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:

- Je nach Leistungsangebot gebuchte Dienstleistung zu dem über Usercentrics bereitgestellten Consent Management System (CMP)
- Bereitstellung des CMP erfolgt ausschließlich über den Hersteller Usercentrics, der in diesem Verhältnis als genehmigter

Sub-Dienstleister in Erscheinung tritt (siehe auch Abschnitt *Unterauftragnehmer*)

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:

- Durch Cookiebox: Analyse, Einrichtung, Wartung und / oder Pflege des Backends, der Banner und ggfs. weiterer Einstellungen für das Usercentrics CMP.
- Durch Usercentrics: Erhebung, Verwaltung, Dokumentation und Weitergabe der Einwilligung der Nutzer des Auftraggebers sowie ggf. sonstige Services.

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 Artt. 44 ff. DSGVO erfüllt sind.

ART DER DATEN

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

Durch Cookiebox:

- Planungs- und Steuerungsdaten
- E-Mail-Adressen der Backend-User

- ggfs. Daten im Rahmen der Einrichtung von Tracking-Services (z. B. im Google Tag Manager)
- Ein Zugriff auf weitere personenbezogene Daten ist bei der Durchführung der Dienstleistung im Backend in der Regel nicht gegeben, aber auch nicht ausgeschlossen

Durch Usercentrics:

- IP-Adresse,
- User Agent,
- ControllerID, ProcessorID, ConsentID, und
- Timestamp

KATEGORIEN BETROFFENER PERSONEN

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Websitebesucher
- Kunden
- Backend-User

3. TECHNISCH-ORGANISATORISCHE MASSNAHME

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://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 *neben Usercentrics* aktuell eingesetzten Sub-Dienstleister kann beim Auftragnehmer eingeholt werden; senden Sie dafür einfach eine E-Mail an 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 dessen 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 AUFTRAGNEHMER

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 verstoße 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 (COOKIEBOX

II. TECHNISCH–ORGANISATORISCHE MASSNAHMEN/SICHERHEITSKONZEPT DES SUB-DIENSTLEISTERS (USERCENTRICS

I. TECHNISCH-ORGANISATORISCHE MASSNAHMEN DES AUFTRAGNEHMERS (COOKIEBOX

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/SICHERHEITSKONZEPT DES SUB-DIENSTLEISTERS (USERCENTRICS

INHALTSVERZEICHNIS

4. Maßnahmen zur Gewährleistung der Verfügbarkeit
5. Gewährleistung der Belastbarkeit der Systeme
6. Maßnahmen zur Wiederherstellung der Verfügbarkeit
7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. MASSNAHMEN ZUR PSEUDONYMISIERUNG VON PERSONENBEZOGENEN DATE

Pseudonymisierung ist die Verarbeitung von personenbezogenen Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifisch betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und sie technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

MASSNAHMEN IN ZUSAMMENHANG MIT DER PSEUDONYMISIERUNG PERSONENBEZOGENER DATEN SIND

- Privacy-by-design
- Alle IDs eines Nutzers (consentID, processorID, consentID) werden mit einem sha-256 kryptografischen Hash pseudonymisiert
- Es liegt ein Pseudonymisierungskonzept vor (u.a. Definition der zu ersetzenden Daten; Pseudonymisierungsregeln, Beschreibung Vorgehensweise, etc.)

2. GEWÄHRLEISTUNG DER VERTRAULICHKEIT

Maßnahmen zur Umsetzung des Gebots der Vertraulichkeit sind unter anderem Maßnahmen zur Zutritts-, Zugriffs- oder Zugangskontrolle. Die in diesem Zusammenhang getroffenen technischen und organisatorischen

Maßnahmen sollen eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

MASSNAHMEN, DIE DIE USERCENTRICS GMBH UMGESETZT HAT, DIE EINEN ZUGANG DURCH UNBEFUGTE AUF DATENVERARBEITUNGSSYSTEME VERHINDERN

- Persönlicher und individueller User-Login bei Anmeldung im System (Google Cloud)
- Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
- Zusätzlicher System-Login für bestimmte Anwendungen
- Automatische Sperrung der Clients nach gewissen Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
- Elektronische Dokumentation sämtlicher Passwörter und Verschlüsselung dieser Dokumentation zum Schutz vor unbefugten Zugriff
- Zwei-Faktor-Authentifizierung
- Regelmäßige Softwareaktualisierung
- Regelmäßige Schwachstellenscans

Die Server werden bei Google Cloud in Frankfurt, Deutschland gehostet. Dieser Hoster gewährleistet Ausfallsicherheit und Schutz vor unberechtigtem Zugriff auf die physische Infrastruktur.

Maßnahmen, die der Subunternehmer Google Cloud umgesetzt hat, können hier eingesehen werden:
https://cloud.google.com/terms/data-processing-terms
#appendix-2-security-measures

3. GEWÄHRLEISTUNG DER INTEGRITÄT

Maßnahmen zur Umsetzung des Gebots der Integrität sind zum einen solche, die auch zur

Eingabekontrolle gehören, zum anderen aber solche, die generell zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Zerstörung oder unbeabsichtigter Schädigung beitragen.

3.1 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:

- Verschlüsselung von E-Mail
- Verschlüsselung von CD/DVD-ROM, externen Festplatten und/ oder Laptops
- Gesichertes WLAN
- SSL-/TLS-Verschlüsselung
- Datenschutzkonforme Vernichtung von Daten, Datenträgern und Ausdrucken
- Protokollierung der Datenweitergabe

3.2 EINGABEKONTROLLE

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob, zu welcher Zeit und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind:

- Gesetzeskonforme Vertragsgestaltung von Verträgen über die Datenverarbeitung personenbezogener Daten mit Subunternehmern mit entsprechender Regelung von Kontrollmechanismen

- Einholung von Selbstauskünften bei Dienstleistern bezüglich deren Maßnahmen zur Umsetzung datenschutzrechtlicher Anforderungen
- Schriftliche Bestätigung von mündlichen Weisungen
- Aufzeichnung und bedarfsgerechtes Vorhalten von entsprechenden, an Systemen durchgeführten Aktionen (z. B. Logfiles)
- Einsatz von Protokollierungs- und Protokollauswertungssysteme
- Festlegung der Befugten für die Erstellung von Datenträgern und der Bearbeitung von Daten

4. GEWÄHRLEISTUNG DER VERFÜGBARKEIT

Der Unterverarbeiter Google Cloud gewährleistet eine Verfügbarkeit von 99,99% im Jahresmittel. Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Einsatz zentral geprüfter und freigegebener Standardsoftware aus sicheren Quellen
- Regelmäßige Durchführung von Datensicherungen bzw. Einsatz von Spiegelungsverfahren
- Außerbetriebnahme von Hardware (insbesondere von Servern) erfolgt nach einer Überprüfung der darin eingesetzten Datenträger und ggf. nach erfolgter Sicherung der relevanten Datensätzen
- Unterbrechungsfreie Stromversorgung (USV) im Serverraum
- Getrennte Aufbewahrung von Datenbeständen, die zu unterschiedlichen Zwecken erhoben wurden
- Mehrschichtige Virenschutz- und Firewall-Architektur
- Notfallplanung (Notfallplan für Sicherheits- und Datenschutzverletzungen mit konkreten Handlungsanweisungen)
- Feuer-/Wasser- und Temperaturfrühwarnsystem in den Serverräumen
- Brandschutztüren

5. GEWÄHRLEISTUNG DER BELASTBARKEIT DER SYSTEME

Hierzu gehören Maßnahmen, die schon in der Phase vor Durchführung der Datenverarbeitung durch den Auftragsverarbeiter zu ergreifen sind. Darüber hinaus ist auch eine kontinuierliche Überwachung der Systeme erforderlich und vorgesehen. Der Unterverarbeiter Google Cloud hat gewährleistet die Belastbarkeit seiner Systeme durch folgende Maßnahmen:

- Load-Balancing
- Dynamische Prozesse und Speicherzuschaltung
- Penetrationstests
- Regelmäßige Belastungstests der Datenverarbeitungssysteme
- Belastungsgrenze für das jeweilige
- Datenverarbeitungssystem im Voraus über das notwendige Minimum ansetzen
- Regelmäßige Schulung des eingesetzten Personals entsprechend dem Gebot zur Sicherstellung der Integrität und Vertraulichkeit der Datenverarbeitung zu handeln

Näheres zu den Verfahren kann hier eingesehen werden:
https://cloud.google.com/security/overview/

6. VERFAHREN ZUR WIEDERHERSTELLUNG DER VERFÜGBARKEIT PERSONENBEZOGENER DATEN NACH EINEM PHYSISCHEN ODER TECHNISCHEN ZWISCHENFALL

Zur Sicherstellung der Wiederherstellbarkeit sind einerseits ausreichende Sicherungen erforderlich, wie aber auch Maßnahmenpläne, die im Sinne von Katastrophen-Fall-Szenarien den laufenden Betrieb wiederherstellen können. Der Unterverarbeiter Google Cloud hat ein ein mehrstufiges Sicherungssystem eingerichtet, darunter Maßnahmen wie:

- Tägliches Backup des gesamten Servers durch den Hoster
- Service Level Agreements (SLAs) mit Dienstleistern
- Backup Verfahren
- Redundanz (z.B. Spiegeln von Festplatten)

- Firewall, IDS/IPS
- Brandschutz und Löschwasserschutz
- Monitoring von Alarmen
- Pläne für Ausfall, Notfall und Wiederherstellung

Näheres zu den Verfahren kann hier eingesehen werden:
https://cloud.google.com/security/overview/

7. VERFAHREN REGELMÄSSIGER ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG DER WIRKSAMKEIT DER TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN

Eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung erfolgt im Rahmen der Durchführung von:

- regelmäßige Revisionen des Sicherheitskonzepts
- Informationen über neu auftretende Schwachstellen und andere Risikofaktoren, ggf. Überarbeitung der Risikoanalyse und -bewertung
- Prüfungen des Datenschutzbeauftragten und des, Informationssicherheitsbeauftragten, Prozesskontrollen durch Qualitätsmanagement