WE BELIEVE
PRIVACY
SHOULD
MATTER
TO OUR CLIENTS

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG

usercentrics

Usercentrics Vertrag – Auftragsverarbeitungsvereinbarung

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“**).

1. Gegenstand und Dauer des Auftrags

1.1. Gegenstand des Auftrags

Gegenstand des Auftrags zur Datenverarbeitung ist die Durchführung folgender Aufgaben durch den Auftragnehmer entsprechend der Leistungsbeschreibung im Angebot ("**Hauptvertrag**"): Erhebung, Verwaltung, Dokumentation und Weitergabe einer zu erteilenden Einwilligung oder auf Basis berechtigter Interessen erhobener personenbezogener Daten der Nutzer des Auftraggebers über die vom Auftragnehmer bereitgestellte Technologie sowie ggf. sonstige Services die mit dem Auftraggeber gemäß Hauptvertrag vereinbart worden sind. Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage des Hauptvertrags. Definitionen im Hauptvertrag gelten auch in dieser Vereinbarung. Definitionen in dieser Vereinbarung gelten nur für diese Vereinbarung.

1.2. Dauer des Auftrags

Die Dauer dieser Vereinbarung (Laufzeit) entspricht der Laufzeit des Hauptvertrages.

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 ergeben sich aus dem Hauptvertrag sowie aus Anlage 3, wobei Anlage 3 im Konfliktfall vorrangig ist.

2.2. Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Daten (gemeinsam auch "**Auftraggeberdaten**"):

- Userdaten:
  - Consent Daten (Consent ID, Consent Nummer, Uhrzeit der Abgabe Consents, Opt-in o. Opt-out, Banner Sprache, Kunden Setting, Template Version)
  - Device Daten (HTTP Agent, HTTP Referrer)

- IP-Adresse

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). Anlage 3, der Hauptvertrag, diese Vereinbarung sowie ggf. die vom Auftraggeber vorgenommenen Einstellungen für die Nutzung des Produkts des Auftragnehmers stellen die Weisungen des Auftraggebers dar. 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, veröffentlicht von der EU Kommission am 4.6.2021, abrufbar hier sowie zusätzlicher Maßnahmen, soweit dies erforderlich ist.

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 Anlage 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 Anlage 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. Die durch den Auftragnehmer bereitgestellte Consent Management Platform (CMP) dient als automatisiertes System dazu, eine Einwilligung der Nutzer des Auftraggebers ("Endnutzer") einzuholen bzw. die für eine Datenverarbeitung auf Basis der berechtigten Interessen des Auftraggebers erforderlichen Maßnahmen umzusetzen und zu dokumentieren. Im Rahmen der CMP können Endnutzer dementsprechend das Recht auf Widerruf der Einwilligung sowie auf Widerspruch gegen eine Verarbeitung auf Basis berechtigter Interessen über entsprechende Einstellungen im Endnutzer-Dialog ausüben. Im Hinblick auf sonstige Betroffenenrechte, deren Ausübung nicht über Funktionalität der CMP ermöglicht wird, wird der Auftragnehmer nur nach Weisung des Auftraggebers über die Daten, die im Auftrag verarbeitet werden, Auskunft geben, diese Daten berichtigen, löschen oder die Datenverarbeitung entsprechend einschränken. 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

Im Falle einer Beendigung der Vereinbarung wird der Auftragnehmer nach Wahl und Aufforderung durch den Auftraggeber sämtliche im Rahmen der Durchführung der Vereinbarung in Besitz des Auftragnehmers gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, unverzüglich, spätestens innerhalb von 30 Tagen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Für vom Auftragnehmer angefertigte Backups gilt abweichend eine Lösch- bzw. Herausgabefrist von längstens 6 Monaten.

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.

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

Technischen und organisatorische Maßnahmen (TOM)
i.S.d. Art. 28 Abs. 3 lit. c, 32 DSGVO

Die **Usercentrics GmbH**, Sendlinger Straße 7, 80331 München, Deutschland (folgend „Usercentrics“) verarbeitet personenbezogene Daten im Auftrag ihrer Kunden. Dabei ist sich Usercentrics seiner Verantwortung als Auftragsverarbeiter bewusst. Entsprechend wurden technische und organisatorische Maßnahmen getroffen, um Risiken und Gefährdungspotenziale, die sich im Rahmen der Verarbeitung personenbezogener Daten ergeben, maßgeblich zu reduzieren. Wie ein der DSGVO entsprechendes Sicherheits- und Datenschutzniveau erzielt wird, ist den folgenden technischen und organisatorischen Maßnahmen zu entnehmen. Diese gelten als mit dem Auftraggeber vereinbart.

Inhaltsverzeichnis

1. Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit b DSGVO)

Usercentrics ergreift Maßnahmen zur Umsetzung des Gebots der Vertraulichkeit. Darunter fallen unter anderem Maßnahmen zur Zutritts-, Zugriffs- und 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.

Zutrittskontrolle

- Sofern personenbezogene Daten Gegenstand der Verarbeitung sind, werden diese in Systemen gespeichert, die sicher sind (z.B. ISO/IEC 27001/27017/27018/27701)
- Zutritt zur Cloud Infrastruktur von Google Cloud - weitere Informationen zu Maßnahmen finden sich hier: https://cloud.google.com/security
- Alle Systeme und Devices werden in regelmäßigen Abständen aktualisiert (Softwareaktualisierung).
- Alle Systeme werden regelmäßig auf Schwachstellen geprüft.
- In den Räumlichkeiten von Usercentrics befindet sich keine kritische IT-Infrastruktur (Serversysteme). Dennoch wird der physikalische Zutritt zu Büroflächen größtmöglich mit Sicherheitsmaßnahmen geschützt. Dazu zählen u.a.
    - Zutritt zum Büro nur mit personalisierten Türtranspondern /Schließzylindern möglich für Mitarbeiter und Dienstleister (z.B. Reinigungsdienst) und protokollierter Schlüssel-/Transponderausgabe-/rücknahme.
    - der Einsatz von Überwachungskameras (Innen – z.B. Eingangsbereich).
    - Besucher müssen klingeln, sich persönlich anmelden, identifizieren und dürfen sich nicht frei in den Räumlichkeiten bewegen.

Zugangskontrolle

- Der Zugang zu personenbezogenen Daten ist nur für einen eingegrenzten Kreis an Mitarbeitern möglich, der zudem mit eigenen persönlichen Zugangsdaten (User-ID & Passwort) und nur verschlüsselten (HTTPS, TLS/SSL) erreichbar ist.
- Gruppen-Accounts /System-Logins nur für bestimmte Anwendungen.
- Getrennte Benutzerkennungen für priviligierte Berechtigungen.
- Benutzerkennungen werden, wenn Mitarbeiter das Unternehmen verlassen, umgehend deaktiviert/gelöscht.
- Passwörter werden nicht im Klartext gespeichert oder unverschlüsselt übertragen.
- Für die Benutzerauthentifizierung gelten Anforderungen an das zu wählende Passwort: 8-12 Zeichen lang; Es sind 3-4 Zeichenarten zu nutzen; Groß- & Kleinschreibung; Keine gängigen Begriffe; Das Passwort ist bei Anlass/Hinweis auf Missbrauch umgehend zu ändern; Passwörter sind umgehend nach Account-Aktivierung durch den Nutzer durch ein neues Passwort wechseln
- Wo immer möglich, wird eine Zwei-Faktor-Authentifizierung eingesetzt.
- Session Management.
- Interne IT-Sicherheitsrichtlinien.
- Automatische Sperrung der Clients (z.B. Mitarbeiter-Arbeitsrechner) nach definierten Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung).

Zugriffskontrolle

- Zugriffe erfolgen gemäß eines Berechtigungskonzepts und Kryptokonzepts.
- Nutzung eines Benutzer- und Benutzergruppenmanagementsystems sowie Zugriffsrechteverwaltung.
- SSH ist, wo immer möglich, deaktiviert.
- Je nach Tätigkeitsgebiet des Mitarbeiters werden abgestufte Berechtigungen vergeben. Hier wird stets nach dem Minimalprinzip gearbeitet.

Weitere Maßnahmen

- Strikte Trennungskontrolle: Sofern unterschiedliche Zwecke vorliegen, werden Daten nicht gemeinsam verarbeitet. Hier unterstützt eine Mandantentrennung (logisch oder physisch) /Funktionstrennung.
- Jedes System für sich wird in seinem jeweiligen Stadium für seine jeweilige Funktion auf einem eigenen Server betrieben (Trennung von Entwicklungs-, Test- und Produktivsystem, Funktionstrennung).
- Sofern der jeweilige Zweck für eine Datenverarbeitung erlischt, werden die Daten gelöscht. Dies erfolgt gemäß des Löschkonzepts.
- Die Verschlüsselung der Data-at-rest erfolgt über AES256 mit verschiedenen Schlüsseln per Datensegment. Die Verschlüsselung der Data-in-transport erfolgt mit TLS 1.3.

2. Gewährleistung der Integrität (Art. 32 Abs. 1 lit b DSGVO)

Es werden Maßnahmen ergriffen, die dem Gebot der Integrität dienen. Darunter fallen unter anderem Maßnahmen zur Eingabekontrolle, aber auch solche, die generell zum Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Zerstörung oder unbeabsichtigter Schädigung beitragen.

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:

- Der Versand von Daten (z.B. E-Mails) erfolgt verschlüsselt.
- Es findet immer dann Datenverschlüsselung statt, wenn ein Datentransport auf Devices stattfindet. Unter diese Regelung fallen z.B. die eingesetzten Arbeitsrechner für unsere Mitarbeiter wie auch verwendete externe Festplatten oder USB-Sticks. Auch für Speicherkarten und CDs/DVD-ROMs gelten interne Verschlüsselungsvorgaben.
- Es kommen ausschließlich sichere Drahtlosnetzwerke (WLAN) zum Einsatz, die alle mit WPA-2 verschlüsselt sind.
- Sofern geboten, kommt VPN-Technologie zum Einsatz.
- Sofern Datenträger, Daten und Ausdrucke nicht mehr genutzt werden, erfolgt eine sichere Löschung bzw. Zerstörung. So wird gewährleistet, dass Daten höchstmöglich nicht wiederherzustellen sind.
- Sofern geboten, erfolgt die Protokollierung der Datenweitergabe.

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:

- Hohe Maßstäbe in der gesetzeskonformen Vertragsgestaltung bei Verträgen über die Verarbeitung personenbezogener Daten mit Subunternehmen, die Regelungen von Kontrollmöglichkeiten enthalten.
- Einsatz von Protokollierungs- und Protokollauswertungssystemen, um Benutzereingaben zu dokumentieren. Sofern an Systemen, die personenbezogene Daten verarbeiten, Anpassungen durchgeführt werden, wird dies aufgezeichnet und bedarfsgerecht vorgehalten (z.B. in Form von Logfiles).
- Die Eingabe von Daten sowie die Ausgabe wird auf Plausibilität geprüft (Prüfung Dateipfade etc.).
- Einholen von Auskünften bei Dienstleistern hinsichtlich der umgesetzten Maßnahmen zur Umsetzung datenschutzrechtlicher Anforderungen.
- Mündliche Weisungen werden schriftlich bestätigt.

3. Gewährleistung der Verfügbarkeit (Art. 32 Abs. 1 lit b DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen die zufällige Zerstörung oder Verlust geschützt sind.

Spezifische Maßnahmen für unsere Produktivumgebung (Consent Management Platform (CMP)) & damit zusammenhängende Systeme

Usercentrics betreibt keine eigenen Serverressourcen in eigenen Rechenzentren. Sofern die Verarbeitung durch Subunternehmer erfolgt, gelten u.a. folgende Maßnahmen – vor und während der Datenverarbeitung:

- Monitoring /Überwachung der Systemaktivitäten durch unsere Mitarbeiter.
- Unsere Produktivumgebung wird in regelmäßigen Abständen gesichert bzw. es kommen Verfahren zur Datenspiegelung zum Einsatz.
- Die Außerbetriebnahme von Hardware (insbesondere von Servern) erfolgt nach einer Überprüfung der darin eingesetzten Datenträger und ggf. nach erfolgter Sicherung der relevanten Datensätzen.
- Die Systeme sind durch eine unterbrechungsfreie Stromversorgung (USV) abgesichert.
- Es kommt eine mehrschichtige Virenschutz- und Firewall-Architektur zum Einsatz.
- Die eingesetzten Rechenzentren verfügen über Feuer-/ Wasser- und Temperaturfrühwarnsysteme in den Serverräumen sowie Brandschutztüren.
- Die Aufbewahrung von Datenbeständen, die zu unterschiedlichen Zwecken erhoben wurden, erfolgt getrennt.
- Regelmäßiges Patch Management.
- Load Balancing.
- Die Zuschaltung von Datenspeicher erfolgt im Rahmen dynamischer Prozesse.
- Es werden regelmäßig Penetrations- und Belastungstests durchgeführt.
- Die Belastungsgrenze wird für das jeweilige Datenverarbeitungssystem im Vorfeld der Datenverarbeitung oberhalb des notwendigen Minimum angesetzt.
- Regelmäßige Trainings des eingesetzten Personals.

Für das Produktivsystem (CMP) & damit zusammenhängende Systeme werden vorrangig **Google Cloud** Ressourcen (Google LLC, 1600 Amphitheatre Parkway, Mountain View, California 94043 USA) eingesetzt.
Hierbei wird zwischen folgenden Ressourcen-Kategorien unterschieden: statisches Hosting, APIs und Datenbanken.

Statisch gehostete Ressourcen sind auf Servern innerhalb der Mitgliedsstaaten der EU gespeichert (exkl. Zürich und London) und werden durch ein globales CDN Netzwerk Cache bereitgestellt mit einer Verfügbarkeit von mindestens 99.95% (https://cloud.google.com/cdn/sla).

APIs oder dynamisch gehostete Ressourcen werden auf Servern innerhalb der Mitgliedsstaaten der EU bereitgestellt, vorrangig Frankfurt und Belgien. Für einige Ressourcen ist ein globaler CDN Netzwerk Cache im Einsatz.

Datenbanken werden auf Servern innerhalb der Mitgliedsstaaten der EU bereitgestellt, vorrangig Frankfurt und Belgien.

Weitere Informationen finden sich unter:

https://cloud.google.com/terms/data-processing-terms#appendix-2-security-measures

Weitere Maßnahmen

- Sofern Unternehmen mit der Verarbeitung personenbezogener Daten beauftragt werden, erfolgt dies immer unter der Voraussetzung eines vorliegenden Auftragsverarbeitungsvertrags, der den Vorgaben des Art. 28 DSGVO entspricht, – dafür werden entsprechende Vertragsmuster vorgehalten. Diese stellen auch sicher, dass Usercentrics über mögliche Gefährdungen der Verfügbarkeit frühzeitig informiert wird.
- Einsatz von Virensoftware auf den Mitarbeiterrechnern.

- Die Speicherung von Daten auf den Mitarbeiterrechnern wird weitestgehend reduziert. Datenspeicherung erfolgt auf sicheren Cloud-Systemen.
- Eingesetzte Standardsoftware unterliegt einer Vorabprüfung und darf nur aus eingegrenzten sicheren Quellen bezogen worden.
- Die interne Office IT ist durch eine unterbrechungsfreie Stromversorgung (USV) im Verteilerraum abgesichert.
- Für Sicherheits- und Datenschutzverletzungen wurden Notfallpläne mit konkreten Handlungsanweisungen etabliert.

4. Gewährleistung der Wiederherstellbarkeit (Art. 32 Abs. 1 lit b DSGVO)

Sofern es zu einem physischen oder technischen Zwischenfall kommt, sind Maßnahmen etabliert, die eine schnelle Verfügbarkeit sicherstellen, und im Rahmen eines Maßnahmenplans über die reine Datensicherung hinausgehen. Um in diesen Katastrophen-Fall-Szenarien den laufenden Betrieb wiederherstellen zu können, wird folgendes unternommen:

Spezifische Maßnahmen für unsere Produktivumgebung (Consent Management Platform) & damit zusammenhängende Systeme

- Tägliches Backup der gesamten Server-Ressourcen durch den Hosting-Anbieter (Google LLC, 1600 Amphitheatre Parkway, Mountain View, California 94043 USA).
- Desaster Recovery.
- Abschluss von Service Level Agreements (SLAs) mit Dienstleistern.
- Mehrstufige Backupverfahren.
- Redundantes Vorhalten (Clustersetups / Geo-Redundanz) von Daten (z.B. Festplattenspiegelung).
- Einsatz von Firewall, IDS/IPS.
- Brand- und Löschwasserschutz.
- Alarm-Monitoring.
- Pläne & Szenarien für Ausfall, Notfall und Wiederherstellung.

Weitere Informationen:
https://cloud.google.com/security

5. Maßnahmen zur Pseudonymisierung von personenbezogenen Daten

Bei Pseudonymisierung handelt es sich um 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. Dazu werden folgende Maßnahmen ergriffen:

- Etablierung eines strikten Privacy-by-design-Ansatzes.
- Etablierung eines Pseudonymisierungskonzeptes (u.a. Definition der zu ersetzenden Daten; Pseudonymisierungsregeln, Beschreibung Vorgehensweise).
- Für die Pseudonymisierung wird ein sha-256 kryptografischen Hash verwendet..

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen

Eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung einer sicheren Verarbeitung von personenbezogenen Daten erfolgt durch folgende Maßnahmen:

Datenschutzmanagementsystem

Alle Verfahren, etwaige Behördenanfragen, Verträge und Verzeichnisse werden zu Dokumentations- und Transparenzzwecken vorgehalten. Änderungen werden ebenfalls dokumentiert.

Informationssicherheitsmanagementsystem

Alle Konzepte, Prozesse und Risikoanalysen werden in einem internen ISMS vorgehalten.

Verarbeitung von Daten im Auftrag von Usercentrics bzw. durch Subunternehmer

Einer Beauftragung geht immer ein umfangreicher Auswahlprozess sowie ein PreCheck voraus. Wir prüfen, ob unser hier ausgeführter hoher Standard auch bei potenziellen Auftragsverarbeitern eingehalten wird. Erst wenn das erfolgt ist und ein Auftragsverarbeitungsvertrag, der den Vorgaben des Art. 28 DSGVO entspricht,geschlossen ist, darf eine Verarbeitung erfolgen. Neben den PreChecks führen wir auch wiederkehrende Prüfungen durch, um das geforderte Niveau permanent aufrechtzuerhalten. Die vereinbarten Leistungen sind konkret in den Auftragsverarbeitungsverträgen festgehalten, um den Auftragsbereich klar abzugrenzen.

Schulungen & Mitarbeitersensibilisierung

Jeder Mitarbeiter erhält zum Start bei Usercentrics alle wichtigen Informationen zum Thema Datenschutz sowie Informationssicherheit und wird zur Vertraulichkeit verpflichtet. Mit regelmäßigen (Auffrischungs-) Schulungen und punktueller Informationsbereitstellung (Artikel, Cases etc.) gewährleisten wir ein ständig hohes Niveau an Mitarbeitersensibilisierung.

Aktualität Sicherheitskonzept

Das Sicherheitskonzept wird einer regelmäßigen Revision unterzogen und bei Bedarf angepasst.

Verantwortlichkeiten

Die Verantwortung für die Umsetzung der hier beschriebenen Maßnahmen und Prozesse liegt innerhalb der zuständigen Departments bzw. Fachbereiche. Das regelmäßige Monitoring erfolgt in Teilen durch den Datenschutzbeauftragten sowie den Information Security Officer.

Weitere Maßnahmen

- Prüfen von Informationen über neu auftretende Schwachstellen und andere Risikofaktoren inkl. ggf. Überarbeitung der Risikoanalyse und Bewertung
- Auditierung des Datenschutzbeauftragten und des Information Security Officer sowie regelmäßige Prozesskontrollen durch entsprechendes Qualitätsmanagement

Kontaktdaten des Datenschutzbeauftragten:

SECUWING GmbH & Co. KG Maximilian Hartung, Frauentorstr. 9, 86152 Augsburg, Deutschland, epost@datenschutz-agentur.de, Tel. +49 (0) 821 907 86 450

Kontaktdaten des Information Security Officer:

activeMind AG Klaus Foitzick, Potsdamer Str. 3, 80802 München, Deutschland, foitzick@activemind.de, Tel. +49 (0) 89 9192 94 900

Interne Datenschutzkoordination:

Jan Philip Schreiber, Head of Operations, Sendlinger Str. 7, 80331 München, Deutschland, privacy@usercentrics.com

Anlage 2 zur Auftragsverarbeitungsvereinbarung

Genehmigte Unterauftragnehmer

#	Name	Betreibergesellschaft	Anschrift des Unterauftragnehmers	Ort der Datenverarbeitung	Einsatzbereich im Rahmen des Vertrags	Betroffene
1	Google	Google Cloud EMEA Ltd. *	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Server in der Europäischen Union *	Hosting	User des Auftraggebers

*Im Übrigen gelten hier die Standardvertragsklauseln zwischen Usercentrics und Google Cloud EMEA Ltd. für jegliche Datenübermittlung in die USA aufgrund der Entscheidung des Europäischen Gerichtshofs vom 16.07.2020 (EuGH, 16.7.2020 - C-311/18 "Schrems II") abrufbar unter https://cloud.google.com/terms/sccs/eu-p2p sowie zusätzliche Maßnahmen, soweit dies erforderlich ist, um ein angemessenes Datenschutzniveau zu gewährleisten (siehe 3.4. der Vereinbarung).

Anlage 3: Leistungsbeschreibung

Usercentrics bietet als Software as a Service (SaaS) Lösung eine Consent Management Platform (CMP) an. Diese dient der Erhebung, Verwaltung, Dokumentation und Weitergabe von Einwilligungen, sowie personenbezogener Daten, die auf Grundlage berechtigter Interessen erhoben wurden. Durch Nutzung der CMP werden bei Aufruf der Webseite die Skripte der einzelnen implementierten Technologien blockiert. Diese Technologien werden erst nach erfolgter Einwilligung ausgespielt. Technologien die auf Grundlage des berechtigten Interesses genutzt werden, werden nicht blockiert und automatisch ausgespielt.

Durch die CMP wird es ermöglicht die Einwilligung des Nutzers sowie zukünftige Änderungen in der Entscheidung nachzuverfolgen und zu dokumentieren. Es wird auch die Möglichkeit des Widerrufs der Einwilligung über eine eingebettete Schaltfläche (Privacy Button/Link) geboten. Durch diese hat der Nutzer die Möglichkeit seine Entscheidung nachträglich anzupassen.

Es werden folgende Daten der Nutzer des Auftraggebers bei Nutzung der CMP erhoben:

- Userdaten:
    - Consent Daten (Consent ID, Consent Nummer, Uhrzeit der Abgabe Consents, Opt-in o. Opt-out, Banner Sprache, Kunden Setting, Template Version)
    - Device Daten (HTTP Agent, HTTP Referrer)
    - IP-Adresse

Zusätzlich wird dem Auftraggeber eine Datenbank zur Verfügung gestellt, die die aktuellste Version der Datenschutztexte (Data Processing Services) der eingesetzten Technologien als Vorlage beinhaltet. Diese dienen lediglich als Vorlage und Usercentrics übernimmt für die Richtigkeit keine Gewähr. Es besteht außerdem die Möglichkeit eigene individuell angepasste Texte für die eingesetzten Technologien zu erstellen. Es steht dem Auftraggeber frei, welche Version in der CMP Live geschaltet wird.

Weiterhin wird ein initialer Scan der Website des Auftraggebers durchgeführt, welcher einen Überblick über die verwendeten Data Processing Services (DPS) ermöglicht. Nach Implementierung der CMP scannt das auf der Webseite integrierte Usercentrics Skript regelmäßig und äußerst genau basierend auf der Live-Benutzeraktivität nach neuen DPS und aktualisiert die Ergebnisse entsprechend.