AUFTRAGSVERARBEITUNG

Dieser Vertrag regelt die datenschutzrechtlichen Pflichten des Kunden (nachfolgend: „Auftraggeber“) und der

taxflix GmbH & Co. KG, Oststraße 11, 50996 Köln (nachfolgend: „Auftragnehmer“)

in Bezug auf die Auftragsverarbeitung personenbezogener Daten im Rahmen der Nutzung von **Taxflix**, einer Online-Fortbildungsplattform für Steuerberatungskanzleien zur Durchführung und Verwaltung digitaler Weiterbildungsangebote.

1. Gegenstand, Dauer des Auftrags, Art und der Zweck der Verarbeitung, Art der Daten, Kategorien der Betroffenen

a) Gegenstand dieses Auftrags ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Rahmen der Bereitstellung und Administration der Taxflix-Plattform sowie der hierzu optional bereitgestellten API-Schnittstelle, insbesondere die automatisierte Anlage und Verwaltung von Nutzerkonten sowie die Authentifizierung und Rechteverwaltung der vom Auftraggeber beziehungsweise dessen Systemen über die API benannten und angelegten Nutzer.
b) Die Dauer dieses Auftrags entspricht der Laufzeit des zugrunde liegenden Hauptvertrags über die Nutzung der Taxflix-Plattform. Der Auftrag endet automatisch mit Beendigung des Hauptvertrags, unbeschadet der Löschungs- und Rückgabepflichten nach Vertragsende gemäß Art. 28 Abs. 3 lit. g) DS-GVO.
c) Der Auftragnehmer erhebt, übermittelt, speichert und nutzt die personenbezogenen Daten des Auftraggebers zu Abwicklungs-, Abrechnungs- und Fortbildungszwecken.
Im Rahmen der vom Auftragnehmer bereitgestellten API-Schnittstelle dient die Verarbeitung ausschließlich der Anlage von Nutzerkonten, der Authentifizierung der Nutzer, der Verwaltung von Zugriffsrechten, der Administration der Plattformnutzung sowie dem Versand von Informationen per E-Mail.
Der Auftragsverarbeiter verarbeitet im Rahmen der Plattformnutzung anfallende Nutzungsdaten (insbesondere aufgerufene Inhalte, Zeitpunkt und Dauer der Nutzung) zu folgenden Zwecken: zur Generierung von Teilnahmebescheinigungen sowie, sofern vom Auftraggeber gewünscht, zur individuellen Bereitstellung von Lerninhalten anhand des festgestellten Nutzungsverhaltens (individuelle Lernpfade).
Im Übrigen werden Nutzungsdaten dem Auftraggeber ausschließlich zu dessen eigenem Controlling zur Verfügung gestellt und insoweit nicht im Verantwortungsbereich des Auftragsverarbeiters ausgewertet.
Eine Verarbeitung von Nutzungsdaten zu eigenen Zwecken des Auftragsverarbeiters, insbesondere zu eigenen Marketing- oder Analysezwecken außerhalb der vorgenannten Zwecke, erfolgt nicht.Der Auftragsverarbeiter stellt dem Auftraggeber eine KI-gestützte Suchfunktion zur Beantwortung von Nutzeranfragen zur Verfügung. Zu diesem Zweck werden Chatverläufe personenbezogen gespeichert. Die Verarbeitung erfolgt ausschließlich zur Beantwortung der jeweiligen Nutzeranfrage sowie zur technischen Bereitstellung der Funktion; eine Verwendung der Chatverläufe zu eigenen Zwecken des Auftragsverarbeiters, insbesondere zum Training oder zur Verbesserung von KI-Modellen, erfolgt nicht
d) Im Rahmen der allgemeinen Nutzung der Taxflix-Plattform verarbeitet der Auftragnehmer den Namen des Auftraggebers, den Namen seines Unternehmens, die Postanschrift, die Telefonnummer sowie die E-Mail-Adresse, ferner audiovisuelle Aufnahmen, soweit diese im Rahmen der Fortbildungsmaßnahmen entstehen.
Im Rahmen der vom Auftragnehmer bereitgestellten API-Schnittstelle verarbeitet der Auftragnehmer Vorname, Nachname und E-Mail-Adresse, jeweils beschränkt auf das für die Bereitstellung und Verwaltung des Nutzerzugangs Erforderliche.
Im Rahmen der Plattformnutzung verarbeitet der Auftragnehmer ferner Nutzungsdaten (insbesondere aufgerufene Inhalte, Zeitpunkt und Dauer der Nutzung) sofern vom Auftraggeber gewünscht auch zur individuellen Bereitstellung von Lerninhalten, sowie personenbezogen gespeicherte Chatverläufe im Rahmen der KI-gestützten Suchfunktion.
Eine Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO ist im Rahmen dieses Auftragsverarbeitungsvertrags nicht vorgesehen. Sollten betroffene Personen gleichwohl unaufgefordert solche Daten übermitteln, etwa in Freitextfeldern, sind diese unverzüglich zu löschen.
e) Kategorien betroffener Personen sind die zur Nutzung der Taxflix-Plattform berechtigten Mitarbeiter des Auftraggebers.

2. Sicherheit der Verarbeitung

Der Auftragnehmer hält in seinem Verantwortungsbereich die vereinbarten technischen und organisatorischen Maßnahmen gemäß Art. 5 Abs. 1 und Art. 32 DS-GVO ein und hat seine innerbetriebliche Organisation gemäß datenschutzrechtlichen Anforderungen gestaltet. Dies beinhaltet die in der **Anlage** dargestellten technisch organisatorischen Maßnahmen.

3. Berichtigung, Löschung und Einschränkung von Daten

Eine Berichtigung, Sperrung oder Löschung der im Auftrag verarbeiteten Daten nimmt der Auftragnehmer nur nach Weisung des Auftraggebers vor. Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen, vorausgesetzt der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert.

4. Pflichten des Auftragnehmers

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen oder zu löschen oder die Verarbeitung einzuschränken. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten oder der Einschränkung der Verarbeitung

wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Der Auftragnehmer wird den Auftraggeber im Falle der Geltendmachung gesetzlicher Betroffenenrechte unterstützen; dies umfasst insbesondere die Unterstützung bei der Beantwortung von Anträgen auf Wahrung der Betroffenenrechte mittels geeigneter technisch-organisatorischer Maßnahmen.

5. Pflichten des Auftragnehmers

Der Auftragnehmer gewährleistet die Einhaltung der folgenden Pflichten:

a) Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Sofern ein Wechsel in der Person des Datenschutzbeauftragten stattfindet, wird dies dem Auftraggeber unverzüglich mitgeteilt.

b) Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen schriftlich zur Vertraulichkeit verpflichtet sein und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden. Auf Anfrage des Auftraggebers wird der Auftragnehmer diesem die Verpflichtungserklärungen vorlegen. Dies ist nicht notwendig, soweit für die betreffenden Personen eine angemessene gesetzliche Verschwiegenheitspflicht besteht.

c) Duldung öffentlicher Kontrollen durch die zuständigen Datenschutzaufsichtsbehörden in gleichem Umfang, wie die Datenschutzaufsichtsbehörden Prüfungen beim Auftraggeber durchführen dürfen. Unterstützung des Auftraggebers bei Kontrollen und Anfragen der Aufsichtsbehörden.

d) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde. Dies gilt auch, soweit eine zuständige Behörde nach Art. 82 ff. DS-GVO bei dem Auftragnehmer ermittelt.

e) Die angemessene Unterstützung des Auftraggebers bei der Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO.

f) Die angemessene Unterstützung des Auftraggebers bei Datenschutz-Folgenabschätzungen gemäß Art. 35 DS-GVO und bei der vorherigen Konsultation der zuständigen Datenschutzaufsichtsbehörden nach Art. 36 DS-GVO.

g) Die angemessene Unterstützung des Auftraggebers bei der Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DS-GVO) und bei der Benachrichtigung der von Verletzungen des Schutzes personenbezogener Daten betroffenen Personen (Art. 34 DS-GVO).

h) Die Vorlage der nach Art. 30 Abs. 2 DS-GVO erforderlichen Angaben.

6. Unterauftragsverhältnisse

Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglichen Leistungen verbundenen Unternehmen Unteraufträge erteilt. Bei Erteilung eines Unterauftrags werden die vertraglichen Vereinbarungen zwischen dem Auftragnehmer und dem Unterauftragnehmer so gestaltet, dass sie den Anforderungen zu Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages entsprechen. Der Auftraggeber einer Unterbeauftragung widersprechen. Eine aktuelle Liste aller Unterauftragsverarbeiter des Auftragnehmers wird auf Anfrage zur Verfügung gestellt; anfragenden Auftraggebern werden Änderungen mit einer Frist von vier Wochen vor Tätigwerden mitgeteilt. Der Auftragnehmer erteilt dem Auftraggeber auf dessen schriftliche Aufforderung hin Auskunft über den wesentlichen Vertragsinhalt (Leistungen ausschließlich Preise) und die Umsetzung der datenschutzrelevanten Pflichten des Unterauftragnehmers.

7. Ort der Verarbeitung

Die Verarbeitung der Daten durch den Auftragnehmer ist räumlich auf die EU und den EWR beschränkt. Die Übermittlung von Daten durch den Auftragnehmer an einen Empfänger mit Sitz außerhalb des EWR ist nur unter den Voraussetzungen der Art. 44 ff. DS-GVO zulässig und bedarf der gesonderten vorherigen schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer wird insbesondere die EU-Standardvertragsklauseln (vgl. den Beschluss 2021/914 der EU-Kommission vom 04.06.2021 oder eine Nachfolgeentscheidung) mit dem Empfänger der Daten abschließen, wenn keine anderweitigen geeigneten Datenschutzgarantien vorhanden sind, z.B. ein Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DS-GVO oder verbindliche interne Datenschutzvorschriften nach Art. 47 DS-GVO.

8. Kontrollrechte des Auftragnehmers

Der Auftraggeber kann sich nach rechtzeitiger schriftlicher Anmeldung zu Prüfzwecken in den Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Gesetze über den Datenschutz überzeugen. Der Auftragnehmer ist verpflichtet, die Kontrollen des Auftraggebers oder eines von diesem beauftragten Prüfers nach diesem Vertrag zu dulden, Mitwirkungsleistungen zu erbringen, soweit für die Kontrolle des Auftraggebers oder eines von diesem beauftragten Prüfers nach diesem Vertrag erforderlich, und dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist Auskünfte zu geben, die zur Durchführung einer umfassenden Auftragskontrolle erforderlich sind. Der Auftragnehmer ermöglicht dem Auftraggeber insbesondere, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

9. Mitteilungen von Datenschutzverletzungen und Fehlern der Verarbeitung

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung, eine Meldung, wenn durch ihn, die bei ihm beschäftigten Personen oder die von ihm eingesetzten Unterauftragnehmer Verstöße gegen Vorschriften zum Schutz der Daten des Auftraggebers (insbesondere die DS-GVO) oder gegen die in dieser Vereinbarung getroffenen Festlegungen vorgefallen sind bzw. ein entsprechender Verdacht besteht, auch bei schwerwiegenden Störungen des Betriebsablaufes. Der Auftragnehmer wird entsprechende

Vorfälle dokumentieren, unverzüglich aufklären und Abhilfe schaffen. Er wird den Auftraggeber über den Fortgang der Angelegenheit bis zur Behebung des Vorfalls informiert halten. Sollte die Verletzung zu einem Risiko für die Rechte und Freiheiten der Betroffenen gemäß Art. 33 DS-GVO führen, wird der Auftragnehmer den Auftraggeber bei der Aufklärung des Vorfalls und im Rahmen der entsprechenden Meldung an die Datenschutzaufsichtsbehörde bzw. die Betroffenen umfassend unterstützen.

10. Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer wird die Weisungen soweit erforderlich dokumentieren.

11. Weisungsbefugnis des Auftraggebers

Der Auftraggeber ist nach freiem Ermessen zur Erteilung von Weisungen an den Auftragnehmer in Bezug auf die Datenverarbeitung berechtigt. Der Auftragnehmer darf Daten nur im Rahmen des Vertrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Berichtigung, Sperrung, Löschung, Herausgabe) mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden (Einzelweisung). Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Erteilt der Auftraggeber Einzelweisungen, die über die Anforderungen der DS-GVO und des BDSG oder über die Anforderungen von anderen datenschutzrechtlichen Gesetzen hinausgehen, trägt der Auftraggeber sämtliche dem Auftragnehmer dadurch verursachten Kosten.

Ist der Auftragnehmer unions- oder mitgliedstaatsrechtlich zu einer von den Weisungen des Auftraggebers abweichenden Verarbeitung verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor Beginn der Verarbeitung in Textform mit, es sei denn, das Recht verbietet dies wegen eines wichtigen öffentlichen Interesses.

12. Vertragsende

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, binnen vier Wochen nach Wahl des Auftraggebers dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren und lediglich für diese Zwecke zu nutzen. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

13. Rückgabe und Löschung von Daten

Vorbehaltlich abweichender Vereinbarungen und gesetzlicher oder satzungsmäßiger Pflichten ist der Auftragnehmer nach Vertragsende verpflichtet, ihm überlassene Datenträger an den Auftraggeber unverzüglich zurückzugeben und ihm in Zusammenhang mit dem Auftrag übergebene und noch nicht gelöschte personenbezogene Daten zu löschen. Über die Herausgabe oder Löschung nach Vertragsende muss der Auftraggeber innerhalb einer vom Auftragnehmer gesetzten Frist entscheiden. Wenn der Auftragnehmer zu vernichtende Unterlagen oder Datenträger mit personenbezogenen Daten dem Auftraggeber nicht zurückgibt, so ist der Auftragnehmer verpflichtet, die Unterlagen ordnungsgemäß zu entsorgen, ohne dass unbefugte Dritte von den Daten Kenntnis erlangen können. Entstehen dem Auftragnehmer nach Vertragsbeendigung Kosten durch die Herausgabe oder Löschung der Daten des Auftraggebers, welche über den üblicherweise hierfür erforderlichen Aufwand hinausgehen, so trägt diese der Auftraggeber.

Anlage: Technische und organisatorische Maßnahmen des Auftragnehmers (Art. 32 DS-GVO, § 64 BDSG)

1) Der Auftragnehmer hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten
2) Diese Maßnahmen können unter anderem die Pseudonymisierung und die Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind.
3) Die Maßnahmen sollen dazu führen, dass
a) die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und,
b) dass die Verfügbarkeit personenbezogener Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.
4) Der Auftragsverarbeiter hat nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

Zugangskontrolle
- ✓ Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte. Zweckmäßige Maßnahmen sind unter anderem:
- ✓ Zutrittskontrollsystem, zentrale Schlüsselverwaltung, Magnetkarte
- ✓ Schlüssel/Schlüsselvergabe ist zentral und organisatorisch klar geregelt
- ✓ Klare Zuweisung der Berechtigungen (Zugang Gebäude, Büro, Serverraum)
- ✓ Gebäudeschutz an Wochenenden und nachts gewährleistet
- ✓ Pförtner/Empfang mit Videoüberwachung
- ✓ Regelungen für Besucher (Besucherausweis, Begleitung im Gebäude)
- ✓ Videoüberwachung sensibler Bereiche des Gebäudes (Tiefgarage)
- ✓ Verschließen von Schränken und Büros bei Nichtanwesenheit

Datenträgerkontrolle
Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern. Zweckmäßige Maßnahmen sind unter anderem:
- ✓ Dezidiertes Kennwortverfahren zum Login [z.B. Klare Passwortregelung (bestimmte Länge, Kombination aus Buchstaben und Zahlen, keine Trivialpasswörter, Änderung in regelmäßigen Abständen). Voreingestellte Passwörter müssen umgehend geändert werden]
- ✓ Automatische Sperrung (z.B. Regelung zur automatischen Sperrung des Computers nach einer bestimmten Zeit der Inaktivität (ca. 5 min) mit anschließendem erneutem Login)
- ✓
- ✓ Automatischer Standby-Betrieb der lokalen Rechner
- ✓ Verschlüsselung von Datenträgern möglich
- ✓ Besondere Vorsicht bei Mitnahme von Laptop/Datenträgern/Smartphones aus den Büroräumen heraus
- ✓ Möglichkeit der Fernlöschung von Smartphones

Speicherkontrolle
Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

Benutzerkontrolle
Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

Zugriffskontrolle
Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben. Zweckmäßige Maßnahmen sind unter anderem:
- ✓ Differenzierte Berechtigungen (Profile, Rollen)
- ✓ Differenziertes Ordnerkonzept (z.B. alle Dateien sind einheitlich und nachvollziehbar zu benennen und so abzuspeichern, dass sie problemlos wiedergefunden werden können).
- ✓ Datenträger sind eindeutig zu kennzeichnen und sicher aufzubewahren.
- ✓ Sichere Löschung von Daten und/ oder Vernichtung von Datenträgern.
- ✓ Ordnung am Arbeitsplatz [Datenträger (USB-Sticks, CD-ROMs) mit vertraulichem Material dürfen nicht offen herumliegen].
- ✓ Anpassung sicherheitsrelevanter Standardeinstellungen von neuen Programmen und IT-Systemen
- ✓ Deinstallation bzw. Deaktivierung nicht benötigter sicherheitsrelevanter Programme und Funktionen (v.a. bei Smartphones)

Übertragungskontrolle
Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Eingabekontrolle
Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind. Zweckmäßige Maßnahmen sind unter anderem:
- ✓ Protokollierungs- und Protokollauswertungssysteme werden eingesetzt bzw. sind als Teile von bestehenden Softwareapplikationen anwendbar
- ✓ Zugriff auf Datenverarbeitungssysteme nur nach Login möglich
- ✓ Keine Weitergabe von Passwörtern

- ✓ Zusätzlich zur automatischen Sperrung: manuelle Abmeldung beim Verlassen des Büros

Transportkontrolle
Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Verschlüsselung (insbes. Laptops)
- ✓ Tunnelverbindung (VPN = Virtual Private Network)
- ✓ Elektronische Signatur möglich
- ✓ Keine Benutzung von nicht freigegebener Hard-/ Software
- ✓ Keine Weiterleitung von E-Mails an private E-Mail-Accounts von Mitarbeitern
- ✓ Vorsicht beim Umgang mit Backup-Bändern
- ✓ Vorgaben an Mitarbeiter bzgl. Ausdrucken von geheimen Unterlagen (Sicherstellung, dass kein anderer Zugriff auf Ausdrucke bekommt).
- ✓ Regelung zum Einsatz von USB-Sticks und CD-ROMs

Wiederherstellbarkeit
Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Zuverlässigkeit
Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Datenintegrität
Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Auftragskontrolle
Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Eindeutige Vertragsgestaltung/Standardvertrag zu Art. 28 DS-GVO vorhanden
- ✓ Formalisierte Auftragserteilung (Auftragsformular)
- ✓ Kriterien zur Auswahl des Auftragnehmers wird stringent eingehalten
- ✓ Kontrolle der Vertragsausführung wird durch den DSB gewährleistet

Verfügbarkeitskontrolle
Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Regelmäßiges Backup-Verfahren ist sichergestellt (Definition: Welche Daten werden wie lange gesichert?; Einbeziehung von Laptops und nicht vernetzten Systemen; Regelmäßige Kontrolle der Sicherungsbänder; Dokumentierung der Sicherungsverfahren)
- ✓ Getrennte Aufbewahrung von Daten ist gewährleistet
- ✓ Virenschutz/Firewall nach aktuellem Stand der Technik ist gewährleistet
- ✓ Schutz gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall im Serverraum
- ✓ Notfallplan besteht und wird regelmäßig geübt
- ✓ Notstromversorgung/Unterbrechungsfreie Stromversorgung (USV)
- ✓ Besondere Vorsicht bei Mitnahme von Laptop/Datenträger aus den Büroräumen heraus
- ✓ Vertretungsregelungen, v.a. bzgl. Administrator

Trennbarkeit
Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Physisch und/oder logisch getrennte Speicherung, Veränderung, Löschung und Übermittlung von Daten, die unterschiedlichen Zwecken dienen (Mandantenfähigkeit)
- ✓ Funktionstrennung, insbesondere zwischen Produktions- und Testdaten

Regelmäßige Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen

- ✓ Regelmäßige fachliche Fortbildung der IT-Verantwortlichen und des betrieblichen Datenschutzbeauftragten
- ✓ Schulung der Mitarbeiter im Umgang mit der IT und zur Schärfung des IT-Sicherheitsbewusstseins
- ✓ Sicherheitshinweise werden allen Mitarbeitern in geeigneter Form bekannt gegeben und sind dauerhaft abrufbar (z.B. durch Veröffentlichung im Intranet)
- ✓ Auswertung von Meldungen und Berichten zu ungewöhnlichen Vorkommnissen
- ✓ Untersuchung erkannter oder vermuteter Verstöße gegen sicherheitsrelevante Vorgaben
- ✓ Regelmäßige Prüfung der Effektivität der bestehenden technischen und organisatorischen Maßnahmen und Prüfung, ob neue technische und organisatorische Maßnahmen erforderlich sind (beides unter Hinzuziehung des Datenschutzbeauftragten)
- ✓ Regelmäßige und anlassbezogene Kontrolle der Funktionalität der IT, einschließlich unter dem Aspekt der Zutrittskontrolle
- ✓ Eskalations- und Meldewege bei sicherheitsrelevanten Vorkommnissen
- ✓ Verfügbarkeit der IT-Verantwortlichen und des betrieblichen Datenschutzbeauftragten als Ansprechpartner bei allen Fragen zur IT-Nutzung und -sicherheit.