Website: https://www.trustcaptcha.com
E-Mail: mail@trustcaptcha.com

# Auftragsverarbeitungsvertrag

# Data processing agreement

Dieses Dokument enthält den rechtlich verbindlichen Auftragsverarbeitungsvertrag in deutscher Fassung einschließlich aller Anhänge sowie eine entsprechende englischsprachige Übersetzung.

This document contains the legally binding order data processing agreement in German, including all annexes, as well as a corresponding English translation.

# Auftragsverarbeitungsvertrag

Zwischen

Example Ltd., Street 1, 12345 City, Country
- nachstehend Verantwortlicher genannt -

und

Trustcaptcha GmbH, Hans-Böckler-Straße 32, 80995 München, Deutschland
- nachfolgend Auftragsverarbeiter genannt -

gelten nachfolgende Regelungen für die Auftragsverarbeitung.

## 1 - Gegenstand und Dauer der Auftragsverarbeitung

### 1.1 Gegenstand

Wesentlicher Gegenstand ist die Bereitstellung eines Software-as-a-Service (SaaS) Online-Dienstes, bekannt als CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). Die vom Vertrag umfassten Leistungen erstrecken sich auf die Bereitstellung, den Betrieb, Wartung, Support, Analyse und Verbesserung der Dienstleistungen des CAPTCHA-Dienstes.

Dieser Vertrag ergänzt den Servicevertrag (nachfolgend Hauptvertrag) zwischen dem Verantwortlichen und Trustcaptcha GmbH. Der Vertrag geht dem Hauptvertrag vor, wenn es um die Erfüllung regulatorischer Anforderungen im Bereich des Datenschutzes oder der Datensicherheit gemäß der DSGVO geht und dies nur in Bezug auf die jeweiligen Felder, in denen personenbezogene Daten verarbeitet werden.

### 1.2 Dauer

Die Dauer (Laufzeit) dieses Vertrags entspricht der Laufzeit des Hauptvertrags, mindestens aber während der Auftragsverarbeiter für den Verantwortlichen personenbezogene Daten verarbeitet. Darüber hinaus stimmen die Parteien überein, dass alle vorherigen Verträge zur Auftragsverarbeitung mit dem Abschluss dieses Vertrages einvernehmlich aufgehoben werden.

## 2 - Konkretisierung der Datenverarbeitung

### 2.1 Zweck und Art der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten für den Verantwortlichen i.S.v. Art. 4 Nr. 2 DSGVO auf Grundlage des Auftrags. Der Zweck der Datenverarbeitung ist der Schutz von Unternehmen, durch die Sicherheitsmechanismen des CAPTCHA-Diensts von Trustcaptcha, sowie die Bereitstellung zusätzlicher Funktionen. Trustcaptcha wertet Daten bei CAPTCHA-Anfragen zur Bedrohungsanalyse aus. Trustcaptcha verarbeitet zudem Daten, um damit verbundene erweiterte Funktionen anbieten zu können. Die Daten können insbesondere, soweit jeweils erforderlich: erhoben, gespeichert, organisiert, verändert, ausgelesen, abgefragt, verwendet, offengelegt, abgeglichen, verknüpft und gelöscht werden.

### 2.2 Gegenstand der Verarbeitung

Gegenstand der Verarbeitung durch den CAPTCHA-Dienst sind Nutzungs-/Verhaltensdaten, Gerätedaten, Verbindungsdaten und Standortdaten. Dazu zählen beispielsweise, abhängig von Gerät und Einstellungen des Nutzers, Angaben zu Geräteeigenschaften und Gerätedaten (z.B. Gerät und Gerätetyp, Betriebssystem, Plugins, Bildschirmgröße, Hardware), IP-Adresse, Referrer-Website, automatisch übermittelte Cookies, Verhaltensdaten wie Maus- und Tastaturverhalten bzw. Berührungen bei Touch-Geräten, sowie Einstellungen (z. B. Sprache). Diese können temporär gespeichert, mit anderen Informationen wie z.B. Uhrzeit, allgemeinen Standortinformationen und IP-Allow-/Blocklists abgeglichen und ausgewertet werden. Manche Daten können temporär zur Weiterentwicklung der Schutzmechanismen gespeichert werden. Die Datenerfassung durch das CAPTCHA beschränkt sich auf technische, verhaltensbezogene und statistische Aspekte, es werden keine inhaltlichen Eingaben ausgewertet. Die vom CAPTCHA-Dienst verarbeiteten Daten werden ausschließlich für die Zwecke der CAPTCHA-Verifikation, sowie um zuverlässig auf zukünftige Bedrohungen vorbereitet zu sein, verarbeitet. Die Daten werden zudem für die Bereitstellung von Statistiken und Nutzungsinformationen für den Verantwortlichen verarbeitet. Um bei wandelnden Anforderungen und Rahmenbedingungen effektiven Schutz zu bieten, sowie durch die Erweiterung um neue Funktionen, können zukünftig auch andere Daten verarbeitet werden.

**2.3 Kategorien betroffener Personen**

Die Verarbeitung betrifft:

- Personen, die die Auswertung (Bot-Verifikation) von einem CAPTCHA-Feld auslösen

**2.4** Die vertraglich vereinbarte Datenverarbeitung personenbezogener Daten wird in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum durchgeführt. Eine Verlagerung in ein Drittland ist nur mit vorheriger Zustimmung des Verantwortlichen zulässig und darf nur bei Erfüllung der speziellen Anforderungen der Art. 44 ff. der DSGVO stattfinden.

## 3 - Technische und organisatorische Maßnahmen

**3.1** Der Auftragsverarbeiter hat die Sicherheit nach Art. 28 Abs. 3 lit. c, gemäß Art. 32 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 zu berücksichtigen (Siehe **Anlage 2**).

**3.2** Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Daher ist es dem Auftragsverarbeiter erlaubt, alternative adäquate Maßnahmen umzusetzen, solange das festgelegte Sicherheitsniveau nicht dauerhaft unterschritten wird. Wesentliche Änderungen werden dokumentiert.

## 4 - Auskunft, Berichtigung, Löschung und Rückgabe von personenbezogenen Daten

**4.1** Der Auftragsverarbeiter kann im Auftrag des Verantwortlichen während der Vertragslaufzeit die vertragsgegenständlichen personenbezogenen Daten berichtigen oder löschen, wenn der Verantwortliche dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragsverarbeiter die datenschutzkonforme Vernichtung von Datenträgern oder sonstigen Materialien auf Grund einer

Einzelbeauftragung durch den Verantwortlichen. Für die Erbringung dieser Unterstützungsleistungen kann der Auftragsverarbeiter ein Entgelt je angefangener Arbeitsstunde berechnen.

**4.2** Der Auftragsverarbeiter ist berechtigt, insbesondere die zur Bedrohungsanalyse vom CAPTCHA-Dienst verarbeiteten personenbezogenen Daten, jederzeit zu löschen oder zu anonymisieren. Dies dient der Reduzierung der verarbeiteten Datenmenge und der Sicherstellung der Effizienz des CAPTCHA-Dienstes.

**4.3** Der Auftragsverarbeiter unterstützt den Verantwortlichen nach besten Kräften bei der Erfüllung der Rechte betroffener Personen (Art. 28 Abs. 3 lit. e DSGVO) und stellt sicher, dass die erforderlichen technischen und organisatorischen Maßnahmen zur Erfüllung dieser Anfragen vorhanden sind.

**4.4** Wendet sich eine betroffene Person zwecks Auskunft, Berichtigung oder Löschung an den Auftragsverarbeiter, wird der Auftragsverarbeiter die betroffene Person an den Verantwortlichen verweisen und leitet den Antrag an den Verantwortlichen weiter. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung von Anträgen betroffener Personen in angemessenem Umfang. Anfragen für Unterstützung hat der Verantwortliche in Textform an den Auftragsverarbeiter zu stellen und diesem die entstehenden Kosten zu erstatten.

**4.5** Nach Beendigung der Dienstleistung löscht der Auftragsverarbeiter, nach Weisung des Verantwortlichen, alle personenbezogenen Daten oder gibt diese dem Verantwortlichen zurück, sofern keine gesetzlichen Aufbewahrungspflichten dem entgegenstehen.

## 5 - Weisungsbefugnis des Verantwortlichen und Pflichten des Auftragsverarbeiters

**5.1** Der Auftragsverarbeiter darf personenbezogene Daten, die Gegenstand des Auftrags sind, nur im Rahmen des Auftrages und der Weisungen des Verantwortlichen verarbeiten, außer es liegt ein Ausnahmefall des Art. 28 Abs. 3 lit. a DSGVO vor. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragsverarbeiter darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Verantwortlichen bestätigt oder abgeändert wurde.

**5.2** Weisungen vom Verantwortlichen muss der Auftragsverarbeiter dokumentieren.

**5.3** Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mindestens Textform).

**5.4** Erteilt der Verantwortliche dem Auftragsverarbeiter Weisungen, die über die vertraglich vereinbarten Leistungen hinausgehen oder unvorhergesehene zusätzliche Maßnahmen erfordern, so hat der Verantwortliche die dadurch entstehenden Kosten zu erstatten.

**5.5** Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO. Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die zur Vertraulichkeit verpflichtet wurden. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

**5.6** Der Auftragsverarbeiter stellt die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen (Siehe **Anlage 2**) sicher.

**5.7** Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

**5.8** Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich 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 Auftragsverarbeiter ermittelt.

**5.9** Soweit der Verantwortliche 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach Möglichkeit zu unterstützen.

**5.10** Der Auftragsverarbeiter 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.

## 6 - Pflichten des Verantwortlichen

**6.1** Der Verantwortliche hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er Verstöße des Auftragsverarbeiters gegen datenschutzrechtliche Bestimmungen feststellt.

**6.2** Verantwortlich für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung, sowie für die Wahrung der Rechte von Betroffenen ist allein der Verantwortliche.

## 7 - Mitteilung bei Verstößen des Auftragsverarbeiters

**7.1** Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Bekanntwerden, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Verantwortlichen bekannt werden. Eine Meldung von Datenschutzverletzungen enthält mindestens:

- eine Beschreibung des Vorfalls, soweit möglich mit Angabe der Art der Verletzung des Schutzes personenbezogener Daten, Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
- Kontaktdaten einer Anlaufstelle für weitere Informationen
- eine Beschreibung der wahrscheinlichen Folgen des gemeldeten Vorfalls, eine Beschreibung der ergriffenen Maßnahmen zur Behebung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

**7.2** Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten, einschließlich der Sicherheit personenbezogener Daten, der Meldung von Datenschutzverletzungen, der Durchführung von Datenschutz-Folgenabschätzungen und der vorherigen Konsultation mit Aufsichtsbehörden. Hierzu gehören insbesondere:

- Implementierung und Aufrechterhaltung angemessener technischer und organisatorischer Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus (Siehe **Anlage 2**).
- Unverzügliche Meldung von Datenschutzverletzungen an die zuständige Aufsichtsbehörde.
- Information der betroffenen Personen über Datenschutzverletzungen, wenn diese voraussichtlich ein hohes Risiko für deren Rechte und Freiheiten darstellen.
- Durchführung von Datenschutz-Folgenabschätzungen, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.
- Konsultation der Aufsichtsbehörde vor der Verarbeitung, wenn aus der Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko darstellt.

## 8 - Kontrollrechte

Der Auftragsverarbeiter weist, nach Anforderung des Verantwortlichen, diesem die Einhaltung der in diesem Vertrag niedergelegten Pflichten nach, jedoch nicht mehr als einmal pro Kalenderjahr. Dies betrifft insbesondere den Nachweis über die Umsetzung der technischen und organisatorischen Maßnahmen. Dieser Nachweis erfolgt durch Zertifizierungen oder Berichte interner oder externer Prüfer, sowie durch Inspektionen in besonderen Fällen. Prüfungen müssen ohne Störung des Betriebsablaufs sowie unter Wahrung der Sicherheits- und Vertraulichkeitsinteressen des Auftragsverarbeiters durchgeführt werden. Prüfungen haben nur innerhalb üblicher Geschäftszeiten zu erfolgen und sind mindestens 14 Tage vorab anzukündigen.

## 9 - Unterauftragsverhältnisse

**9.1** Ein Unterauftragsverhältnis im Rahmen dieses Vertrags sind solche Leistungen, bei denen der Auftragsverarbeiter weitere Unterauftragsverarbeiter mit der Verarbeitung von im Vertrag vereinbarten personenbezogenen Daten, die im direkten Bezug zur Erbringung der Hauptdienstleistung stehen, beauftragt.

**9.2** Ein Unterauftragsverhältnis erfordert, dass der Unterauftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt bekommt, die in dem Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt.

**9.3** Der Verantwortliche stimmt den in **Anlage 1** aufgeführten, bereits beauftragten Unterauftragsverarbeitern zu.

**9.4** Der Verantwortliche stimmt zu, dass der Auftragsverarbeiter Unterauftragsverarbeiter hinzuzieht oder ersetzt. Vor Hinzuziehung oder Ersetzung der Unterauftragsverarbeiter zeigt der Auftragsverarbeiter dem Verantwortlichen Änderungen, mit einer angemessenen Frist, schriftlich oder in Textform an. Im Falle eines Einspruchs des Verantwortlichen steht dem Auftragsverarbeiter das Recht zur außerordentlichen Kündigung dieser Vereinbarung sowie des zugrundeliegenden Servicevertrags zu.

**9.5** Wenn der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb der EU oder des EWR erbringt, ist der Auftragsverarbeiter dafür verantwortlich, dass die datenschutzrechtlichen Anforderungen durch geeignete Maßnahmen erfüllt werden.

## 10 - Sonstiges

**10.1** Der Verantwortliche ist verpflichtet, alle im Rahmen dieses Vertragsverhältnisses erlangten Kenntnisse über Geschäftsgeheimnisse und Datensicherheitsmaßnahmen des Auftragsverarbeiters als vertraulich zu behandeln. Diese Verpflichtung gilt auch nach Beendigung dieses Vertrags. Sollten Zweifel bestehen, ob eine Information der Geheimhaltungspflicht unterliegt, so ist diese Information bis zur schriftlichen Freigabe durch den Auftragsverarbeiter als vertraulich zu behandeln.

**10.2** Sollten die Daten des Verantwortlichen beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich darüber zu informieren.

**10.3** Änderungen und Ergänzungen dieses Vertrags und aller ihrer Bestandteile, einschließlich etwaiger Zusicherungen des Auftragsverarbeiters, bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

**10.4** Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

**10.5** Es gilt das Recht der Bundesrepublik Deutschland.

**10.6** Gerichtsstand ist das Gericht am Sitz des Anbieters und damit München.

## Anlage 1: Unterauftragsverarbeiter

**Hetzner Online GmbH**

Hetzner Online GmbH
Industriestr. 25, 91710 Gunzenhausen, Deutschland
Server-Hosting und IT-Infrastruktur

**netcup GmbH**

netcup GmbH
Daimlerstraße 25, 76185 Karlsruhe, Deutschland
Server-Hosting und IT-Infrastruktur

## Anlage 2: Technische und organisatorische Maßnahmen

**1 - Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)**

**1.1 Zutrittskontrolle:**

Rechenzentrumsräume:

- Trustcaptcha Kundendaten werden in gesicherten Cloud-Rechenzentren innerhalb der europäischen Union verarbeitet und gespeichert
- Alle von uns genutzten Rechenzentren werden von europäischen Unternehmen betrieben
- Alle Rechenzentrumsbetreiber sind nach Industriestandards wie ISO/IEC 27001 zertifiziert und haben mit uns Auftragsverarbeitungsverträge abgeschlossen, die u.a. den Zugang zu unseren IT-Systemen regeln und beschränken
- Zutritt zu Räumen, in denen sich Datenverarbeitungsanlagen befinden, ist Unbefugten verwehrt

**1.2 Zugangskontrolle:**

- Der Benutzer- und Administratorzugriff auf das Trustcaptcha-System beruht auf einem Zugriffsberechtigungsmodell. Jeder Nutzer erhält eine eindeutige ID, sodass alle Systemkomponenten nur von berechtigten Benutzern und Administratoren genutzt werden können
- Es existieren Richtlinien zur Passwortkomplexität
- Passworteingabe erforderlich für Anmeldung
- Es existieren Vorgaben zur Nutzung von Zwei-Faktor-Authentifizierung (2FA)
- Bei Trustcaptcha gilt das Prinzip der Minimalberechtigung. Jeder Benutzer erhält nur die, für die Durchführung seiner vertraglichen Tätigkeiten erforderlichen Zugriffsrechte.
- Benutzerkonten werden zunächst immer mit den wenigsten Zugriffsrechten ausgestattet.
- Für die Einräumung von Zugriffsrechten über die Minimalberechtigung hinaus, muss eine entsprechende Berechtigung vorliegen
- Monitoring von kritischen Systemen
- Einsatz von Firewall-Systemen auf CAPTCHA-Serversystemen
- Der Zugriff auf Trustcaptcha Serversysteme erfolgt SSH-verschlüsselt

**1.3 Zugriffskontrolle:**

- Zugriffsberechtigung auf Trustcaptcha Produktivsysteme ist auf einen kleinen Kreis von Mitarbeitern (Trustcaptcha Systemadministratoren) beschränkt
- Es existiert ein internes Kontrollsystem, das die Rechtmäßigkeit für Zugriffe auf Trustcaptcha Produktivsysteme stichprobenartig überprüft

**1.4 Trennungskontrolle:**

- Test- und Produktivdaten sind in strikt unabhängigen Systemen getrennt
- Entwicklungssysteme sind unabhängig von Test- und Produktivsystemen
- Unterschiedliche Domains und SSL-Zertifikate für Test- und Produktivsysteme

**1.5 Pseudonymisierung**

- Pseudonymisierung oder Anonymisierung von personenbezogenen Daten auf Systemen soweit möglich

**2 - Integrität (Art. 32 Abs. 1 lit. b DSGVO)**

**2.1 Eingabe- und Weitergabekontrolle:**

- Übertragung personenbezogener Daten zwischen Trustcaptcha Systemen erfolgt innerhalb gesicherter Subsysteme
- Soweit Daten zu beauftragten Partnern übertragen werden, sind diese Datenübertragungskanäle TLS verschlüsselt
- Wo kritischer Zugriff auf Produktivsysteme möglich ist, existieren Richtlinien zum Einsatz von VPN-Verbindungen
- Datenabrufe und Übermittlungsaktivitäten werden protokolliert

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

**3.1 Verfügbarkeitskontrolle:**

- Es werden regelmäßig automatische Sicherungskopien und Backups der Trustcaptcha Kundendaten erstellt
- Es gibt ein Konzept zur Rekonstruktion der Datenbestände und zudem eine regelmäßige Überprüfung, dass die Datensicherungen auch tatsächlich wieder eingespielt werden können
- Trustcaptcha Produktivsysteme sind mehrfach redundant ausgelegt

**3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO):**

- Mehrfach-redundante Auslegung von Serversystemen
- Backups werden regelmäßig auf Wiedereinspielbarkeit geprüft
- Es werden Notfallübungen durchgeführt, in denen Wiederherstellungsszenarien geübt werden

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

**4.1 Maßnahmen:**

- Trustcaptcha verfügt über Datenschutzmanagementvorgaben. Die Überwachung und Bewertung, findet fortlaufend statt.
- Datenschutzfreundliche Voreinstellungen werden bei der Softwareentwicklung berücksichtigt (Art. 25 Abs. 2 DSGVO)

**4.2 Auftragskontrolle:**

- Abschluss von Auftragsverarbeitungsverträgen gemäß Art. 28 DSGVO
- Verhinderung von Zugriffen unbefugter Dritter auf personenbezogene Daten
- Auswahl der Dienstleister nach strengen Kriterien
- Regelmäßige Überprüfungen der Unterauftragsverarbeiter

## Hinweise zum Vertragsabschluss

Vertragsversion: 24.11.1

Der Vertrag wurde von folgendem Nutzer auf eigene Initiative auf der Trustcaptcha Online-Website abgeschlossen.

John Doe (john@doe.com), 2025-02-13 13:07:41 UTC

Der Vertragsabschluss wurde von uns elektronisch anerkannt und der Vertrag im PDF-Format generiert. Der unterzeichnete Vertrag wurde dem jeweiligen Nutzer per E-Mail zugesandt und steht auf unserer Website für alle berechtigten Nutzer zum Download bereit.

# Data processing agreement

Between

Example Ltd., Street 1, 12345 City, Country
- hereinafter referred to as the controller -

and

Trustcaptcha GmbH, Hans-Böckler-Straße 32, 80995 Munich, Germany
- hereinafter referred to as the processor -

the following provisions apply to data processing.

## 1 - Subject matter and duration of the order processing

### 1.1 Object

The main object is the provision of a Software-as-a-Service (SaaS) online service known as CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). The services covered by this contract extend to the provision, operation, maintenance, support, analysis and improvement of the CAPTCHA service.

This contract supplements the service contract (hereinafter referred to as the main contract) between the controller and the processor. The contract takes precedence over the main contract when it comes to the fulfilment of regulatory requirements in the area of data protection or data security in accordance with the GDPR and only in relation to the respective fields in which personal data is processed.

### 1.2 Duration

The duration (term) of this contract corresponds to the term of the main contract, but at least for as long as the processor processes personal data for the controller. In addition, the parties agree that all previous data processing contracts shall be cancelled by mutual agreement upon conclusion of this contract.

## 2 - Specification of the data processing

### 2.1 Purpose and type of processing

The processor processes personal data for the controller within the meaning of Art. 4 No. 2 GDPR on the basis of the contract. The purpose of the data processing is the protection of companies through the security mechanisms of the Trustcaptcha CAPTCHA service and the provision of additional functions. Trustcaptcha analyses data from CAPTCHA requests to provide threat detection. Trustcaptcha also processes data to offer related extended functions. In particular, the data may be: collected, stored, organised, modified, read out, queried, used, disclosed, compared, linked and deleted.

### 2.2 Object of the processing

The object of processing by the CAPTCHA service is usage/behavioural data, device data, connection data and location data. Depending on the user's device and settings, this includes, for example, information on device properties and device data (e.g. device and device type, operating system, plugins, screen size, hardware), IP

address, referrer website, automatically transmitted cookies, behavioural data such as mouse and keyboard behaviour or touches on touch devices, as well as settings (e.g. language). This data may be stored temporarily for threat detection, compared with other information such as time, general location information and IP allow /block lists and analysed. Some data may be stored temporarily to further develop the protection mechanisms. Data collection by CAPTCHA is limited to technical, behavioural and statistical aspects; no content-related input is evaluated. The data processed by the CAPTCHA service is processed exclusively for the purposes of CAPTCHA verification and to be reliably prepared for future threats. The data is also processed to provide the controller with statistics and usage information. Other data may also be processed in the future to provide effective protection in the event of changing requirements and framework conditions, as well as through the addition of new functions.

**2.3 Categories of data subjects**

The processing concerns:

- Persons who trigger the evaluation (bot verification) of a CAPTCHA field

**2.4** The contractually agreed data processing of personal data is carried out in a member state of the European Union or in another state party to the agreement on the European Economic Area. A transfer to a third country is only permitted with the prior consent of the controller and may only take place if the special requirements of Art. 44 et seq. of the GDPR are met.

## 3 - Technical and organisational measures

**3.1** The processor must establish security in accordance with Art. 28 para. 3 lit. c, pursuant to Art. 32 GDPR. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons must be considered (see **Annex 2**).

**3.2** The technical and organisational measures are subject to technical progress and further development. Therefore, the processor is permitted to implement alternative adequate measures if the specified security level is not permanently undercut. Significant changes are documented.

## 4 - Access, rectification, erasure and return of personal data

**4.1** The processor may rectify or erase the personal data covered by the contract on behalf of the controller during the term of the contract if the controller so instructs and this is covered by the scope of the instructions. If deletion in compliance with data protection regulations or a corresponding restriction of data processing is not possible, the processor shall undertake the destruction of data carriers or other materials in compliance with data protection regulations on the basis of an individual order from the controller. For the provision of these support services, the processor may charge a fee per hour of work or part thereof.

**4.2** The processor shall be entitled to delete or anonymise the personal data processed by the CAPTCHA service for threat analysis purposes in particular at any time. This is essential to reduce the amount of data processed and to ensure the efficiency of the CAPTCHA service.

**4.3** The processor shall support the controller to the best of its ability in fulfilling the rights of data subjects (Art. 28 para. 3 lit. e GDPR) and shall ensure that the necessary technical and organisational measures are in place to fulfil these requests.

**4.4** If a data subject contacts the processor for access, rectification or erasure, the processor shall refer the data subject to the controller and forward the request to the controller. The processor shall support the controller in the fulfilment of requests from data subjects to a reasonable extent. Requests for support shall be made by the controller in textual form to the processor and the processor shall be reimbursed for any costs incurred.

**4.5** After completion of the service, the processor shall delete all personal data or return it to the controller as instructed by the controller, provided that there are no statutory retention obligations to the contrary.

## 5 - Authorisation of the controller to issue instructions and obligations of the processor

**5.1** The processor may only process personal data that is the subject of the order within the scope of the order and the instructions of the controller, unless there is an exceptional case pursuant to Art. 28 para. 3 lit. a GDPR. The processor shall inform the controller immediately if it is of the opinion that an instruction violates applicable laws. The processor may suspend the implementation of the instruction until it has been confirmed or amended by the controller.

**5.2** Instructions from the controller must be documented by the processor.

**5.3** The controller shall confirm verbal instructions immediately (at least in text form).

**5.4** If the controller issues instructions to the processor that go beyond the contractually agreed services or require unforeseen additional measures, the controller shall reimburse the costs incurred as a result.

**5.5** Maintaining confidentiality in accordance with Art. 28 para. 3 lit. b, Art. 29, Art. 32 para. 4 GDPR. When carrying out the work, the processor shall only use employees who have been obliged to maintain confidentiality. The processor and any person subordinate to the processor who has access to personal data may only process this data in accordance with the controller's instructions, including the authorisations granted in this agreement, unless they are legally obliged to do so.

**5.6** The processor shall ensure the implementation of and compliance with all technical and organisational measures required for this contract (see **Annex 2**).

**5.7** The controller and the processor shall co-operate with the supervisory authority in the performance of their duties upon request.

**5.8** The processor shall inform the controller without undue delay of any inspection activities and measures of the supervisory authority insofar as they relate to this order. This shall also apply if a competent authority investigates the processor in the context of administrative offence or criminal proceedings relating to the processing of personal data during commissioned processing.

**5.9** If the controller is subject to an inspection by the supervisory authority, administrative offence or criminal proceedings, a liability claim by a data subject or a third party or any other claim in connection with the commissioned processing at the processor, the processor shall support the controller as far as possible.

**5.10** The processor shall regularly monitor the internal processes and the technical and organisational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.

## 6 - Obligations of the controller

**6.1** The controller must inform the processor immediately and in full if it discovers any breaches of data protection provisions by the processor.

**6.2** The controller shall be solely responsible for assessing the permissibility of the commissioned processing and for safeguarding the rights of data subjects.

## 7 - Notification of breaches by the processor

**7.1** The processor shall notify the controller without undue delay, but at the latest within 48 hours of becoming aware of any breaches of the controller's personal data protection. A notification of data breaches shall contain at least:

- a description of the incident, including, where possible, the nature of the personal data breach, the categories and approximate number of data subjects concerned, the categories concerned and the approximate number of personal data records concerned
- contact details of a contact point for further information
- a description of the likely consequences of the reported incident, a description of the measures taken to remedy it and, where appropriate, measures to mitigate its possible adverse effects

**7.2** The processor shall assist the controller in complying with the obligations set out in Articles 32 to 36 of the GDPR, including the security of personal data, the notification of data breaches, the performance of data protection impact assessments and prior consultation with supervisory authorities. This includes in particular:

- Implementing and maintaining appropriate technical and organisational measures to ensure a level of protection appropriate to the risk (See **Annex 2**).
- Immediate notification of data breaches to the competent supervisory authority.
- Informing data subjects about data breaches if these are likely to pose a high risk to their rights and freedoms.
- Carrying out data protection impact assessments if processing is likely to result in a high risk to the rights and freedoms of natural persons.
- Consultation of the supervisory authority prior to processing if the data protection impact assessment indicates that the processing poses a high risk.

## 8 - Control rights

The processor shall, at the request of the controller, provide evidence of compliance with the obligations set out in this contract, but no more than once per calendar year. This applies in particular to proof of the implementation of technical and organisational measures. This proof is provided by means of certifications or reports by internal or external auditors, as well as by inspections in special cases. Audits must be carried out without disrupting operations and with due regard for the security and confidentiality interests of the processor. Audits must only be carried out during normal business hours and must be announced at least 14 days in advance.

## 9 - Subcontracts

**9.1** A subcontract within the scope of this agreement is one in which the processor commissions other sub-processors to process personal data agreed in the agreement that is directly related to the provision of the main service.

**9.2** A subcontracting relationship requires that the sub-processor be subject to the same data protection obligations as those laid down in the contract between the controller and the processor by means of a contract or other legal instrument under union law or the law of the member state concerned, in particular providing sufficient guarantees that the appropriate technical and organisational measures are implemented in such a way that the processing is carried out in accordance with the requirements of this regulation.

**9.3** The controller consents to the sub-processors already engaged as listed in **Annex 1**.

**9.4** The controller agrees that the processor may involve or replace sub-processors. Before involving or replacing the sub-processors, the processor shall notify the controller of any changes in writing or in text form with a reasonable period of notice. In the event of an objection by the controller, the processor shall have the right to extraordinary termination of this agreement and the underlying Service agreement.

**9.5** If the sub-processor provides the agreed service outside the EU or the EEA, the processor shall be responsible for ensuring that the data protection requirements are met by taking appropriate measures.

## 10 - Miscellaneous

**10.1** The controller is obliged to treat as confidential all knowledge of the processor's business secrets and data security measures obtained within the scope of this contractual relationship. This obligation shall also apply after termination of this contract. If there is any doubt as to whether information is subject to the confidentiality obligation, this information shall be treated as confidential until it has been released in writing by the processor.

**10.2** Should the controller's data be jeopardised by seizure or confiscation, by insolvency or composition proceedings or by other events or measures by third parties, the processor shall inform the controller of this immediately.

**10.3** Amendments and supplements to this agreement and all its components, including any assurances given by the processor, shall require a written agreement, which may also be in an electronic format (text form) and an express reference to the fact that it is an amendment or supplement to this contract. This also applies to the waiver of this formal requirement.

**10.4** Should individual parts of this contract be invalid, this shall not affect the validity of the remainder of the contract.

**10.5** The law of the Federal Republic of Germany shall apply.

**10.6** The place of jurisdiction shall be the court at the registered office of the processor and therefore Munich.

## Annex 1: Subcontracted processors

**Hetzner Online GmbH**

Hetzner Online GmbH
Industriestr. 25, 91710 Gunzenhausen, Germany
Server hosting and IT infrastructure

**netcup GmbH**

netcup GmbH
Daimlerstraße 25, 76185 Karlsruhe, Germany
Server hosting and IT infrastructure

## Annex 2: Technical and organisational measures

**1 - Confidentiality (Art. 32 para. 1 lit. b GDPR)**

**1.1 Physical access control:**

Data centre rooms:

- Trustcaptcha CAPTCHA data is processed and stored in secure cloud data centres within the European Union
- All of the data centres we use are operated by European companies
- All data centre operators are certified in accordance with industry standards such as ISO/IEC 27001 and have concluded order processing contracts with us which, among other things, regulate and restrict access to our IT systems
- Unauthorised persons are denied access to rooms in which data processing systems are located

**1.2 Electronic access control:**

- User and administrator access to the Trustcaptcha system is based on an access authorisation model. Each user receives a unique ID so that all system components can only be used by authorised users and administrators
- There are guidelines for password complexity
- Password entry required for login
- There are guidelines for the use of two-factor authentication (2FA)
- The principle of minimum authorisation applies to Trustcaptcha. Each user only receives the access rights required to fulfil their contractual activities.
- User accounts are initially always assigned the fewest access rights.
- In order to grant access rights beyond the minimum authorisation, a corresponding authorisation must be available
- Monitoring of critical systems
- Use of firewall systems on CAPTCHA server systems
- Access to Trustcaptcha server systems is SSH-encrypted

**1.3 Access control:**

- Access authorisation to Trustcaptcha production systems is restricted to a small group of employees (Trustcaptcha system administrators)
- There is an internal control system that randomly checks the legitimacy of access to Trustcaptcha production systems

**1.4 Separation control:**

- Test and production data are separated in strictly independent systems
- Development systems are independent of test and production systems
- Different domains and SSL certificates for test and production systems

**1.5 Pseudonymisation**

- Pseudonymisation or anonymisation of personal data on systems as far as possible

**2 - Integrity (Art. 32 para. 1 lit. b GDPR)**

**2.1 Input and transfer control:**

- Transfer of personal data between Trustcaptcha systems takes place within secure subsystems
- Where data is transferred to authorised partners, these data transfer channels are TLS encrypted
- Where critical access to production systems is possible, there are policies for the use of VPN connections
- Data retrieval and transmission activities are logged

**3 - Availability and resilience (Art. 32 para. 1 lit. b GDPR)**

**3.1 Availability control:**

- Automatic backup copies and backups of Trustcaptcha CAPTCHA data are created regularly
- There is a concept for the reconstruction of the data and a regular check that the data backups can actually be restored
- Trustcaptcha production systems are designed with multiple redundancies

**3.2 Rapid recoverability (Art. 32 para. 1 lit. c GDPR):**

- Multiple redundant design of server systems
- Backups are regularly checked for recoverability
- Emergency exercises are carried out in which recovery scenarios are practised

**4 - Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)**

**4.1 Measures:**

- Trustcaptcha has data protection management guidelines. Monitoring and evaluation takes place on an ongoing basis.
- Data protection-friendly default settings are taken into account in software development (Art. 25 para. 2 GDPR)

**4.2 Order control:**

- Conclusion of data processing agreements in accordance with Art. 28 GDPR
- Prevention of access to personal data by unauthorised third parties
- Selection of service sub-processors according to strict criteria
- Regular checks of subcontracted processors

## Notes on the contract conclusion

Contract version: 24.11.1

The contract was concluded by the following user on his own initiative on the Trustcaptcha Online website.

John Doe (john@doe.com), 2025-02-13 13:07:41 UTC

The conclusion of the contract was recognised by us electronically and the contract was generated in PDF format. We have sent the signed contract to the relevant user by e-mail and it is available for download on our website for all authorised users.