Vereinbarung gem. Art. 28 DSGVO über die Auftragsverarbeitung personenbezogener Daten

Stand 14.12.2020

Die nachfolgende Vereinbarung über die Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO) kommt zwischen der FinanzGeek GmbH, Brückenstraße 2, 67551 Worms, Deutschland als Auftragnehmerin (nachfolgend „Auftragnehmer“) und ihren Kunden als Auftraggeber zustande. Auftraggeber können Endkunden sein, die die Leistungen der FinanzGeek GmbH nicht lediglich zu privaten Zwecken nutzen. Der Auftraggeber beauftragt die FinanzGeek GmbH nach Maßgabe der nachfolgenden Vereinbarung mit der Verarbeitung von personenbezogenen Daten.

1. **Präambel**

   Der Auftragnehmer erbringt auf Grundlage der bestehenden vertraglichen Vereinbarung über die Nutzung der Softwareanwendung FinanzGeek für den Auftraggeber Leistungen zur Analyse und Management der Finanzen und Bankkonten des Auftraggebers sowie hiermit zusammenhängende Leistungen, wie die Verwaltung von Rechnungen, Steuern und Projektplanungen (nachfolgend „Hauptvertrag“). Hierbei verarbeitet der Auftragnehmer personenbezogene Daten, für die der Auftraggeber verantwortlich im Sinne der DSGVO bzw. der datenschutzrechtlichen Vorschriften ist.
   Mit der vorliegenden Vereinbarung zur Auftragsverarbeitung (nachfolgend „AVV“), sollen die jeweils damit verbundenen datenschutzrechtlichen Verpflichtungen konkret geregelt werden. Diese AVV soll dabei Anlage und Bestandteil des Hauptvertrages sein.

2. **Umfang der Beauftragung**

a. Die Regelungen dieser AVV gelten immer dann, sobald der Auftragnehmer im Rahmen seiner hauptvertraglichen Leistungserbringung Zugang/Zugriff zu personenbezogenen Daten (nachfolgend „Daten“) erhält, für die der Auftraggeber verantwortlich im Sinne der datenschutzrechtlichen Vorschriften ist. In diesen Fällen verarbeitet der Auftragnehmer Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt hierbei Verantwortlicher im datenschutzrechtlichen Sinn. Für die Einhaltung aller datenschutzrechtlichen Vorgaben, insbesondere der DSGVO, aber auch dafür, dass die gesetzlichen Betroffenenansprüche im Zusammenhang mit personenbezogenen Daten eingehalten werden, ist insofern der Auftraggeber verantwortlich.

b. Die Datenverarbeitung durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie folgt:

Art der Daten	**Art und Zweck der Datenverarbeitung**	**Kategorien betroffener Personen**
Rechnungsdaten (Name und Anschrift des Rechnungsempfängers, erbrachte Leistung, Betrag und Zahlungsziel)	Erstellung und Versand von Rechnungen und Mahnungen; Übermittlung von Rechnungsdaten an Steuerberater; Analyse der Zahlungsströme.	Rechnungsempfänger des Auftraggebers

Zahldaten (Kontoinhaber, Überweisungsdaten)	Management der Zahlungsein- und ausgänge. Analyse der Zahlströme.	Endkunden des Auftraggebers; Zahlungsempfänger des Auftraggebers.
Personaldaten	Management der Zahlungsein- und ausgänge. Analyse der Zahlungsströme. Vereinfachung der Organisation, Weiterleitung der personenbezogenen Daten über die Cloud an das Personal.	Personal des Auftraggebers

Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

c. Dem Auftragnehmer bleibt es vorbehalten, die Daten zu anonymisieren oder zu aggregieren, so dass eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist, und in dieser Form zum Zweck der bedarfsgerechten Gestaltung, der Weiterentwicklung und der Optimierung sowie der Erbringung des nach Maßgabe des Hauptvertrags vereinbarten Dienstes zu verwenden. Die Parteien stimmen darin überein, dass anonymisierte bzw. nach obiger Maßgabe aggregierte Daten nicht mehr als personenbezogene Daten im Sinne dieses Vertrags gelten.

d. Die Datenverarbeitung durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44 - 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

3. **Weisungsbefugnisse des Auftraggebers**

a. Der Auftragnehmer verarbeitet die Daten entsprechend den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

b. Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des im Hauptvertrag festgelegten Änderungsverfahrens, in dem die Weisung zu dokumentieren und die Übernahme etwa dadurch bedingter Mehrkosten des Auftragnehmers durch den Auftraggeber zu regeln ist.

c. Der Auftraggeber hat dafür zu sorgen, dass Weisungen möglichst klar und nachvollziehbar sind. Weisungen dürfen dabei nicht gegen das Recht der EU oder der Mitgliedstaaten verstoßen. Ist eine Weisung aus der Sicht des Auftragnehmers unklar, so wird er den Auftraggeber unverzüglich schriftlich oder per E-Mail darauf hinweisen und um Klarstellung bitten. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung (z.B. per E-Mail oder über ein Ticketsystem) an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Daten beim Auftraggeber liegt.

4. **Verantwortlichkeit des Auftraggebers**

a. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

b. Dem Auftraggeber obliegt es, dem Auftragnehmer die Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen, und er ist verantwortlich für die Qualität der Auftraggeber-Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

c. Der Auftraggeber wird dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.

d. Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

5. **Anforderung an Personal**

Zur Erfüllung seiner Verpflichtungen wird der Auftragnehmer ausschließlich Personen einsetzen, die sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen.

6. **Sicherheit der Verarbeitung (technisch organisatorische Maßnahmen)**

a. Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.

b. Die aktuellen technisch organisatorischen Maßnahmen sind in der **Anlage 1** zu dieser AVV dargestellt.

c. Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen.

7. **Einschaltung von Subunternehmern**

Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung Subunternehmer und Unterauftragsverarbeiter einzusetzen. Aktuell setzt der Auftragnehmer folgende Subunternehmer ein: Telehouse Deutschland GmbH, 1&1 IONOS SE, STRATO AG, PrimingCloud GmbH, finAPI GmbH, Colima GmbH.

a. Subunternehmer im Sinne dieser Vereinbarung nur solche, die Leistungen erbringen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung des Auftragnehmers aufweisen.
b. Finanzgeek ist berechtigt, weitere Auftragsverarbeiter ohne Genehmigung des Auftraggebers zu beauftragen. Finanzgeek wird den Auftraggeber über einen weiteren Auftragsverarbeiter

rechtzeitig informieren. Sofern der Auftraggeber aus berechtigtem Interesse gegen die Beauftragung des Weiteren Auftragsverarbeiters Einspruch erhebt, wird Finanzgeek von einem Einsatz des Subunternehmers im Zusammenhang mit den personenbezogenen Daten des Auftraggebers nach Möglichkeit Abstand nehmen. Sollte dies technisch nicht oder nur mit unverhältnismäßigem Aufwand möglich sein, steht finanzgeek ein sofortiges und außerordentliches Kündigungsrecht zu. Der Auftragnehmer wird Unterauftragsverarbeiter als Subunternehmer sodann nur beauftragen, soweit sichergestellt ist, dass diese die Voraussetzungen von Art 28 DSGVO erfüllen.

8. **Rechte der Betroffenen**

a. Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

b. Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

c. Der Auftragnehmer wird dem Auftraggeber Informationen über die gespeicherten Daten, die Empfänger von Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt, und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.

d. Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten, Auftraggeber-Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

e. Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten nach Art. 20 DSGVO besitzt, wird der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei der Bereitstellung der Auftraggeber-Daten in einem gängigen und maschinenlesbaren Format unterstützen, wenn der Auftraggeber sich die Daten nicht anderweitig beschaffen kann.

9. **Mitteilungs- und Unterstützungspflichten des Auftragnehmers**

a. Trifft den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Daten (insbesondere nach Art. 33, 34 DSGVO), wird der Auftragnehmer den Auftraggeber zeitnah über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten unterstützen.

b. Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden **Datenschutz-Folgenabschätzungen** und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

10. **Datenlöschung**

a. Der Auftragnehmer wird die Daten nach Beendigung dieses Vertrages löschen, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung dieser Daten besteht.

b. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

11. **Nachweise und Überprüfungen**

a. Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

b. Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.

c. Kommt es im Einzelfall zu einer Überprüfung durch den Auftraggeber oder von ihm beauftragten Prüfer, gilt Folgendes:

- Überprüfungen und Kontrollen haben auf eigene Kosten des Auftraggebers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs beim Auftragnehmer sowie unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers stattzufinden;
- Überprüfungen und Kontrollen sind vorab unter Berücksichtigung einer angemessenen Vorlaufzeit beim Auftragnehmer anzumelden

Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

d. Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.

e. Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von diesem § 11 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

f. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrage anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder

Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

12. **Vertragsdauer und Kündigung**

Die Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

13. **Haftung**

a. Erleidet eine Person im Zusammenhang mit der vorliegenden Auftragsdurchführung einen materiellen oder immateriellen Schaden, richtet sich die Haftung der Parteien im Innenverhältnis für diesen Schaden entsprechend des jeweiligen Anteils und jeweiligen Verantwortung der betreffenden Partei. Wird hierbei eine Partei ganz oder überwiegend auf Schadensersatz in Anspruch genommen, so kann die in Anspruch genommene Partei gegenüber der anderen Freistellung oder Schadloshaltung verlangen, wenn dies ihrem Anteil an der Verantwortung entspricht.

b. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

c. Der Auftragnehmer ist berechtigt, zum Zwecke der eigenen Enthaftung gemäß Art 82 Absatz 3 DS-GVO Details zu Weisungen des Auftraggebers sowie zur erfolgten Datenverarbeitung offenzulegen. Der Auftraggeber wird alles Erforderliche veranlassen, damit sich der Auftragnehmer in diesem Zusammenhang Dritten gegenüber enthaften kann.

d. Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

14. **Schlussbestimmungen**

a. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.

b. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

Anlage 1 „Technisch organisatorische Maßnahmen“ des Auftragnehmers

Inhalt

Der Verantwortliche hat geeignete Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert.

Der allgemeine Teil beschreibt technische und organisatorische Maßnahmen die unabhängig von den jeweiligen Dienstleistungen und Services, Standorten und Kunden gelten. In den Anhängen sind Maßnahmen beschrieben, die über die im allgemeinen Teil dokumentierten Maßnahmen hinaus gelten.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a. **Zutrittskontrolle**
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel (-Konzept), elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

---

b. **Zugangskontrolle**
Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern und/oder externen Schnittstellen (USB, HDMI etc.), Passwortvergabe, Passwortrichtlinie, VPN, Firewall Hardware/Software;

---

c. **Zugriffskontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen, ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)

---

d. **Trennungskontrolle**
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing, Berechtigungskonzept, logische Mandantentrennung;

---

e. **Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)**
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

---

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

a. **Weitergabekontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur, E-Mail-Verschlüsselung;

---

b. **Eingabekontrolle**
Berechtigungskonzept, Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement, Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen);

---

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a. **Verfügbarkeitskontrolle**
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne, Feuer- und Rauchmelder, Feuerlöschgeräte in Serverraum;

---

b. **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);**

Die Verfügbarkeit von personenbezogenen Daten ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können

- Einsatz von Hardware- und Softwarefirewalls
- Intrusion Detection Systeme
- Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag
- Unterbrechungsfreie-Stromversorgung (USV)
- Notfallhandbücher für die Datenwiederherstellung, Schutz gegen versehentliche Zerstörung und Verlust
- Durchführung von Wiederherstellungstests
- Wo notwendig Nutzung redundanter Systeme (z.B. RAID)
- Regelmäßiger Test von Datensicherungen
- Externe Audits und Sicherheitstests

---

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

a. **Datenschutz-Management;**

- Datenschutzbeauftragte und ein Informationssicherheitsbeauftragter sind benannt
- Etablierung einer Datenschutz- und Informationssicherheitsorganisation
- Alle Mitarbeiter sind auf die Vertraulichkeit im Umgang mit personenbezogenen

Daten verpflichtet und werden auf das Telekommunikationsgeheimnis hingewiesen
- Mitarbeiter sind im Umgang mit personenbezogenen Daten sensibilisiert
- Neue Mitarbeiter erhalten Informationsmaterial bezüglich des Umgangs mit personenbezogenen Daten
- Ein Verzeichnis von Verarbeitungstätigkeiten wird gepflegt und Datenschutzfolgenabschätzungen werden bei Bedarf durchgeführt
- Prozesse zur Wahrnehmung von Betroffenenrechten sind etabliert

---

b. **Incident-Response-Management;**

   a. Dokumentierter Prozess zur Erkennung, Meldung und Dokumentation von Datenschutzverletzungen unter Einbindung des Datenschutzbeauftragten
   b. Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen unter Einbindung des Informationssicherheitsbeauftragten

---

c. **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);**

   a. Es wird prozessual sichergestellt, dass Systeme und Produkte datenschutzfreundlich entwickelt werden
   b. Es werden nur diejenigen personenbezogenen Daten erhoben, die für den jeweiligen Zweck erforderlich sind

---

d. **Auftragskontrolle**

   Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.
