WE BELIEVE
PRIVACY
SHOULD
MATTER
TO OUR CLIENTS

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

Usercentrics Vertrag – Auftragsverarbeitungsvereinbarung (Anlage 1 zum Angebot)

Vereinbarung zwischen dem

Vertragspartner

…

…

(im Folgenden **„Auftraggeber“**)

und der

Usercentrics GmbH

Sendlinger Str. 7

80331 München

(im Folgenden **„Auftragnehmer“)**

über die Verarbeitung von personenbezogenen Daten im Auftrag (**„Vereinbarung“**). Definitionen in den AGB oder der Leistungsbeschreibung gelten auch in dieser Auftragsverarbeitungsvereinbarung. Definitionen in dieser Auftragsverarbeitungsvereinbarung gelten nur für diese Auftragsverarbeitungsvereinbarung.

1. Gegenstand und Dauer des Auftrags

1.1. Gegenstand des Auftrags

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer entsprechend der Leistungsbeschreibung im Angebot: Erhebung, Verwaltung, Dokumentation und Weitergabe der Einwilligung der Nutzer des Auftraggebers sowie ggf. sonstige Services. Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage der AGB.

1.2. Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Vertrages.

2. Konkretisierung des Auftragsinhalts

2.1. Umfang, Art und Zweck

Umfang, Art und Zweck der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsbeschreibung im Angebot.

2.2. Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Daten:

- Kundendaten: Settings Login Daten
- Userdaten:

- Consent Daten (Consent ID, Consent Nummer, Uhrzeit des Consents, implizit o. expliziter Consent, Opt-in o. Opt-out, Banner Sprache, Kunden Setting, Template Version)
- Device Daten (HTTP Agent, HTTP Referrer)

2.3. **Kreis der Betroffenen**

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst:

- Webseitenbesucher oder App-Nutzer,
- Kunden / Registrierte User

3. Weisungsbefugnis des Auftraggebers / Ort der Datenverarbeitung

3.1. Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers (vgl. Art. 28 Abs. 3 lit. a DSGVO). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Entstehende Zusatzaufwände sind vom Auftraggeber auf Time- und Material-Basis zu vergüten. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

3.2. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Verpflichtungen nach Unionsrecht oder dem Recht eines EU-Mitgliedstaats, sowie zur Einhaltung von Aufbewahrungspflichten erforderlich sind.

3.3. Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend Art. 28 Abs. 3 Uabs. 2 DSGVO zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

3.4. Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer findet innerhalb der EU / des EWR statt. Der Auftragnehmer ist verpflichtet, den Auftraggeber vor Aufnahme der Verarbeitung auf eine gesetzliche Verpflichtung des Auftragnehmers hinzuweisen, die Verarbeitung der Auftraggeberdaten an einem anderen Ort durchzuführen, sofern eine solche Mitteilung nicht gesetzlich untersagt ist. Die Verarbeitung und / oder Verbringung in ein Drittland außerhalb des Gebietes der EU / EWR oder an eine internationale Organisation bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. In diesem Fall ist der Auftragnehmer zudem verpflichtet, entsprechend den gesetzlich anwendbaren Vorgaben sowie gerichtlichen und behördlichen Auslegungen derselben für ein angemessenes Datenschutzniveau am Ort der Datenverarbeitung zu sorgen oder – nach Wahl des Auftraggebers – dem Auftraggeber die Möglichkeit einzuräumen, für ein angemessenen Datenschutzniveau zu sorgen, unter anderem durch den Abschluss von oder dem Beitritt zu EU-Standardvertragsklauseln.

4. Vertraulichkeit

Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung von personenbezogenen Daten befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die personenbezogenen Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- / Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

5. Technisch-organisatorische Maßnahmen

5.1. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird angemessene technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten des Auftraggebers treffen, die den Anforderungen des Art. 32 DSGVO genügen. Insbesondere sind die technischen und organisatorischen Maßnahmen dergestalt zu treffen, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Datenverarbeitung auf Dauer sichergestellt sind. Diese technischen und organisatorischen Maßnahmen sind in Anhang 1 dieser Vereinbarung beschrieben. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

5.2. 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.

6. Unterauftragsverhältnisse

6.1. Die Einschaltung und/oder Änderung von Unterauftragnehmern durch den Auftragnehmer ist grundsätzlich nur mit Zustimmung des Auftraggebers gestattet. Der Auftraggeber stimmt dem Einsatz von Unterauftragnehmern wie folgt zu:

6.1.1. Der Auftraggeber stimmt dem Einsatz der in Anhang 2 dieser Vereinbarung aufgeführten Unterauftragnehmer bereits jetzt zu.

6.1.2. Der Auftraggeber stimmt dem Einsatz bzw. der Änderung weiterer Unterauftragnehmer zu, wenn der Auftragnehmer den Einsatz bzw. die Änderung dreißig (30) Tage vor Beginn der Datenverarbeitung schriftlich (E-Mail ausreichend) dem Auftraggeber mitteilt. Der Auftraggeber kann dem Einsatz eines neuen Unterauftragnehmers bzw. der Änderung widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zum Einsatz oder zur Änderung als gegeben. Der Auftraggeber nimmt zur Kenntnis, dass in bestimmten Fällen die Leistung ohne den Einsatz eines bestimmten Unterauftragnehmers nicht mehr erbracht werden kann. In diesen Fällen ist jede Partei zur Kündigung ohne die Einhaltung einer Frist berechtigt. Liegt ein wichtiger datenschutzrechtlicher Grund für den Widerspruch vor und ist eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt. Der Auftraggeber hat seine Absicht zur Kündigung innerhalb von einer Woche nach Scheitern der einvernehmlichen Lösung schriftlich gegenüber dem Auftragnehmer zu erklären. Der Auftragnehmer kann innerhalb von zwei Wochen nach Zugang der Absichtserklärung dem Widerspruch abhelfen. Wird dem Widerspruch nicht abgeholfen, kann der Auftraggeber die Sonderkündigung erklären, die mit Zugang wirksam wird.

6.2. Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer/n so zu gestalten, dass sie dieselben Datenschutzpflichten wie in diesem Auftrag vereinbart enthalten, unter Berücksichtigung der Art und des Umfangs der Datenverarbeitung im Rahmen des Unterauftrags. Die Verpflichtung des Unterauftragsverarbeiters muss schriftlich erfolgen bzw. im elektronischen Format.

6.3. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

7. Betroffenenrechte

7.1. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen nach Kapitel III der DSGVO.

7.2. Der Auftragnehmer hat nur nach Weisung des Auftraggebers über die Daten, die im Auftrag verarbeitet werden, Auskunft zu geben, diese Daten zu berichtigen, zu löschen oder die Datenverarbeitung entsprechend einzuschränken. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Auskunft, Berichtigung oder Löschung seiner / ihrer Daten sowie hinsichtlich der Einschränkung der Datenverarbeitung wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

8. Mitwirkungspflichten des Auftragnehmers

8.1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen.

8.2. Im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO gilt Folgendes: Der Auftragnehmer ist verpflichtet, den Auftraggeber (i) über die Verletzung des Schutzes personenbezogener Daten unverzüglich zu informieren und (ii) bei einer solchen Verletzung erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO (Meldungen und Benachrichtigungen bei Verletzung des Schutzes personenbezogener Daten) für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziffer 3 dieser Vereinbarung durchführen.

8.3. Soweit der Auftraggeber im Falle eines Sicherheitsvorfalles Benachrichtigungs- oder Mitteilungspflichten hat, verpflichtet sich der Auftragnehmer, den Auftraggeber auf dessen Kosten zu unterstützen.

9. Sonstige Pflichten des Auftragnehmers

9.1. Soweit gesetzlich vorgeschrieben bestellt der Auftragnehmer einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO, §§ 38, 6 BDSG neu ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme auf Anfrage mitgeteilt.

9.2. Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach Art. 58 DSGVO unterrichten. Dies gilt auch, soweit eine zuständige Behörde nach Art. 83 DSGVO beim Auftragnehmer ermittelt.

9.3. Der Auftragnehmer wird die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. –erfüllung sicherstellen, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

10. Informations- und Überprüfungsrecht des Auftraggebers

10.1. Der Auftraggeber hat das Recht, die nach Art. 28 Abs. 3 h) DSGVO erforderlichen Informationen zum Nachweis der Einhaltung der vereinbarten Pflichten des Auftragnehmers anzufordern und Überprüfungen im Einvernehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen.

10.2. Die Parteien vereinbaren, dass der Auftragnehmer zum Nachweis der Einhaltung seiner Pflichten und Umsetzung der technischen und organisatorischen Maßnahmen berechtigt ist, dem Auftraggeber aussagekräftige Dokumentationen vorzulegen. Eine aussagekräftige Dokumentation kann durch die Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter), einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001) oder einer durch die zuständigen Aufsichtsbehörden genehmigten Zertifizierung erbracht werden.

10.3. Das Recht des Auftraggebers Vor-Ort-Kontrollen durchzuführen, wird hierdurch nicht beeinträchtigt. Der Auftraggeber wird jedoch abwägen, ob nach Vorlage von aussagekräftiger Dokumentation eine Vor-Ort-Kontrolle noch erforderlich ist, insbesondere unter Berücksichtigung der Aufrechterhaltung des ordnungsgemäßen Betriebs des Auftragnehmers.

10.4. Der Auftraggeber 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 verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

11. Löschung von Daten und Rückgabe von Datenträgern

Nach Wahl und Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Vertrags – hat der Auftragnehmer sämtliche in seinen Besitz gelangte 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.

12. Haftung

Die Haftung der Parteien aus dieser Vereinbarung richtet sich im Innenverhältnis nach den Haftungsregelungen in den AGB des Auftragnehmers, soweit sich nicht aus der Leistungsbeschreibung im Angebot oder einer gesonderten Vereinbarung der Parteien etwas anderes ergibt. Für die Haftung im Außenverhältnis gelten die gesetzlichen Bestimmungen nach Art. 82 DSGVO.

Ort, Datum	Ort, Datum
Unterschrift des Auftraggebers	**Usercentrics GmbH**
	Mischa Rürup, Geschäftsführer

Anlage 1 - Technisch–organisatorische Maßnahmen/Sicherheitskonzept der Usercentrics GmbH

Inhaltsverzeichnis

Folgende technische und organisatorische Maßnahmen sind vom Auftragnehmer umgesetzt und mit dem Auftraggeber vereinbart.

1. Maßnahmen zur Pseudonymisierung von personenbezogenen Daten

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

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.

Anhang 2 zur Auftragsverarbeitungsvereinbarung

Genehmigte Unterauftragnehmer

#	Name	Betreibergesellschaft	Anschrift des Unterauftragnehmers	Ort der Datenverarbeitung	Einsatzbereich im Rahmen des Vertrags	Betroffene
1	Google	Google Ireland Limited *	Gordon House, Barrow Street Dublin 4. Irland	Server in der Europäischen Union	Hosting	User des Auftraggebers
1	Auth0	Auth0 Inc.*	10800 NE 8th Street, Suite 700, Bellevue, WA 98004, United States of America	Server in der Europäischen Union	Login Authentifizierung	Auftraggeber

* im Übrigen gelten hier für einen etwaigen Datentransfer in die USA aufgrund der Entscheidung des EuGH vom 16.07.2020 (EuGH, 16.7.2020 – C-311/18 “Schrems II”) die Standardvertragsklauseln zwischen Usercentrics und der Google Ireland Ltd. (abrufbar unter https://cloud.google.com/terms/eu-model-contract-clause) sowie Auth0 (abrufbar unter https://cdn.auth0.com/website/legal/files/dpa/data-processing-addendum-8-20.pdf?_ga=2.176298087.393185399.1600347978-2067480355.1593507683) zur Gewährleistung eines angemessen Datenschutzniveaus (siehe 3.4. der Vereinbarung).