Vertrag über die Auftragsverarbeitung personenbezogener Daten

Vertragspartner

Auftraggeber	Auftragnehmer
	IPBee GmbH Froschkönigweg 6 21244 Buchholz Deutschland

1. Gegenstand der Beauftragung

a) Der Auftraggeber lässt durch Unterauftragnehmer des Auftragnehmers auf Grundlage dieses Vertrages personenbezogene Daten im Auftrag verarbeiten. Mit dem vorliegenden Vertrag über die Auftragsverarbeitung konkretisieren die Parteien die grundlegenden Vereinbarungen, die der entsprechenden Tätigkeit des Auftragnehmers zu Grunde liegen. Die Dauer der Verarbeitung der personenbezogenen Daten ist an die Vertragsdauer dieses Vertrages (siehe auch Punkt 15) zwischen Auftraggeber und Auftragnehmer gebunden.

b) Der Zweck der Verarbeitung der personenbezogenen Daten umfasst die Herstellung „fälschungssicherer digitaler Zeugnisse". Die Herstellung „fälschungssicherer digitaler Zeugnisse" beruht auf einer Technologie, welche die Überprüfbarkeit der Originalität von digitalen Dateien ermöglicht. Hierzu werden auf Basis der Originaldokumente berechnete Fingerabdrücke (HASH-Werte) in öffentlichen (public) Blockchains abgelegt. Zur Übertragung und Speicherung der Daten werden unterschiedliche Prozesse angestoßen und Daten auf verschiedenen Servern verarbeitet. Personenbezogene Daten werden bisher und bis auf Weiteres ausschließlich auf Servern der Unterauftragnehmer abgelegt, nicht auf den Servern des Auftragnehmers und nicht auf den Blockchains.

c) Ausschließlich zur Erfüllung dieses Zwecks und im Zusammenhang der insoweit vom Auftragnehmer zu erbringenden Leistungen werden personenbezogene Daten aus dem Herrschaftsbereich des Auftraggebers durch Unterauftragnehmer i. S. d. Art. 4 Nr. 2 DSGVO verarbeitet; insbesondere erhoben, gespeichert, verändert, ausgelesen, abgefragt, verwendet, abgeglichen, verknüpft und gelöscht.

2. Von der Verarbeitung betroffene Arten personenbezogener Daten

a. Von der Auftragsverarbeitung können folgende Arten personenbezogener Daten betroffen sein:

- Angaben zu Zeugnisinhabern und Daten auf dem Zeugnis: Stammdaten wie Name und Anschrift, Geburtsdatum, Geburtsort, E-Mail-Adresse, Abschlussart, Kurse/Fächer, Noten, Bemerkungen, Besondere Lernleistungen, Fehlstunden, Name der Schule, Schulnummer, Schüler-ID, Namen von Lehrpersonal oder Schulleitung.

- Angaben zu Ansprechpartnern zum Zwecke der Bearbeitung des Prozesses/Workflows bzw. Mitbenutzern (User) der Institution des Auftraggebers: Anrede, Name, Vorname, E-Mail-Adresse, Telefonnummer, durchgeführte Aktionen innerhalb von Prozessen zum Zwecke des Logins und der Verwaltung von Zeugnissen und deren Inhabern.

b. Im Prozess können Zeugnisse als PDF-Datei hochgeladen und den Zeugnisinhabern zugeordnet werden. Die Verantwortung für die Korrektheit dieser Inhalte trägt allein der Auftraggeber. Insbesondere sind keine Dateien hochzuladen, die gegen die Lizenzvereinbarungen oder geltendes Recht verstoßen.

c. Ob die vom Auftragnehmer zu erbringenden Leistungen und die insoweit getroffenen Vereinbarungen geeignet sind für die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO, bedarf einer Risikobewertung durch den Auftraggeber.

3. Kategorien der von der Verarbeitung betroffener Personen

Von der Auftragsverarbeitung sind folgende Kategorien von personenbezogenen Daten betroffen:

a) Schülerdaten des Auftraggebers (Zeugnisinhaber)
b) Mitarbeiterdaten des Auftraggebers (User)

4. Technische und organisatorische Maßnahmen

Der Auftragnehmer ergreift für die im Auftrag verarbeiteten personenbezogenen Daten die in der Anlage 1 aufgeführten technischen und organisatorischen Maßnahmen.

5. Weisungsberechtigte Personen

a) Die folgenden Personen sind für den Auftraggeber weisungsberechtigt; er kann die Liste der weisungsberechtigten Personen jederzeit durch einseitige Erklärung modifizieren. Weisungsberechtigte Personen sind:

1. _____

2. _____

3. _____

b) Der Auftragnehmer erklärt, dass die folgenden Personen für ihn entsprechend empfangsbevollmächtigt sind:Jan F. Timme, Dr. Mirjam Brautmeier

6. Unterauftragnehmer

a. Der Auftragnehmer setzt für das Hosting folgenden Unterauftragnehmer ein:

Wieske's Crew GmbH, Süderstraße 195, 20537 Hamburg, eingesetzt durch Unterauftragnehmer, aktuell ALLISA GmbH
STRATO AG, Otto-Ostrowski-Straße 7,10249 Berlin

b) Der Auftraggeber gestattet weiter die Beauftragung solcher Unterauftragnehmer, die verbundene Unternehmen des Auftragnehmers gem. § 15 AktG sind. Der Auftragnehmer hat den Auftraggeber laufend informiert zu halten, welches Unternehmen insoweit mit der Erbringung welcher Leistungen beauftragt ist und ggf. die Voraussetzungen des § 15 AktG nachzuweisen. Der Auftragnehmer verpflichtet sich, seine Weisungsbefugnisse gegenüber diesen Unternehmen im Einklang mit diesem Vertrag und den Weisungen des Auftraggebers auszuüben.

c) Der Auftragnehmer wird den eventuellen Unterauftragnehmern im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegen, die in diesem Vertrag zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind.

d) Nicht als Unterauftragsverhältnisse im Sinne der vorstehenden Regelungen sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen sowie Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um denSchutz personenbezogener Daten zu gewährleisten.

7. Ort der Auftragsverarbeitung

Die Auftragsverarbeitung findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Eine Offenlegung an Drittländer erfolgt nicht.

8. Verantwortlichkeit des Auftraggebers

a) Der Auftraggeber ist Verantwortlicher für die Auftragsverarbeitung der personenbezogenen Daten im Sinne des Art. 4 Nr.7 DSGVO. Er ist für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

b) Dem Auftraggeber obliegt die Entscheidung über die Zulässigkeit der Datenverarbeitung in jedem Einzelfall. Der Auftragnehmer ist berechtigt und verpflichtet, auf etwaige Bedenken hinsichtlich der rechtlichen Zulässigkeit der Datenverarbeitung hinzuweisen.

9. Weisungsrecht des Auftraggebers

a) Der Auftraggeber hat jederzeit das Recht, ergänzende Weisungen über Art, Umfang und Verfahren der Verarbeitung der personenbezogenen Daten zu erteilen. Weisungen können mündlich oder in Textform erfolgen. Mündliche Weisungen sind unverzüglich in Textform gegenüber dem Auftragnehmer zu bestätigen.

b) Der Auftragnehmer wird den Auftraggeber unverzüglich in Textform informieren, wenn nach seiner Auffassung eine vom Auftraggeber erteilte Weisung gegen gesetzliche Regelungen verstößt. Der

Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

10. Kontrollrechte des Auftraggebers, Maßnahmen von Aufsichtsbehörden

a) Dem Auftraggeber stehen alle Kontrollrechte zu, welche zur Wahrung seiner datenschutzrechtlichen Obliegenheiten erforderlich sind.

b) Auf Verlangen des Auftraggebers ist diesem zu üblichen Geschäftszeiten Zugang und Einsicht zu den Datenverarbeitungssystemen des Auftragnehmers und der Unterauftragnehmer zu gewähren, die er für die Zwecke dieses Vertrages einsetzt. Solche Vorort-Kontrollen sind auf eine Prüfung je Kalenderjahr beschränkt, sofern nicht ein wichtiger Grund vorliegt, der Auftraggeber Anhaltspunkte für einen Verstoß gegen die Vorgaben dieses Vertrages hat, es zur Wahrung gesetzlicher Verpflichtungen des Auftraggebers erforderlich ist oder eine Kontrolle durch die Aufsichtsbehörde erfolgt.

c) Eine Vorort-Kontrolle bedarf der vorherigen Ankündigung mit angemessener Frist, sofern kein wichtiger Grund vorliegt. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen die Beauftragung dieses Prüfers ein Einspruchsrecht.

d) Der Auftragnehmer darf die Vorort-Kontrolle von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der personenbezogenen Daten und Geschäftsgeheimnisse anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Dies gilt nicht bei einer Tätigkeit der Aufsichtsbehörde.

e) Für die Unterstützung bei der Durchführung einer Vorort-Kontrolle darf der Auftragnehmer eine angemessene Vergütung verlangen, wenn nicht er den Anlass für die Kontrolle zu vertreten hat.

11. Pflichten des Auftragnehmers

a) Jegliche Verarbeitung der personenbezogenen Daten durch den Auftragnehmer oder durch etwaige Unterauftragnehmer, die diesem Vertrag unterfällt, erfolgt ausschließlich auf Grundlage dieses Vertrages sowie den vom Auftraggeber erteilten Weisungen. Dies gilt nicht, wenn der Auftragnehmer zu einer anderen Verarbeitung durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

b) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation im Rahmen der Verarbeitung der personenbezogenen Daten so gestalten, dass sie den gesetzlichen Anforderungen sowie den in diesem Vertrag vereinbarten Anforderungen gerecht wird. Der Auftragnehmer hat insbesondere die technischen und organisatorischen Maßnahmen zu treffen, die

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der personenbezogenen Daten auf Dauer sicherstellen und
- die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem

physischen oder technischen Zwischenfall sicherstellen.

c) Eine Änderung der in der Anlage 1 vereinbarten technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das jeweils vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer hat den Auftraggeber über wesentliche Änderungen unaufgefordert zu informieren.

d) Der Auftragnehmer berichtigt oder löscht personenbezogene Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück.

e) Daten, Datenträger sowie sämtliche sonstige Materialien inkl. Sicherungskopien mit personenbezogenen Daten, die diesem Vertrag unterfallen, sind nach Auftragsende je nach Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Sofern der Auftraggeber eine Weisung zur Löschung erteilt, die vom bisher Vereinbarten abweicht und entstehen hieraus zusätzliche Kosten für den Auftragnehmer, so trägt diese der Auftraggeber. Die Löschung ist in geeigneter Weise zu dokumentieren.

f) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird. Dies gilt nicht, wenn nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung des Auftraggebers zur Speicherung der personenbezogenenDaten weiter besteht. In diesem Fall gilt für die Dauer dieser Verpflichtung dieser Vertrag entsprechend weiter.

g) Zur Verarbeitung der personenbezogenen Daten befugte Personen sind vom Auftragnehmer zur Vertraulichkeit zu verpflichten oder haben einer angemessenen gesetzlichen Verschwiegenheitspflicht zu unterliegen. Dies ist dem Auftraggeber auf Wunsch nachzuweisen.

h) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden (drohenden) Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist oder zu erfolgen droht. Die entsprechende Meldung soll zumindest folgende Informationen enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

i) Sofern es zu einer unzulässigen Verarbeitung oder Offenbarung personenbezogener Daten gekommen sein sollte, trifft der Auftragnehmer die erforderlichen Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber zum weiteren Vorgehen ab.

12. Nachweispflichten des Auftragnehmers

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

b. Für die Überprüfung der Einhaltung der jeweils vereinbarten technischen und organisatorischen Maßnahmen und deren Wirksamkeit kann der Auftragnehmer auf angemessene Zertifizierungen oder andere geeignete Prüfungsnachweise verweisen. Angemessen sind insbesondere Zertifizierungen nach Art. 40 DSGVO oder Nachweise nach Art. 42 DSGVO.

c. Daneben kommen als Nachweis in Betracht eine Zertifizierung nach ISO 27001 oder ISO 27017, eine ISO 27001- Zertifizierung auf Basis des IT-Grundschutz, eine Zertifizierung nach anerkannten und geeigneten Branchenstandards oder ein Prüfungsnachweis gemäß SOC / PS 951. Die Zertifizierungs- und Prüfungsverfahren sind von einem anerkannten unabhängigen Dritten durchzuführen. Der Auftragnehmer hat seine Zertifikate oder Prüfungsnachweise zur Verfügung zu stellen. Des Weiteren können andere geeignete Mittel (z.B. Tätigkeitsberichte des Datenschutzbeauftragten oder Auszüge aus Berichten der Wirtschaftsprüfer) zum Nachweis der Einhaltung der vereinbarten Schutzmaßnahmen dem Auftraggeber zur Verfügung gestellt werden.

13. Betroffenenrechte

a) Wenn sich eine betroffene Person mit dem Ersuchen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer wendet, wird er die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach den Angaben der betroffenen Person möglich ist, und das Ersuchen unverzüglich an den Auftraggeber weiterleiten. Soweit eine Mitwirkung des Auftragnehmers für die Umsetzung des Ersuchens - insbesondere Auskunft, Berichtigung, Sperrung oder Löschung - erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

b) Wenn der Auftraggeber nach den datenschutzrechtlichen Bestimmungen auf Haftung und Schadenersatz von einer betroffenen Person in Anspruch genommen werden sollte, verpflichtet sich der Auftragnehmer diesen gegen angemessene Vergütung bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

14. Vergütung des Auftragnehmers

Dem Auftragnehmer steht für die von ihm unter diesem Vertrag erbrachten Leistungen kein gesondertes Entgelt zu, soferndies nicht ausdrücklich anders vereinbart ist.

15. Dauer des Vertrages, Beendigung des Vertrages

Dieser Vertrag wird auf unbestimmte Zeit geschlossen. Er kann von den Vertragsparteien mit einer Frist von 4 Wochen zum Jahresende oder aus wichtigem Grund gekündigt werden.

16. Schlussbestimmungen

a) Dieser Vertrag enthält alle Vereinbarungen der Parteien zum Vertragsgegenstand. Etwaig abweichende Nebenabreden und frühere Vereinbarungen zum Vertragsgegenstand werden hiermit unwirksam.

b) Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform, soweit nicht gesetzlich eine strengere Form vorgeschrieben ist. Dies gilt auch für jeden Verzicht auf das Formerfordernis.

c) Allgemeine Geschäftsbedingungen der Parteien finden auf diesen Vertrag keine Anwendung. Dies gilt auch dann, wenn auf deren Einbeziehung in späteren Dokumenten, die im Zusammenhang mit diesem Vertrag stehen (z.B. Abruf von Leistungen) unwidersprochen hingewiesen wurde.

d) Sollte eine Bestimmung dieses Vertrages ganz oder teilweise nichtig, unwirksam oder nicht durchsetzbar sein oder werden, oder sollte eine an sich notwendige Regelung nicht enthalten sein, werden die Wirksamkeit und die Durchsetzbarkeit aller übrigen Bestimmungen dieses Vertrages nicht berührt. Anstelle der nichtigen, unwirksamen oder nicht durchsetzbaren Bestimmung oder zur Ausfüllung der Regelungslücke werden die Parteien eine rechtlich zulässige Regelung vereinbaren, die so weit wie möglich dem entspricht, was die Parteien gewollt haben oder nach dem Sinn und Zweck dieses Vertrages vereinbart haben würden, wenn sie die Unwirksamkeit oder die Regelungslücke erkannt hätten. Beruht die Nichtigkeit einer Bestimmung auf einem darin festgelegten Maß der Leistung oder der Zeit (Frist oder Termin),so gilt die Bestimmung mit einem dem ursprünglichen Maß am nächsten kommenden rechtlich zulässigen Maß als vereinbart. Es ist der ausdrückliche Wille der Parteien, dass diese salvatorische Klausel keine bloße Beweislastumkehr zur Folge hat, sondern § 139 BGB insgesamt abbedungen ist.

e) Der Vertrag unterliegt allein dem Recht der Bundesrepublik Deutschland. Das internationale Privatrecht findet keine Anwendung, soweit es abdingbar ist.

f) Alleiniger Gerichtsstand für alle Streitigkeiten im Zusammenhang mit dieser Vereinbarung ist der Sitz des Auftragnehmers.

_____	Buchholz, _____
Ort, den	Ort, den
_____	Jan F. Timme
Name Auftraggeber	Name Auftragnehmer
_____	_____
Unterschrift	Unterschrift

Anlage 1

Technische und organisatorische Maßnahmen der Unterauftragnehmer von IPBee.

I) **Vertraulichkeit** (Art. 32 Abs. 1 lit. b DSGVO)

1) Zutrittskontrolle: Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:
   a. Türsicherungen (elektrische Türöffner, Sicherheitsschloss)
   b. Sicherheitstüren (separater Schließzylinder Gebäudeeingang, Büroeingang 1. Etage)
   c. Zaunanlage abschließbar
   d. Schlüsselverwaltung/Dokumentation der Schlüsselvergabe

2) **Zugangskontrolle**: Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben:
   a. Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
   b. Begrenzung der befugten Benutzer
   c. Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
   d. Zusätzlicher System-Log-In für bestimmte Anwendungen
   e. Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
   f. Firewall

3) **Zugriffskontrolle**: Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:
   a. Verwaltung und Dokumentation von differenzierten Berechtigungen innerhalb der Systemanwendungen
   b. Abschluss von Verträgen zur Auftragsverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von personenbezogenen Daten Gegenstand der Dienstleistung ist.
   c. Profile/Rollen
   d. Vier-Augen-Prinzip
   e. Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
   f. Nicht-reversible Löschung von Datenträgern

4) **Trennungskontrolle**: Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.
   a. Speicherung der Datensätze in physikalisch getrennten Datenbanken
   b. Verarbeitung auf getrennten Systemen
   c. Zugriffsberechtigungen nach funktioneller Zuständigkeit
   d. Zugriffsberechtigungen auf Feldebene
   e. Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
   f. Mandantenfähigkeit von IT-Systemen
   g. Verwendung von Testdaten
   h. Trennung von Entwicklungs- und Produktionsumgebung

II) **Integrität** (Art. 32 Abs. 1 lit. b DSGVO)

1) **Weitergabekontrolle**: Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:
   a. Verschlüsselung von Email bzw.- Email-Anhängen (z.B. WinZip)
   b. Verschlüsselung des Speichermediums von Laptops
   c. Gesicherter File Transfer (z.B. sftp)
   d. Gesicherter Datentransport (z.B. SSL, ftps, TLS)
   e. Verschlüsselung von CD/DVD- ROM, externen Festplatten oder USB-Sticks
   f. Gesichertes WLAN
   g. Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)

2) **Eingabekontrolle**: Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat.
   a. Zugriffsrechte
   b. Systemseitige Protokollierungen
   c. Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
   d. Mehraugenprinzip

III) **Verfügbarkeit und Belastbarkeit** (Art. 32 Abs. 1 lit. b DSGVO)
Verfügbarkeitskontrolle und Belastbarkeitskontrolle: Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

a. Back-Up Verfahren
b. Bedarfsgerechtes Einspielen von Sicherheits-Updates
c. Spiegeln von Festplatten
d. Virenschutz
e. Firewall

IV) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

1) **Datenschutz-Management**: Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

a. Interne Datenschutz-Richtlinie
b. Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
c. Verpflichtung der Mitarbeiter auf das Datengeheimnis
d. Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten
e. Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)

V) **Auftragskontrolle**: Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können:

a. Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
b. Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
c. Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
d. Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
e. Verpflichtung der Mitarbeiter auf das Datengeheimnis