Auftragsverarbeitungsvertrag
nach Art. 28 Abs. 3 DSGVO

Die nachstehenden Bestimmungen gelten gegenüber den Kunden (im Folgenden „Auftraggeber“) der CMO Dienstleistungen GmbH, Kaiserstraße 57/1, 72764 Reutlingen (im Folgenden „CMO“ bzw. „Auftragnehmer“) in allen Fällen, in denen die CMO Daten im Auftrag verarbeitet, soweit sich aus dem Angebot der CMO oder dem zugrundeliegenden Hauptvertrag nicht etwas anderes ergibt.

Inhaltsverzeichnis

1. Präambel

Der Auftragnehmer ermöglicht den Zugang zu einem globalen Value-Added-Network (VAN) sowie die Nutzung der über dieses angebotenen Daten und Dienstleistungen. Ferner bietet er Software, Hardware und Dienstleistungen zur Nutzung des Zugangs zum VAN sowie zur Realisierung kundenspezifischer Kommunikations- und Informationslösungen an.

Der Auftragnehmer erbringt gegenüber dem Auftraggeber im Rahmen eines gesonderten, auf Grundlage des Angebots des Auftragnehmers schriftlich oder in elektronischer Form geschlossenen Vertrages sowie in diesen einbezogener Allgemeiner Geschäftsbedingungen (im Folgenden insgesamt als „Hauptvertrag“ bezeichnet) verschiedene Internet-Dienstleistungen (im Folgenden insgesamt als „Leistungen“ bezeichnet).

2. Gegenstand und Dauer

2.1. Der Auftragnehmer verarbeitet im Rahmen der Erbringung der von ihm aufgrund des Hauptvertrages geschuldeten Leistungen personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO.

2.2. Gegenstand und Dauer der Verarbeitung der Daten ergeben sich aus dem Hauptvertrag, soweit sich aus den Bestimmungen dieses Vertrages nicht darüber hinausgehende Verpflichtungen ergeben.

2.3. Dieser Vertrag regelt die Verarbeitung der personenbezogenen Daten, die der Auftragnehmer im Rahmen der Erfüllung des Hauptvertrages für den Auftraggeber verarbeitet („Daten“).

2.4. Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrages.

3. Konkretisierung des Auftragsinhalts

3.1. Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus dem Hauptvertrag.

3.2. Gegenstand der Verarbeitung personenbezogener Daten sind

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- die vom Kunden im System gespeicherten Daten.

3.3. Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen

- Beschäftigte des Kunden sowie
- alle Personen, zu denen der Kunde Daten im System speichert.

3.4. Die vertraglich vereinbarten Leistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Leistungen oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

4. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

4.1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Der Auftragnehmer wird solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterleiten.

4.2. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

4.3. Die Weisungen des Auftraggebers werden anfänglich durch diese Vereinbarung sowie den Hauptvertrag festgelegt. Danach kann der Auftraggeber einzelne Weisungen schriftlich oder in einem dokumentierten elektronischen Format ändern, ergänzen oder ersetzen. In Eilfällen können mündliche Weisungen erteilt werden. Diese sind vom Auftraggeber unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Geht der Inhalt von Weisungen des Auftraggebers über dasjenige hinaus, was der Auftragnehmer dem Auftraggeber nach dem Hauptvertrag schuldet, hat der Auftraggeber die entsprechenden Leistungen dem Auftragnehmer gesondert zu vergüten. Ist eine Weisung nur mit unverhältnismäßig hohem Aufwand umsetzbar, steht dem Auftragnehmer ein Recht zur außerordentlichen Kündigung des Hauptvertrages und dieses Vertrages zu.

4.4. Der Auftraggeber ist berechtigt, sich wie unter Nr. 6 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

4.5. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

4.6. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

5. Pflichten des Auftragnehmers

5.1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); 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 (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

5.2. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

5.3. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen zumindest logisch getrennt gespeichert werden. Der Auftragnehmer hat die Einhaltung seiner Pflichten aus diesem Vertrag mindestens einmal in jedem Kalenderjahr zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

5.4. Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer den Auftraggeber im Rahmen seiner Möglichkeiten zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO). Für hierfür entstehenden Mehraufwand steht dem Auftragnehmer eine zusätzliche Vergütung zu.

5.5. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

5.6. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen. Die vorstehenden Löschungspflichten gelten nicht für Datenkopien,

die in regelmäßig erstellten Sicherungskopien von umfassenden Datenbeständen des Auftragnehmers enthalten sind, deren isolierte Löschung für den Auftragnehmer einen erheblichen Aufwand bedeuten würde und die im Rahmen des vom Auftragnehmer angewandten Sicherungs-Zyklus spätestens nach einem Jahr automatisch gelöscht oder überschrieben werden. Die Wiederherstellung und jede sonstige Nutzung solcher Kopien bis zu ihrer automatischen Löschung bzw. Überschreibung ist nach Vertragsbeendigung unzulässig. Der Auftraggeber kann vom Auftragnehmer auch die sofortige Löschung solcher Sicherungskopien verlangen, wenn der Auftraggeber dem Auftragnehmer die hierdurch verursachten Kosten erstattet; dies umfasst auch eine Aufwandsentschädigung für die Arbeitszeit des vom Auftragnehmer beanspruchten Personals

5.7. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen, soweit der Auftraggeber nicht gesetzlich zur Auftragserteilung verpflichtet ist.

5.8. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – außer aus dringlichen, vom Auftraggeber zu dokumentierenden Gründen – nach Terminvereinbarung zu den üblichen Geschäftszeiten des Auftragnehmers ohne Störung des Betriebsablaufs und nicht häufiger als alle 12 Monate berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der zugehörigen vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Sollte der durch den Auftraggeber beauftragte Dritte in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Für hierfür entstehenden Mehraufwand steht dem Auftragnehmer eine zusätzliche Vergütung zu.

5.9. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

5.10. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

6.1. Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche

Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO.

6.2. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO).

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

7.1. Als Unterauftragsverhältnis im Sinne dieses Vertrages sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Leistungen aus dem Hauptvertrag beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post- und Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software der Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der personenbezogenen Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessen und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

7.2. Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer allgemein gestattet, Art. 28 Abs. 2 DSGVO. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Auftragnehmer muss dafür Sorge tragen, dass er Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.

7.3. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

7.4. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO). Sofern dem Vertrag mit einem

Subunternehmer dessen eigene Vertragsbedingungen zugrunde liegen, müssen diese Vertragsbedingungen entweder vom Auftragnehmer genehmigt oder mindestens das Schutzniveau des vorliegenden Vertrages erreichen. Der Auftraggeber hat das Recht, auf Verlangen Einsicht in die relevanten Vertragsbedingungen zu nehmen.

7.5. Die Weiterleitung von Daten an einen Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

7.6. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

7.7. Die zurzeit für den Auftragnehmer mit der Verarbeitung von personenbezogenen Daten beschäftigten Subunternehmer ergeben sich aus der Tabelle im Anhang 1.

Grundlage der Beauftragung dieser Subunternehmer sind ihre jeweiligen Standardbedingungen (einschließlich ihrer Standard-Maßnahmen zum technischen und organisatorischen Schutz der jeweils verarbeiteten Daten), die auf den o.g. Websites veröffentlicht sind. Mit der Beauftragung dieser Subunternehmer sowie deren jeweiligen Standardbedingungen erklärt sich der Auftraggeber einverstanden.

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

8.1. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

8.2. Das als Anhang beigefügte Datenschutzkonzept des Auftragnehmers stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

8.3. Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO).

8.4. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

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

Nach Vertragsbeendigung hat der Auftragnehmer sämtliche in Besitz des Auftragnehmers sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, zu löschen. Bis zur Vertragsbeendigung kann der Auftraggeber die Daten über die auf Auftragnehmer bereitgestellten Standard-Schnittstellen selbst über das Internet abrufen und bei sich speichern. Der Auftraggeber kann vom Auftragnehmer auch die Bereitstellung der Daten in anderer Form verlangen, wenn der Auftraggeber dem Auftragnehmer die hierdurch verursachten Kosten erstattet; dies umfasst auch eine Aufwandsentschädigung für die Arbeitszeit des vom Auftragnehmer beanspruchten Personals.

10. Verschiedenes

10.1. Für Nebenabreden zu diesem Vertrag ist die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

10.2. Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrages über die Auftragsverarbeitung von personenbezogenen Daten den Regelungen des Hauptvertrages vor.

10.3. Sollten die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

10.4. Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

10.5. Es gilt deutsches Recht unter Ausschluss eventueller Verweisungen auf andere Rechtsordnungen und unter Ausschluss des UN Kaufrechts.

10.6. Soweit sich nicht aus dem Hauptvertrag ein anderer Gerichtsstand ergibt, ist ausschließlicher Gerichtsstand für Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag beim Sitz des Auftragnehmers.

Anhang 1 – Subunternehmer

Subunternehmer des Auftragnehmers

Zurzeit sind für den Auftragnehmer keine Subunternehmer mit der Verarbeitung von personenbezogenen Daten beschäftigt.

Anhang 2 – Technische und organisatorische Maßnahmen

Datenschutzkonzept des Auftragnehmers (technische und organisatorische Maßnahmen)

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Nr.	Begriffsdefinition	Auflistung und kurze Beschreibung der vorhandenen Schutzmaßnahmen
Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)		
1	**Zutrittskontrolle**	
	Kein unbefugter Zutritt zu Datenverarbeitungsanlagen.	• Zugangskontrollsysteme Zutritts-Token und Chipkarten • Protokollierung der Besucher • Schlüssel • Elektrische Türöffner/-schließer • Videoüberwachung
2	**Zugangskontrolle**	
	Keine unbefugte Benutzung von Datenverarbeitungssystemen.	• Authentifikation mit Userkennung + Passwort • Einsatz von Firewalls • Einsatz von Anti-Viren-Software • Passwortvergabe / Passwortregeln
3	**Zugriffskontrolle**	
	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems	• Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte) • Protokollieren und Auswertung von Zugriffen • Änderungen und Löschung.
4	**Trennungskontrolle**	
	Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden	• Mandantenfähigkeit • Getrennte Datenbanken • Zweckbindung • Funktionstrennung (Produktionsumgebung / Testumgebung)

5	**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.	Anonymisierung von IP-Adressen in den Server-Protokollen nach 30 Tagen
Integrität (Art. 32 Abs. 1 lit. b DS-GVO)		
6	**Weitergabekontrolle**	
	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport. Die Maßnahmen müssen insbesondere die Verschlüsselung von Daten auf mobilen Geräten, mobilen Datenspeichern und Wechselmedien (bspw. Laptops, Smartphones, USB Sticks, Bänder) umfassen sowie die Verschlüsselte Übertragung von Daten.	• Transportverschlüsselung (bspw. Virtual Private Networks) • Passwort-Schutz
7	**Eingabekontrolle**	
	Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	• Benutzeridentifikation • Eingabevalidierung • Protokollierung und Überwachung • Auswertung • Dokumentenmanagement

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)		
8	**Verfügbarkeitskontrolle**	
	Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust	• Brandschutzmaßnahmen • Überspannungsschutz • Unterbrechungsfreie Stromversorgung (USV) • Backup-Strategie (online/offline; on-site/off-site), • Backup-Verfahren • Spiegeln von Festplatten (bspw. RAID-Verfahren) • Getrennte Aufbewahrung • Virenschutz • Firewall
9	**Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)**	
	Maßnahmen zur geregelten und zügigen Wiederherstellung von Daten und Services nach einem Vorfall.	• Regelmäßige Backups • Meldewege • Notfallpläne
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)		
10	**Datenschutz-Management**	
	Organisationsstruktur und Prozesse um nachvollziehbaren Schutz von Daten zu ermöglichen.	• Dokumentation der Prozesse im Verarbeitungsverzeichnis
11	**Incident-Response-Management**	
	Prozesse um die rasche und zielgerichtete Behandlung von (Datenschutz-)Vorfällen zu ermöglichen. Dies umfasst insbesondere das Melden von Datenschutzverstößen.	• Verpflichtung aller Mitarbeiter, Datenverstöße unverzüglich an die Geschäftsführung zu melden.
12	**Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)**	
	Technische und organisatorische Maßnahmen um die Datenschutzgrundsätze (gemäß Art. 5 DS-GVO) wirksam umzusetzen.	• Maßnahmen zur Datenminimierung • Anonymisierung / Pseudonymisierung

13	**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.	• Keine Verwendung der Daten zu eigenen Zwecken