Anlage 5: Vertrag zur Auftragsverarbeitung

Allgemeines

Diese Vereinbarung wird zwischen den Parteien als ergänzende Regelung zur Einhaltung der datenschutzrechtlichen Regelungen gemäß Art. 28 der Datenschutz-Grundverordnung (DSGVO) getroffen und konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem mit Actaport geschlossenen Vertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben.

.

Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i. S. d. Art. 4 Nr. 2 DSGVO zugrunde gelegt. Der Provider wird nachfolgend als „Auftragnehmer“ bezeichnet.

1. Gegenstand des Vertrages

1.1. Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Bereitstellung, Weiterentwicklung und Pflege der cloudbasierten SaaS-Anwendung „Actaport“ auf Grundlage des „Nutzungsvertrag Actaport“ (nachfolgend als „Hauptvertrag“ bezeichnet). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag Art. 1, den dazugehörigen AGB sowie der dazugehörigen Leistungsbeschreibung. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

1.2. Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrages vor.

1.3. Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

2. Art der verarbeiteten Daten, Kreis der Betroffenen

2.1. Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf personenbezogenen Daten. Diese Daten umfassen

- Namen, Adress-, Bank- und Kontaktdaten wie E-Mail-Adresse und Telefonnummer von Mandanten des Auftraggebers
- Namen, Adress-, Bank- und Kontaktdaten wie E-Mail-Adresse und Telefonnummer von Gegner der Mandanten des Auftraggebers
- Name und Kontaktdaten der Beschäftigten des Auftraggebers
- Inhalte der Kommunikation, insb. Mandantenunterlagen

2.2. Kreis der von der Datenverarbeitung Betroffenen:

- Beschäftigte des Auftraggebers
- Mandanten des Auftraggebers
- Dritte wie Gegner der Mandanten des Auftraggebers, Gerichte, Gerichtsvollzieher, Versicherungen und andere in der Mandatsbearbeitung involvierte Personen

3. Laufzeit

3.1. Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben

3.2. Ein außerordentliches Kündigungsrecht jeder Partei bleibt unberührt.

4. Weisungsrecht

4.1. Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

4.2. Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

4.3. Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

4.4. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

4.5. Die Parteien können weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der Anhang 3 benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber oder beim Auftragnehmer ändern, wird dies die jeweilige Partei die andere Partei in Textform mitteilen.

4.6. Sofern der Auftragnehmer durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, dazu verpflichtet ist, personenbezogene Daten außerhalb der Weisungen des Auftraggebers zu verarbeiten, 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.

5. Allgemeine Pflichten und Schutzmaßnahmen des Auftragnehmers, Vertraulichkeit

5.1. Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Zusammenhang mit dem Hauptvertrag im Auftrag verarbeitet, vor der unbefugten Kenntnisnahme Dritter geschützt sind.

5.2. Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich, spätestens innerhalb von 48 Stunden, informieren, ausgenommen von dieser Frist sind Wochenenden und Feiertage.

5.3. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegt.

5.4. Der Auftragnehmer wird seinen Pflichten aus Art. 30 Abs. 2 DSGVO zum Führen eines Verarbeitungsverzeichnisses nachkommen.

5.5. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Art. 33-36 DSGVO genannten Pflichten, soweit der Auftraggeber insoweit auf die Unterstützung des Auftragnehmers angewiesen ist.

5.6. Der Auftragnehmer trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO. Dem Auftraggeber sind diese in der im Anhang 1 zu dieser Vereinbarung dargestellten, technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

5.7. Der Auftragnehmer hat die HB E-Commerce Rechtsanwaltsgesellschaft mbH, Kohlgartenstraße 11-15, 04105 Leipzig, datenschutz@hb-ecommerce.eu zur externen Datenschutzbeauftragten nach Art. 37 DSGVO und § 38 BDSG benannt.

5.8. Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Dies gilt insbesondere in den Fällen, in denen der Auftraggeber zur Einhaltung der Schweigepflicht aus § 203 StGB verpflichtet ist. Der Auftraggeber wird dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitteilen.

5.9. Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird seine Beschäftigten und durch ihn Beauftragte, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden, entsprechend verpflichten und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.

5.10. Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Dies gilt auch für alle Unterauftragsverhältnisse. Eine Verarbeitung der personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers, die zumindest in Textform erfolgen muss. Eine Zustimmung des Auftraggebers kommt nur dann in Betracht, wenn gewährleistet ist, dass die jeweils nach den Art. 44 – 49 DSGVO einzuhaltenden Rechtsvorschriften eingehalten werden, um ein angemessenes Schutzniveau für den Schutz der personenbezogenen Daten zu gewährleisten.

6. Kontrollrechte des Auftraggebers

6.1. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren. Der Auftragnehmer unterstützt den Auftraggeber bei der Durchführung und Umsetzung der Kontrollrechte.

6.2. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle im Sinne des Absatz 1 erforderlich sind.

6.3. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese in der Regel zu den üblichen Geschäftszeiten ohne wesentliche Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Sollte der durch den Auftraggeber beauftragte Prüfer in einem direkten Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

6.4. Der Auftragnehmer stellt dem Auftraggeber auf dessen Anforderung hinreichende Garantien zur Verfügung, dass die Subunternehmer nach Ziffer 7.4. geeignete technische und organisatorische Maßnahmen implementiert haben, sodass die Verarbeitung im Einklang mit der DSGVO erfolgt.

6.5. Für die Ermöglichung der Kontrollrechte durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen, sofern kein Verstoß gegen geltende Gesetze oder die vorstehende Vereinbarung vorliegt.

6.6. Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO i.V.m. § 40 BDSG, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen.

7. Unterauftragsverhältnisse

7.1. Der Auftraggeber stimmt zu, dass der Auftragnehmer, die in Anhang 2 genannten Subunternehmer zur Erfüllung der vertraglich vereinbarten Leistungen hinzuzieht. Vor Hinzuziehung weiterer oder Ersetzung der bisherigen Subunternehmer informiert der Auftragnehmer den Auftraggeber. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz

personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer hat zudem mit dem Subunternehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Subunternehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

7.2. Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist von 14 Tagen – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

7.3. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln und ggf. Schaffung weiterer Garantien).

7.4. Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, wenn keine Verarbeitung von Daten im Auftrag des Verantwortlichen erfolgt, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen und Nebenleistungen, wie beispielsweise Transport und Wartung ohne Zugriff auf personenbezogene Daten, Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice ohne Zugriff auf personenbezogene Daten, die im Auftrag verarbeitet werden, sind nicht erfasst. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

7.5. Kommt ein Subunternehmer seinen datenschutzrechtlichen Pflichten im Zusammenhang mit der Verarbeitung von personenbezogenen Daten des Auftraggebers nicht nach, so haftet der Auftragnehmer nach Art. 28 Abs. 4 Satz 2 DSGVO gegenüber dem Auftraggeber für die Einhaltung der Pflichten des betroffenen Subunternehmers.

8. Anfragen und Rechte Betroffener

8.1. Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

8.2. Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, der Pflicht des Auftraggebers zur Beantwortung und Erfüllung von Anfragen von Betroffenen nach den Art. 12 - 23 DSGVO nachzukommen, soweit der Auftraggeber insoweit auf die Unterstützung des Auftragnehmers angewiesen ist.

9. Haftung

9.1. Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung

9.2. Die Parteien stellen sich gegenseitig frei von Ansprüchen betroffener Personen, die nicht auf einem Verschulden der jeweils anderen Partei beruhen. Dies gilt nur dann, wenn der freistellenden Partei ein Verschulden vorzuwerfen ist. Die Beweislast für das fehlende Verschulden trägt die jeweilige Partei. Diese Entlastung gilt nur, wenn beide Parteien schriftlich zustimmen, bevor sie Ansprüche Dritter anerkennen oder Vergleiche (gerichtlich oder außergerichtlich) schließen

10. Beendigung des Hauptvertrages

10.1. Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags und Beendigung der Verarbeitungsleistungen oder jederzeit auf dessen Anforderung alle personenbezogenen Daten nach Wahl des Auftraggebers, alle ihm überlassenen Unterlagen, Daten und Datenträger, sowie erstellten Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen zurückgeben, soweit der Auftraggeber darauf nicht selbst Zugriff nehmen kann, oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Kopien und Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung bei Vertragsbeendigung noch vorhandener Daten zu führen.

10.2. Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

11. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

Anhänge

Anhang 1 – Technische und organisatorische Maßnahmen des Auftragnehmers
Anhang 2 – Genehmigte Subunternehmer

Anhang 1:
Technische und organisatorische Maßnahmen des Auftragnehmers zum Datenschutz gemäß Art. 32 DSGVO

Der Auftragnehmer ist verpflichtet, nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO einzuhalten:

12. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.
Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

X	elektronisches Schließsystem Außentüren	X	Sicherheitsschlösser
X	Türen mit Knauf Außenseite	X	Klingelanlage mit Kamera
X	elektronische Zutrittstoken (personalisiert)	X	Empfang / Rezeption / Pförtner
X	Besucher in Begleitung durch Mitarbeiter	X	Absicherung der Gebäudeschächte
X	Sorgfalt bei Auswahl der Reinigungsdienste	X	Manuelles Schließsystem Innentüren
X	Schlüsselregelung / Liste		

13. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.
Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen,

Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

X	Login mit Benutzername und Passwort	X	Firewall
X	Separieren der Prozesse	X	Anti-Virus-Software Clients
X	VPN bei Remote Zugriffen	X	Verschlüsselung von Datenträgern
X	Automatische Desktopsperre	X	Schlüsselregelung
X	Personenkontrolle Pförtner / Empfang	X	OTP-Verfahren
X	Verwalten von Benutzerberechtigungen (Cloud Systeme)	X	Erstellen von Benutzerprofilen
X	Richtlinie „Sicheres Passwort“	X	Richtlinie Datenschutz
X	Richtlinie „IT-Security“	X	Richtlinie für allgemeine Sicherheit am Arbeitsplatz
X	Anleitung „Manuelle Desktopsperre“	X	Richtlinie „Clean Desk“
X	Kontrollgruppen	X	System-Policies

14. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

X	Einsatz Berechtigungskonzepte	X	Minimale Anzahl an Administratoren
X	Verwaltung Benutzerrechte durch Administratoren	X	Protokollierung von Zugriffen auf Anwendungen, konkret bei der

			Eingabe, Änderung und Löschung von Daten
X	Sichere Aufbewahrung von Datenträgern	X	Zeitlich begrenzte Berechtigung über Tokens

15. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

X	Trennung von Produktiv- und Testumgebung	X	Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
X	Mandantenfähigkeit relevanter Anwendungen	X	Steuerung über Berechtigungskonzept
X	Festlegung von Datenbankrechten	X	Datensätze sind mit Zweckattributen versehen

16. Pseudonymisierung

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.

X	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist zu anonymisieren / pseudonymisieren		

17. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an

welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

X	Verschlüsselung von Datenträgern	X	Nutzung von verschlüsselten Protokollen wie https und sftp
X	Nutzung von Signaturverfahren	X	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
X	Sorgfalt bei Auswahl von Transportdienstleister	X	Einschränkung des Zugriffs von passwortgeschützten Daten auf Zeitraum und Häufigkeit

18. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

X	Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	X	Nachvollziehbarkeit von Eingabe, Änderung oder Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
X	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	X	Klare Zuständigkeiten für Löschungen

19. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

X	Feuer- und Rauchmeldeanlagen	X	Feuerlöscher Serverraum
X	Serverraum klimatisiert	X	Schutzsteckdosenleiste Serverraum mit Überspannungsschutz
X	RAID System / Festplattenspiegelung	X	Getrennte Partitionen für Betriebssysteme und Daten
X	Systemmonitoring / Alerting		

20. Datenschutzmaßnahmen

X	Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mindestens jährlich durchgeführt	X	Datenschutzbeauftragter
X	Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet	X	Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
X	Datenschutz-Folgenabschätzung (DSFA wird bei Bedarf durchgeführt)	X	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

21. Incident-Response-Management

X	Einsatz von Firewall und regelmäßige Aktualisierung	X	Einbindung von DSB / ISB in Sicherheitsvorfällen und Datenpannen
X	Incident-Verfahrensanweisung		

22. Datenschutzfreundliche Voreinstellungen

X	Es werden nicht mehr personenbezogene Daten	X	Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

	erhoben, als für den jeweiligen Zweck erforderlich sind		

23. Auftragskontrolle (Outsourcing an Dritte)

X	Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation	X	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
X	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln	X	Schriftliche Weisung an den Auftragnehmer
X	Verpflichtung der Mitarbeiter des Auftragnehmers auf die Verpflichtung zur Vertraulichkeit	X	Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht

Anhang 2:
Genehmigte Unterauftragnehmer

Die nachfolgenden Unternehmen sind genehmigte Unterauftragnehmer im Sinne der Ziff. 7:

#	Name	Betreibergesellschaft	Anschrift des Unterauftragnehmers	Ort der Datenverarbeitung	Einsatzbereich im Rahmen des Vertrags	Betroffene
1	BuchhaltungsButler	Buchhaltungs Butler GmbH	Ausbau 1, 15910 Unterspreewald	Server in der Europäischen Union	Buchhaltungs Add-ons	Mandanten und Mitarbeiter des Auftraggebers
2	Deutscher Anwaltverlag	Deutscher Anwaltverlag und Institut der Anwaltschaft GmbH	Rochusstr. 2-4, 53123 Bochum	Server in der Europäischen Union	Anwaltgebühren-rechner	Mandanten und Mitarbeiter des Auftraggebers
3	Microsoft Cloud	Microsoft Ireland Operations Ltd.*	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Deutschland	Hosting	Mandanten und Mitarbeiter des Auftraggebers
4	Neberle GmbH	Neberle GmbH	Andreas-Hofer-Str. 20 96049 Bamberg	Deutschland	Onboarding Buchhaltungs Add-ons	Mandanten und Mitarbeiter des Auftraggebers
5	Zoho Analytics	Zoho Corporation GmbH	Trinkausstr. 7 40213 Düsseldorf	Server in der Europäischen Union	Controlling-Add-ons	Mandanten und Mitarbeiter des Auftraggebers

6	Plusserver	PlusServer GmbH	Venloer Straße 47 50672 Köln	Deutschland	Volltextsuche	Mandanten und Mitarbeiter des Auftraggebers
7	e.Consult	e.Consult AG	Neugrabenweg 1 66123 Saarbrücken	Deutschland	Anbindung an e.Consult-Plattform via Add.ons	Mandanten und Mitarbeiter des Auftraggebers
8	Billwerk	Billwerk Germany GmbH	Mainzer Landstraße 51 60329 Frankfurt am Main	Deutschland	Subscription Management und Rechnungsstellung	Mitarbeiter des Auftraggebers
9	Silberfluss	Silberfluss Technologies GmbH	Agnes-Pockels-Bogen 1 80992 München	Deutschland	Mandanten-Portal	Mandanten und Mitarbeiter des Auftraggebers

* Für die USA ist ein Angemessenheitsbeschluss der EU-Kommission vorhanden, das sog. Trans-Atlantic Data Privacy Framework (TADPF). Microsoft hat sich nach dem TADPF zertifiziert und damit verpflichtet, europäische Datenschutzgrundsätze einzuhalten.