VERTRAG ÜBER AUFTRAGSVERARBEITUNG IM SINNE VON ART. 28 ABS. 3 DSGVO

Stand vom: 24.02.2020

ZWISCHEN

P-N-S UG (haftungsbeschränkt)
Viehofer Platz 14
45127 Essen

- im Folgenden: Auftraggeber -

UND

Usercentrics GmbH
Rosental 4
80331 München

- im Folgenden: Auftragnehmer -

1. Allgemeine Bestimmungen und Vertragsgegenstand

1.1. Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragnehmer (Art. 28 DSGVO). Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist der Auftraggeber. Die Auftragsdetails entnehmen Sie der **Anlage 1**.

1.2. Die Verarbeitung der vertragsgegenständlichen personenbezogenen Daten außerhalb der Europäischen Union ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

2. Vertragslaufzeit und Kündigung

2.1. Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3.1. Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragnehmer zu. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragnehmer substantiiert anzweifelt, ist der Auftragnehmer berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert. Besteht die Möglichkeit, dass der Auftragnehmer durch das Befolgen der Weisung einem Haftungsrisiko ausgesetzt wird, kann die Durchführung der Weisung bis zur Klärung der Haftung im Innenverhältnis ausgesetzt werden.

3.2. Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z. B. per E-Mail) zu erteilen. Mündliche Weisung sind in begründeten Einzelfällen zulässig und werden vom Auftraggeber unverzüglich schriftlich oder in einem elektronischen Format bestätigt. In der Bestätigung ist ausdrücklich zu begründen, warum keine schriftliche Weisung erfolgen konnte. Der Auftragnehmer hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3.3. Der Auftraggeber benennt auf Verlangen des Auftragnehmers eine oder mehrere weisungsberechtigte Personen. Personelle Änderungen sind dem Auftragnehmer unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1. Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren. Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragnehmers nicht mehr als erforderlich beeinträchtigen.

4.2. Die Ergebnisse der Kontrollen und Weisungen sind vom Auftraggeber in geeigneter Weise zu protokollieren.

5. Allgemeine Pflichten des Auftragnehmers

5.1. Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragnehmer erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z. B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragnehmer dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

5.2. Der Auftragnehmer hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

6. Technische und organisatorische Maßnahmen

6.1. Der Auftragnehmer hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 2 dieses Vertrags dokumentiert. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben von Art. 32 DSGVO ausgewählt. Der Auftragnehmer wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen.

7. Unterstützungspflichten des Auftragnehmers

7.1. Der Auftragnehmer wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO, unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Der Auftragnehmer wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflichten bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der Informationen, die dem Auftragnehmer zur Verfügung stehen.

8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)

8.1. Der Auftragnehmer ist zum Einsatz von Unterauftragsverarbeitern (Subunternehmern) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden Subunternehmerverhältnisse des Auftragnehmers sind diesem Vertrag abschließend in Anlage 3 beigefügt. Für die in Anlage 3 aufgezählten Subunternehmer gilt die Zustimmung mit Abschluss dieses Vertrags als erteilt.

8.2. Beabsichtigt der Auftragnehmer den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber rechtzeitig - spätestens jedoch zwei Wochen - vor deren Einsatz in schriftlicher oder elektronischer Form anzeigen. Der Auftraggeber hat nach dieser Mitteilung zwei Wochen Zeit, der Hinzuziehung des / der Subunternehmer zu widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Hinzuziehung des / der Subunternehmer(s) als genehmigt. Im Falle eines Widerspruchs dürfen die betroffenen Subunternehmer nicht eingesetzt werden. Widersprüche sind nur zulässig, wenn der Auftraggeber begründete Anhaltspunkte dafür hat, dass durch den Einsatz des Unterauftragnehmers die Datensicherheit oder der Datenschutz eingeschränkt würde, die Einhaltung gesetzlicher oder vertraglicher Bestimmungen gefährdet wäre und / oder sonstige berechtigte Interessen des Auftraggebers entgegenstehen; die entsprechenden Verdachtsmomente sind dem Widerspruch beizufügen.

8.3. Subunternehmer werden vom Auftragnehmer unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Nebenleistungen, welche der Auftragnehmer zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse im Sinne des Art. 28 DSGVO dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit und / oder Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragnehmer wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards (insbesondere durch entsprechende Vertraulichkeitsvereinbarungen) sicherstellen.

8.4. Sämtliche Verträge zwischen dem Auftragnehmer und dem Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen.

8.5. Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten des Auftragnehmers

9.1. Verstöße gegen diesen Vertrag, gegen Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragnehmer selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

9.2. Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragnehmer um Auskunft, Berichtigung, Einschränkung der Verarbeitung oder Löschung, wird der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragnehmer dem Ersuchen des Betroffenen ohne Weisung / Zustimmung des Auftraggebers nachkommen.

9.3. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragnehmer den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch welche die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

10.1. Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine rechtliche oder vertragliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z. B. gesetzliche Aufbewahrungsfristen).

11. Datengeheimnis und Vertraulichkeit

11.1. Der Auftragnehmer ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln. Der Auftragnehmer verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragnehmer aufnehmen.

12. Schlussbestimmungen

12.1. Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

12.2. Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

12.3. Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

12.4. Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

Anlagen

Anlage 1 – Auftragsdetails

1. Der vorliegende Vertrag umfasst (ggf. im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:

Nutzung der Management Plattform; mit der Nutzer-Einwilligungen DSGVO-konform eingeholt, verwaltet und dokumentiert werden können.

2. Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

2.1 Anonymisierte IP Adresse

2.2 Consent Daten (Conenst ID, Consent Nummer, Device ID, Uhrzeit, Kunden Settings-Version, Banner Sprache, Kunden Setting, Opt-in/Opt-out, Template, Template Version, Consent explizit/implizit)

2.3 Device Daten (HTTP Agent (Name und Version des browsers), HTTP Referrer, Device ID)

3. Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

3.1 Besucher

3.2 Potenzielle Kunden

Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO

Der Auftragnehmer setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

1. Auftragskontrolle (organisatorisch)

1.1. Auftragnehmer Weisung - Schriftliche Weisungen an den Auftragnehmer

2. Datenschutz-Management (organisatorisch)

2.1. Sensibilisierung - Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich

2.2. Schulung/Verpflichtung - Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet

2.3. Datenschutzbeauftragter - Externer Datenschutzbeauftragter:

Dr. Sebastian Kraska Rechtsanwalt, Dipl.-Kfm.
IITR Datenschutz GmbH
External data protection officer
Marienplatz 2
80331 Munich
Germany
E-mail: datenschutz@usercentrics.com

3. Datenschutz-Management (technisch)

3.1. Prüfung technischer Schutzmaßnahmen - Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt

3.2. Anerkannte Sicherheitszertifizierung - Sicherheitszertifizierung nach ISO 27001, BSI ITGrundschutz oder ISIS1

4. Eingabekontrolle (technisch)

4.1. Veränderungsprotokollierung - Technische Protokollierung der Eingabe, Änderung und Löschung von Daten

4.2. Elektronisches Aufzeichnen - von Eingaben - von Datenverarbeitungen, insbesondere Nutzung, Änderung und Löschung von Daten - der Nutzung von Administrations-Tools

5. Transport- und Weitergabekontrolle

5.1. Vorgabe von verbindlichen oder möglichen Speicherorten für Daten

5.2. Kontrolle der Datenträgerentfernung

5.3. Interne Verifizierungsanforderungen - Vier-Augen Prinzip

5.4. Authentifizierung der berechtigten Personen

6. Transport- und Weitergabekontrolle (technisch)

6.1. Signaturverfahren - Nutzung von Signaturverfahren

6.2. Protokollierung der Zugriffe und Abrufe

7. Trennungskontrolle

7.1. Trennung von Daten, die unter einem Alias (Pseudonym) gespeichert wurden von den Originaldaten

8. Trennungskontrolle (technisch)

8.1. Physikalische Trennung - Systeme/Datenbanken/Datenträger

8.2. Berechtigungskonzept - Steuerung über Berechtigungskonzept

9. Verfügbarkeitskontrolle (organisatorisch)

9.1. Notfallmanagement - Notfallplan vorhanden. Schulung der Mitarbeiter

9.2. Backupkonzept - Backup & Recovery-Konzept (ausformuliert)

10. Verfügbarkeitskontrolle (technisch)

10.1. Festplattenspiegelung - RAID System / Festplattenspiegelung

11. Zugangskontrolle (organisatorisch)

11.1. Zweckmäßiger und/oder zeitlich beschränkter Zugang zu Endgeräten und/oder der Nutzer und der Identifikationsmerkmale

11.2. Zugangsberechtigungen - Für Angestellte, einschließlich der jeweiligen Dokumentation

11.3. Zugangsberechtigung nur für bestimmte Einzelpersonen

11.4. Überprüfungs-, Korrektur- und Kontrollsysteme

11.5. Regeln und Vorschriften für Dritte - z.B. IT-Dienstleister

11.6. Prozesse für die Überprüfung und den Release von Programmen

11.7. Protokollierung von Vorfällen - Überwachung von Einbruchsversuchen

11.8. Passwort-Richtlinien - regelmäßige Änderung, Mindestlänge, Komplexität etc.

11.9. Organisation von Dateien - Regelungen über die Organisation von Dateien

11.10. Differenzierte Zugangsregeln - Teilweise Blockierung

11.11. Benutzernamen und Passwörter

11.12. Arbeitsanweisung für die Dokumentenvorlage für die Registrierung von Daten

12. Zugangskontrolle (technisch)

12.1. Virenschutz - Einsatz von Anti-Viren-Software

12.2. Verschlüsselung von Daten im Fall der Online-Übertragung

12.3. Verschlüsselung mobiler Datenträger

12.4. Schutz des Übertragungskanals vor unberechtigtem Zugang

12.5. Firewall - Einsatz einer Firewall

12.6. Automatische Löschung der Benutzer-ID bei mehrmaliger Eingabe eines falschen Passworts

12.7. Automatische Desktopsperre

12.8. Automatische Abmeldung von Benutzer-IDs, die über einen gewissen Zeit-raum nicht genutzt wurden

13. Zugriffskontrolle/Pseudonymisierung (organisatorisch)

13.1. Systemtrennung - Trennung von Produktiv- und Testumgebung

13.2. Sicherung der Bereiche, in denen sich Datenträger befinden

13.3. Kontrolle der Entfernung von Datenträgern

13.4. Kennzeichnung der Bereiche, in denen sich Datenträger befinden können/dürfen

13.5. Einsatz Berechtigungskonzepte - Berechtigungskonzept vorhanden.

13.6. Differenzierte Zugriffsregelungen - z. B. partielle Sperrung, genaue Nutzerrollen oder Profile

13.7. Bestimmte Zugriffsregeln für Prozesse, Kontrollkarten, Prozesssteuerungsmethoden, Programmkatalogisierungsberechtigung

13.8. Autorisierter Zugriff - Zugriff nur für dafür autorisiertes Personal

13.9. Administratoren - Minimale Anzahl an Administratoren mit besonderen Zugriffsberechtigungen

14. Zugriffskontrolle/Pseudonymisierung (technisch)

14.1. Vernichtung von Datenträgern - Unwiderrufliche Vernichtung von nicht mehr benötigten Datenträgern

14.2. Sichere Löschung - Sichere Löschung von Datenträgern durch Einsatz von spezieller Software

14.3. Schutzmaßnahmen für die Dateneingabe in den Speicher und für das Lesen, die Sperrung und Löschung von gespeicherten Daten

14.4. Pseudonymisierung - Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System

14.5. Protokollierung - Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten

14.6. Physische Löschung von Datenträgern

14.7. Nutzung von Verschlüsselung für sicherheitskritische Dateien

14.8. Identifikation des Endgerätes und/oder des Nutzers im System des Auftragsverarbeiters

14.9. Endgeräte mit Zugriffsbenutzerschlüssel oder Benutzercode

14.10. Automatische Abmeldung von Nutzer IDs - Abmeldung nach einem gewissen Zeitraum

14.11. Aktenschredder - Nutzung eines Aktenschredders

15. Zutrittskontrolle

15.1. Sicherung der dezentralisierten Datenverarbeitungsanlagen und der Arbeitsplatzrechner

15.2. Schutz und Einschränkung von Zutrittswegen

15.3. Closed shops - Bestimmte Sicherheitsbereiche mit eigenen Zutrittskontrollen

15.4. Bauliche Maßnahmen - Zäune, Überwachungskameras, verschlossene Türen, Tore und Fenster etc.

16. Zutrittskontrolle (organisatorisch)

16.1. Zutrittskonzept - Zutrittskonzept / Besucherregelung

16.2. Vertrauenswürdiges Wachpersonal - Sorgfältige Auswahl von Wachpersonal

16.3. Vertrauenswürdiges Reinigungspersonal - Sorgfältige Auswahl von Reinigungspersonal

16.4. Schlüsselregelung - Vergabe policy, Quittierung

17. Zutrittskontrolle (technisch)

17.1. Videoüberwachung - Videoüberwachung der Eingänge

17.2. Verschließbarkeit von Eingängen zu Datenverarbeitungseinrichtungen - Räume, Gehäuse, Computer-Hardware und ähnliche Geräte

17.3. Sicherheitstür - Verwendung von Sicherheitstüren

17.4. Sicherheitsschlösser - Verwendung von Sicherheitsschlössern in Türen

17.5. Gebäudeschachtsicherung - Secrurity Officer

17.6. Elektronisches Schließsystem - Transponder-Schließsystem

17.7. Alarmanlage - Sicherung des Gebäudes oder Eingängen mittels einer Alarmanlage

Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

Google Cloud

Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland