnahmen unterliegen:

(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) 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.

(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.

(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. lit. b DSGVO)

(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.

(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):

(1) Um die Daten nach einem Ausfall wiederherstellen zu können, existiert ein vollständiges Backup- & Recovery-Konzept.

(2) Es wird eine tägliche Datensicherung automatisch durchgeführt.

(3) Um größtmögliche Verfügbarkeit der Daten zu erzielen, werden in den Servern RAID-Systeme eingesetzt.

(4) Auf Wunsch werden Hochverfügbarkeitslösungen umgesetzt.

(5) Im Rechenzentrum wird Gebrauch von unterbrechungsfreier Stromversorgung gemacht.

(6) Das Rechenzentrum verfügt über einen automatisch anlaufenden Dieselgenerator, um Stromausfälle überbrücken zu können, welche über die Batteriekapazität der eingesetzten USV-Anlagen gehen.

(7) Der Dieselgenerator wird regelmäßig mittels durchgeführter Testläufe auf Betriebsbereitschaft hin überprüft.

(8) Es besteht eine mehrfach-redundante Anbindung an Backbone Provider.

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:

(1) Die TOM werden nach einem definierten Prozess regelmäßig auf Wirksamkeit und Einhaltung eines angemessenen technischen Standes überprüft.

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

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

(1) Die lblu AG hat einen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten Prozesse.

(2) Verpflichtung der Beschäftigten auf das Datengeheimnis (vormals § 5 BDSG).

(3) Abschluss von Verträgen zur Verarbeitung von personenbezogenen Daten im Auftrag unter Berücksichtigung der jeweiligen Anforderungen, wenn diese vom Auftraggeber mitgeteilt werden.

(4) Serverstandorte sind - sofern nicht anderweitig vereinbart - Rechenzentren in Deutschland.