

Januar 2023

# Privacy Hub AVV

## Vereinbarung zum Datenschutz bei der Auftragsverarbeitung gemäß Art. 28 DSGVO

### Präambel

Die vorliegende AVV wird geschlossen zwischen Ihnen („Kunde“ bzw. „Auftraggeber“) und der Cookiebox GmbH („Dienstleister“ bzw. „Auftragnehmer“) und ist Bestandteil der AGB.

Der Auftragnehmer verarbeitet im Rahmen abgeschlossener oder abzuschließender Verträge personenbezogene Daten aus dem datenschutzrechtlichen Verantwortungsbereich des Auftraggebers im Sinne des Art. 28 Datenschutzgrundverordnung (DSGVO). Die dem Auftragnehmer vom Auftraggeber überlassenen personenbezogenen Daten unterliegen den Bestimmungen des DSGVO und den sonstigen datenschutzrechtlichen Vorschriften (z. B. BDSG).

Diese Vereinbarung legt die Rahmenbedingungen zur Gewährleistung der Einhaltung der datenschutzrechtlichen Regelungen fest.

### 1. Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Privacy Hub – ein Redaktionssystem zur zentralen Organisation und Umsetzung der DSGVO-Vorgaben auf Websites, Apps und Social Media Accounts. Die Dauer des Auftrags ist unbefristet.

### 2. Konkretisierung des Auftragsinhalts

Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck der Aufgaben des Auftragnehmers:

Hosting der dynamischen Datenschutzerklärung (“Website DSE”)

Hosting der Informationen für Betroffene gem. Art. 13 / 14 DSGVO  
("Datenschutzinformationen DSI")

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

## Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Planungs- und Steuerungsdaten
- IP-Adressen

## Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Websitebesucher
- Kunden
- Interessenten
- Lieferanten
- Handelsvertreter
- Ansprechpartner

## 3. Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in Anlage 1].

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

## 4. Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## 5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Frau Martina Brinkmann benannt; Kontaktdaten siehe: <https://www.cookiebox.pro/datenschutzerklaerung/>
2. Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
3. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1].
4. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
5. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies

gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

6. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
7. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
8. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

## 6. Unterauftragsverhältnisse

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. 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.

Die Liste der aktuellen Sub-Dienstleister kann beim Auftragnehmer eingeholt werden; senden Sie dafür einfach eine E-Mail an [post@cookiebox.pro](mailto:post@cookiebox.pro). Mit Buchung der Leistung gilt die Genehmigung der Sub-Dienstleister als erteilt. Ist der Auftraggeber aus wichtigem Grund mit der Weitergabe der Daten an einen bestimmten Sub-Dienstleister nicht einverstanden, können beide Seiten von ihrem Sonderkündigungsrecht Gebrauch machen.

Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und deren erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU / des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

Eine weitere Auslagerung durch den Unterauftragnehmer ist grundsätzlich gestattet; sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## 7. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz).

Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

## 8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

1. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
2. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;

3. die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
4. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung und
5. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

## 9. Weisungsbefugnis des Auftraggebers

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstöße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## 10. Löschung von Daten und Rückgabe von Datenträgern

Kopien oder Duplikate der Daten 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.

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, 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. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

# 11. Laufzeit und Kündigung

Diese Vereinbarung tritt mit Vertragsabschluss in Kraft und behält Gültigkeit, solange das betreffende Dienstleistungsverhältnis andauert.

## Anlage 1:

- I. Technisch-organisatorische Maßnahmen des Auftragnehmers
- II. Technisch-organisatorische Maßnahmen des Sub-Dienstleisters

## I. Technisch-organisatorische Maßnahmen des Auftragnehmers

### 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle - Kein unbefugter Zutritt zu Datenverarbeitungsanlagen
  - Schlüssel
- Zugangskontrolle - Keine unbefugte Systembenutzung
  - (sichere) Kennwörter
  - automatische Sperrmechanismen
- Zugriffskontrolle - Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems
  - Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
  - Protokollierung von Zugriffen
- Trennungskontrolle - Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden
  - Mandantenfähigkeit
  - Sandboxing
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) - 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 DSGVO)

- Weitergabekontrolle - Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport
  - Verschlüsselung
- Eingabekontrolle - Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind
  - Protokollierung

### 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle - Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust
  - Backup-Strategie (online/offline; on-site/off-site)
  - Virenschutz
  - Firewall
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

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

- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- Auftragskontrolle - Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers
  - Eindeutige Vertragsgestaltung
  - formalisiertes Auftragsmanagement
  - strenge Auswahl des Dienstleisters
  - Vorabüberzeugungspflicht
  - Nachkontrollen

## II. Technisch-organisatorische Maßnahmen des Sub-Dienstleisters

V1.0 vom 01.01.2023

### Präambel

Der Sub-Dienstleister vermietet die Datenverarbeitungsanlage an den Auftraggeber. Dies beinhaltet die Vermietung von Hard- und Software, sowie die Bereitstellung von Anbindungen an das Internet sowie weitere Dienste entsprechend der jeweiligen Vereinbarung. Der Auftraggeber entscheidet allein und ausschließlich darüber, welche personenbezogene Daten in welcher Weise verarbeitet werden. Die hierfür erforderlichen Programme zur Datenverarbeitung werden durch den Auftraggeber erstellt und eingesetzt. Der Sub-Dienstleister sorgt für die technische Einsatzbereitschaft des Systems entsprechend den vertraglichen Vereinbarungen und führt Buch darüber, welche Anlagen durch den Auftraggeber in welchem Umfang genutzt werden. Die Datenverarbeitung erfolgt durch den Auftraggeber. Der Sub-Unternehmer hat keinerlei Einfluss auf die durch den Auftraggeber durchgeführten Datenverarbeitungsvorgänge.

## Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

### Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen in den Rechenzentren

#### 1. Zutrittskontrollsystem

Ein Schließsystem in Form einer mindestens 1-Faktor-Authentifizierung (z.B. Transponder, Chipkarte, Klingelsystem mit Personenkontrolle per Bild und Ton) ermöglicht den Zutritt zu Datenverarbeitungsanlagen erst nach positiver Zutrittsprüfung.

#### 2. Schlüsselregelung

Schlüsselausgaben an Personen zum Zutritt zu Datenverarbeitungsanlagen werden dokumentiert.

#### 3. Protokollierung der Besucher

Besucher, die Zutritt zu Datenverarbeitungsanlagen erhalten (z.B. im Falle von Hardware-Austausch durch den Hersteller) werden in einem Besucherbuch erfasst.

#### 4. Einbruchmeldeanlage

Der Zutritt zu Datenverarbeitungsanlagen ist per Einbruchmeldeanlage abgesichert.

#### 5. Videoüberwachung

Datenverarbeitungsanlagen werden per Videoüberwachung gesichert.

### Zugangskontrolle

Keine unbefugte Systembenutzung

#### 1. Passwortvergabe

Ein Zugang zu den Datenverarbeitungssystemen ist grundsätzlich nur mittels einer Kombination aus einem Benutzernamen und dem zugeordneten Passwort möglich.

#### 2. Passwortsrichtlinie

Passwörter für Datenverarbeitungsanlagen müssen Mindest-Komplexitätsanforderungen der unternehmensweiten Richtlinie entsprechen; Passwörter von Mitarbeitern müssen regelmäßig geändert werden.

#### 3. Administrativer Zugriff

Sämtliche Datenverarbeitungssysteme sind zu Wartungszwecken ausschließlich über freigegebene IP-Adressbereiche und verschlüsselt erreichbar (z.B. VPN- Beschränkungen).

#### 4. Firewall

Schutz der Infrastruktur durch Firewalls (Soft- und/oder Hardware), Beschränkungen ungenutzter Ports sowie Benutzername und Passwort vor unberechtigten Zugriffen

geschützt. Systeme, die Hauptvertragsleistungen bereitstellen, werden, entsprechend der jeweiligen Vereinbarung im Hauptvertrag, mit einer Firewall ausgestattet.

#### 5. Einsatz von Anti-Viren-Software

Systeme, die zum Zugriff auf Datenverarbeitungssysteme genutzt werden, sind mit einer Anti-Viren-Software ausgestattet. Diese Software wird regelmäßig auf die neuesten Virus-Definitionen aktualisiert. Systeme, die Kundenleistungen bereitstellen, werden, entsprechend der jeweiligen Vereinbarung im Hauptvertrag, mit einer Anti-Viren-Software ausgestattet.

#### 6. Verschlüsselung von mobilen Datenträgern

Sofern mobile Datenträger oder mobile Geräte zum Einsatz kommen, werden die Inhalte verschlüsselt.

## Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

#### 1. Zuordnung von Benutzerrechten

Der Zugriff auf Datenverarbeitungssysteme wird für Personen auf die jeweils mindestens notwendigen Daten durch Vergabe entsprechender Benutzerrechte eingeschränkt. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

#### 2. Sichere Aufbewahrung von Datenträgern

Datenträger, die personenbezogene Daten enthalten, werden verschlossen gelagert

#### 3. Verwaltung der Rechte durch einen eingeschränkten Personenkreis

Ausschließlich berechtigte Systemadministratoren sind in der Lage, Rechte anderer Personen zu Datenverarbeitungssystem zu verwalten. Der Kreis der berechtigten Systemadministratoren wird auf die kleinstmögliche Auswahl von Personen reduziert. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

#### 4. Protokollierung der Zugriffe

Zugriffe auf Dienste (z. B. Webdienste) werden DSGVO-konform in Log-Files protokolliert. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat jedoch keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

#### 5. Ordnungsgemäße Vernichtung von Datenträgern

Datenträger, die personenbezogene Daten enthalten werden gemäß DIN 66399 vernichtet.

#### 6. Regelmäßige Wartung der Datenverarbeitungssysteme

## Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

### 1. Festlegung von Datenbankrechten

Der Zugriff von Systemen und Benutzern auf Datenbanken wird auf die jeweils notwendigen Daten eingeschränkt.

### 2. Trennung von Produktiv- und Testsystemen

Produktiv- und Testumgebungen werden isoliert voneinander betrieben. Ein Zugriff einer Umgebung auf Daten der jeweils anderen Umgebung wird durch den Einsatz von z.B. getrennten Datenbanksystemen und Serversystemen unterbunden.

### 3. Logische Mandantentrennung

Durch den Einsatz unterschiedlicher softwareseitiger Mechanismen wird eine Trennung der Daten von Mandanten gewährleistet.

## Integrität (Art. 32 Abs. 1 lit. b DSGVO)

### 1. Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

### 2. Transport

Sofern personenbezogene Daten weitergegeben werden, findet dies grundsätzlich verschlüsselt statt. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

### 3. Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

### 4. Zuordnung von Benutzerrechten

Der Zugriff auf Datenverarbeitungssysteme wird für Personen auf die jeweils mindestens notwendigen Daten durch Vergabe entsprechender Benutzerrechte eingeschränkt.

### 5. Protokollierung von Dateneingaben

Die Datenverarbeitung erfolgt durch den Kunden, Seitens des Auftragnehmers besteht kein Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme. Die Eingabekontrolle der Daten kann daher ausschließlich durch den Kunden umgesetzt werden.

### 6. Nachvollziehbarkeit der Eingabe

Die Datenverarbeitung erfolgt durch den Kunden. Seitens des Auftragnehmers besteht kein Einfluss auf die durch den Kunden verwendeten Datenverarbeitungsprogramme. Die

Eingabekontrolle kann daher ausschließlich durch den Kunden umgesetzt werden. Bei Änderungen durch den Auftragnehmer werden die Administrationszugriffe adäquat protokolliert.

## Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

### Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

#### 1. Unterbrechungsfreie Stromversorgung in Serverräumen (Rechenzentren)

Serverräume sind durch unterbrechungsfreie Stromversorgungen geschützt. Der Schutz ist zweistufig aufgebaut. Bei Bedarf wird ein Notstrom-Aggregat automatisch aktiviert, das die Stromversorgung der Serverräume übernimmt.

#### 2. Klimaanlage in Serverräumen (Rechenzentren)

Eine für den Betrieb von Serversystemen angemessene Temperatur und Luftfeuchtigkeit wird in Serverräumen durch ausreichend dimensionierte Klimaanlage gewährleistet.

#### 3. Feuer- und Rauchmeldeanlagen in Serverräumen (Rechenzentren)

Durch den Einsatz von Feuer- und Rauchmeldeanlagen wird ein Brand frühzeitig erkannt. Feuerlöschanlagen löschen auftretende Brände.

#### 4. Datensicherungskonzept und Aufbewahrung von Datensicherungen

Datensicherungen von personenbezogenen Daten werden nur nach Vereinbarung bzw. gemäß des abgeschlossenen Hauptvertrages angefertigt und auf separaten und für Datensicherungen dediziert eingesetzten Systemen aufbewahrt.

#### 5. Monitoring

Systemkritische Instanzen werden durch Monitoring überwacht. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

## Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

### Datenschutz-Management

Der Auftragnehmer etabliert ein Datenschutzmanagement, das den Schutz der personenbezogenen Daten sicherstellt.

## Incident-Response-Management

Regelmäßige Überprüfung der IT-Infrastruktur. Der Auftragnehmer etabliert einen Vorfalldaktionsplan.

## Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Der Auftragnehmer stellt innerhalb seiner Möglichkeiten sicher, dass durch Voreinstellung nur Daten, die für den jeweiligen bestimmten Verarbeitungszweck unbedingt erforderlich sind, verarbeitet werden. Die Datenverarbeitung selbst erfolgt durch den Kunden. Der Auftragnehmer hat keinerlei Einfluss auf die durch den Kunden durchgeführten Datenverarbeitungsvorgänge.

## Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers

### 1. Auswahl von geeigneten Auftragnehmern

Bei der Auswahl von Auftragnehmern, die personenbezogene Daten im Auftrag verarbeiten, werden nur solche Auftragnehmer ausgewählt, die mindestens die gesetzlich vorgeschriebenen Anforderungen an die Verarbeitung von personenbezogenen Daten einhalten

### 2. Überwachung der Auftragnehmer

Der Auftragnehmer wird regelmäßig auf die Einhaltung der zugesicherten technischen und organisatorischen Maßnahmen bei der Verarbeitung von personenbezogenen Daten überprüft.