Vereinbarung über eine Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:
die jeweilige Kundin bzw. der jeweilige Kunde des Auftragsverarbeiters, die bzw. der mit dem Auftragnehmer einen Vertrag über die nachstehend genannten Leistungen geschlossen hat

– nachfolgend Auftraggeber genannt – und

Der Auftragsverarbeiter:
die Komplizinnen OG
Zollergasse 37/10
1070 Wien

– nachfolgend Auftragnehmer genannt – wird folgender Vertrag geschlossen:

Die Regelungen zu Hosting und Captcha-Dienst gelten nur, sofern diese Leistungen zwischen den Parteien vereinbart sind. Stand: 11/2026

1. Gegenstand der Vereinbarung

1.1 Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben: Entwicklung, Pflege und Wartung von Websites. Test- und Entwicklungsversionen der Websites werden dabei auf Servern der hosttech GmbH betrieben.

1.2 Zusätzlicher Gegenstand dieses Auftrages sind Internetdienstleistungen (Hosting) im Rahmen der vom Auftragnehmer auf seinen Internetseiten angebotenen und in den jeweiligen Leistungsbeschreibungen konkretisierten Produkten. Insoweit ist diese Vereinbarung als Ergänzung zu den Hosting AGB von die Komplizinnen OG zu verstehen.

1.3 Zur Abwicklung von Support-Anfragen betreibt der Auftragnehmer ein eigenes Helpdesk-System auf Basis der Software Zammad.

1.4 Zusätzlich stellt der Auftragnehmer dem Auftraggeber einen selbst betriebenen Captcha-Dienst zum Schutz der Formulare der Website vor automatisierten Zugriffen (Spam, Bots) zur Verfügung. Eingesetzt wird die Open-Source-Software Cap, die auf einem Proof-of-Work-Verfahren basiert und ohne Cookies, Tracking oder Profilbildung auskommt. Einzelheiten sind der Anlage 4 zu entnehmen.

1.5 Folgende Datenkategorien werden verarbeitet: Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bestelldaten, alle weiteren in der Website und deren Datenbanken gespeicherten Daten, Nutzungs- und Verbindungsdaten (z. B. IP-Adressen in Server-Logfiles), Inhalte von Support-Anfragen (Tickets und E-Mail-Korrespondenz im Helpdesk-System), technische Verbindungsdaten der Besucher*innen beim Captcha-Dienst (IP-Adresse, Zeitstempel, Browserkennung, Challenge- und Token-Daten).

1.6 Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: Kunden, Interessenten, Lieferanten, Ansprechpartner & Geschäftspartner sowie Besucher*innen und Nutzer*innen der Website des Auftraggebers.

2. Zustandekommen und Dauer der Vereinbarung

2.1 Diese Vereinbarung kommt durch Unterzeichnung durch beide Parteien oder durch Annahme des Auftraggebers per E-Mail an den Auftragnehmer zustande, in der der Auftraggeber unter Bezugnahme auf diese Vereinbarung deren Annahme erklärt. Die Annahme per E-Mail erfüllt das Erfordernis der Schriftform in elektronischem Format gemäß Art 28 Abs 9 DSGVO.

2.2 Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von einem Monat jederzeit gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Pflichten des Auftragnehmers

3.1 Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er – sofern gesetzlich zulässig – den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

3.2 Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

3.3 Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage 1 sowie den technisch-organisatorischen Maßnahmen der Sub-Auftragsverarbeiter in den weiteren Anlagen zu entnehmen).

3.4 Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

3.5 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

3.6 Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

3.7 Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

3.8 Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

3.9 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, dass eine Weisung des Auftraggebers gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

4. Rechte und Pflichten des Auftraggebers

4.1 Für die Beurteilung der Zulässigkeit der Datenerhebung / -verarbeitung / -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

4.2 Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und schriftlich festzulegen.

4.3 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

4.4 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

5. Ort der Durchführung der Datenverarbeitung

5.1 Die Datenverarbeitung erfolgt grundsätzlich innerhalb der EU bzw. des EWR. Davon ausgenommen ist das Helpdesk-System (Zammad), das auf einem Server der Hostinger International Ltd. in einem Rechenzentrum im Vereinigten Königreich (England) betrieben wird. Für das Vereinigte Königreich besteht ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Art 45 DSGVO, eine Übermittlung dorthin ist daher ohne weitere Genehmigung zulässig. Die Server der hosttech GmbH, auf denen die Websites des Auftraggebers sowie Test- und Entwicklungsversionen betrieben werden, stehen in einem Rechenzentrum in Wien (Österreich). Der Captcha-Dienst wird auf einem Server der Hostinger International Ltd. in einem Rechenzentrum in Frankreich (EU) betrieben.

5.2 Bei den Sub-Auftragsverarbeitern Microsoft, Slack, Notion und Anthropic kann eine Verarbeitung bzw. ein Zugriff auch in Drittländern, insbesondere in den USA, erfolgen. Eine solche Übermittlung erfolgt nur, wenn die Voraussetzungen der Art 44 ff DSGVO erfüllt sind, und zwar auf Grundlage des Angemessenheitsbeschlusses der Europäischen Kommission zum EU-US Data Privacy Framework (Art 45 DSGVO), soweit der jeweilige Anbieter danach zertifiziert ist, und/oder auf Grundlage der von der Europäischen Kommission erlassenen Standardvertragsklauseln (Art 46 Abs 2 lit c DSGVO).

6. Sub-Auftragsverarbeiter

6.1 Der Auftragnehmer ist befugt, folgende Unternehmen als Sub-Auftragsverarbeiter hinzuzuziehen, um die notwendige Infrastruktur bereitstellen zu können:

hosttech GmbH
Warwitzstrasse 9
5020 Salzburg, Österreich
Leistung: Server-Infrastruktur für Test- und Entwicklungsumgebungen sowie Webhosting der Websites des Auftraggebers, Rechenzentrum in Wien

Hostinger International Ltd.
61 Lordou Vironos Street
6023 Larnaca, Zypern
Leistung: Server für das Helpdesk-System Zammad, Rechenzentrum in England (Vereinigtes Königreich)
Leistung: Server für den Captcha-Dienst, Rechenzentrum in Frankreich

Microsoft Ireland Operations Limited
One Microsoft Place, South County Business Park
Leopardstown, Dublin 18, D18 P521, Irland
Leistung: Microsoft 365 (E-Mail-Kommunikation, Kalender, Dateiablage und Dokumentenbearbeitung)

Slack Technologies Limited
Salesforce Tower, 60 R801, North Dock
Dublin, Irland
Leistung: interne Team-Kommunikation zu Projekten und Support-Fällen

Notion Labs, Inc.
685 Market Street
San Francisco, CA 94105, USA
Leistung: Projektdokumentation, Aufgaben- und Wissensverwaltung

Anthropic Ireland, Limited
6th Floor, South Bank House, Barrow Street
Dublin 4, D04 TR29, Irland
Leistung: KI-gestützte Unterstützung bei Softwareentwicklung, Fehleranalyse und Support (Claude)

Die technisch-organisatorischen Maßnahmen der Sub-Auftragsverarbeiter sind den Anlagen zu entnehmen bzw. werden für Microsoft, Slack, Notion und Anthropic auf Anfrage zur Verfügung gestellt.

6.2 Beim Einsatz von KI-Diensten (Anthropic) verwendet der Auftragnehmer ausschließlich Unternehmenszugänge, bei denen der Anbieter vertraglich zusichert, die übermittelten Daten nicht zum Training seiner Modelle zu verwenden. Personenbezogene Daten werden dabei nur übermittelt, soweit dies für die jeweilige Aufgabe erforderlich ist. Es erfolgt keine automatisierte Entscheidungsfindung im Sinne des Art 22 DSGVO.

6.3 Der Auftragnehmer kann darüber hinaus weitere Sub-Auftragsverarbeiter für Wartungsarbeiten / Webentwicklung hinzuziehen. Beabsichtigte Änderungen oder die Heranziehung eines neuen Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann.

6.4 Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

Anlagen

Anlage 1: Technisch-organisatorische Maßnahmen von die Komplizinnen OG
Anlage 2: Technisch-organisatorische Maßnahmen von hosttech GmbH
Anlage 3: Technisch-organisatorische Maßnahmen von Hostinger International Ltd.
Anlage 4: Captcha-Dienst – Leistungsbeschreibung und TOM

ANLAGE 1
technisch-organisatorische Maßnahmen
von die Komplizinnen OG

Vertraulichkeit

Zutrittskontrolle:

Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen:

- Schlüssel
- Alarmanlage

Zugangskontrolle:

Schutz vor unbefugter Systembenutzung:

- Kennwortschutz
- Zwei-Faktor-Authentifizierung bzw. Passkeys für interne Verwaltungssysteme
- verschlüsselte Ablage von Zugangsdaten
- Verschlüsselung von Datenträgern
- teilweise Verschlüsselung von Datenbanken

Zugriffskontrolle:

Zur Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems.

- Schutz vor unberechtigten Zugriffen durch regelmäßige Sicherheitsupdates und Backups
- periodische Überprüfung der vergebenen Berechtigungen

Integrität

Weitergabekontrolle:

Zur Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.

- teilw. Verschlüsselung der Daten
- Übertragung vorzugsweise über verschlüsselte Verbindungen (HTTPS/TLS, SFTP, SSH), teilweise auch über FTP, wenn das Zielsystem keine verschlüsselte Übertragung anbietet

Verfügbarkeit und Belastbarkeit:

- rasche Wiederherstellbarkeit durch Backups
- Löschungsfristen: Sowohl für Daten selbst als auch Metadaten wie Logfiles

Verfügbarkeitskontrolle:

- tägliches Backup der Webserverdaten
- Sicherung aller Verwaltungsdaten mindestens drei mal die Woche
- Festplattenspiegelung
- Monitoring aller relevanten Systeme
- Virenschutz, Firewall, SPAM-Filter

Helpdesk-System (Zammad):

Support-Anfragen werden in einem selbst betriebenen Zammad-System auf einem Server der Hostinger International Ltd. (Rechenzentrum in England, Vereinigtes Königreich) bearbeitet.

- Zugriff ausschließlich über verschlüsselte Verbindungen (HTTPS/TLS)
- persönliche Benutzerkonten mit Rollen- und Rechtevergabe, Zugriff nur für Mitarbeiter*innen des Auftragnehmers
- Administration des Servers ausschließlich durch den Auftragnehmer, regelmäßige Sicherheitsupdates

Cloud-Dienste und KI-Werkzeuge:

- Nutzung von Microsoft 365, Slack, Notion und Claude ausschließlich über Unternehmenskonten mit persönlichen Benutzerkonten und Zwei-Faktor-Authentifizierung
- bei KI-Diensten: kein Training mit übermittelten Daten (vertraglich zugesichert), Übermittlung personenbezogener Daten nur im erforderlichen Umfang
- keine Ablage von Zugangsdaten und Passwörtern in Chat- oder Notiz-Tools

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung:

- Datenschutz-Management
- Datenschutzfreundliche Voreinstellungen
- Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers

ANLAGE 2
technisch-organisatorische Maßnahmen
von hosttech GmbH

Vertraulichkeit

Zutrittskontrolle:

Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen:

- dokumentierte Schlüssel- oder -Chipkartenvergabe
- elektrische Türöffner mit Zutrittsstatistik
- Alarmanlagen
- Videoüberwachung

Zugangskontrolle:

Schutz vor unbefugter Systembenutzung:

- Kennwortschutz (einschließlich entsprechender Policy)
- Zugriff nur für Mitarbeiter von Auftragnehmer
- automatische Sperrmechanismen sofern möglich

Zugriffskontrolle:

Zur Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems.

- Schutz vor unberechtigten Zugriffen durch regelmäßige Sicherheitsupdates und Backups
- Standardprozess für Berechtigungsvergabe
- Protokollierung von Zugriffen
- periodische Überprüfung der vergebenen Berechtigungen

Klassifikationsschema für Daten:

Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

Integrität

Weitergabekontrolle:

Zur Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.

- Mitarbeiter werden regelmäßig im Datenschutzrecht geschult
- Mitarbeiter sind auf das Datengeheimnis verpflichtet

Eingabekontrolle:

- Eingabe der Daten durch den Auftraggeber oder berechtigte Mitarbeiter des Auftragnehmers
- Protokollierung von Änderungen

Verfügbarkeit und Belastbarkeit:

- rasche Wiederherstellbarkeit durch Backups
- Löschungsfristen: Sowohl für Daten selbst als auch Metadaten wie Logfiles

Verfügbarkeitskontrolle:

- Tägliche Sicherung aller relevanten Daten (sofern im Angebot enthalten / gebucht)
- unterbrechungsfreie Stromversorgung (USV)
- Festplattenspiegelung
- Monitoring aller relevanten Systeme
- Virenschutz, Firewall, SPAM-Filter
- Meldewege und Notfallpläne
- Security Checks auf Infrastruktur- und Applikationsebene
- Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern

Datensicherung:

- Physikalische oder logische Trennung der Daten
- Datensicherung physikalisch oder logisch getrennt von Ursprungsdaten

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung:

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen

Auftragskontrolle:

Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers

- eindeutige Vertragsgestaltung
- formalisiertes Auftragsmanagement
- Regelmäßige Mitarbeiterschulungen im Datenschutzrecht
- AGB & Datenschutzerklärung enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers

ANLAGE 3
technisch-organisatorische Maßnahmen
von Hostinger International Ltd.

Vertraulichkeit

Zutrittskontrolle:

Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen:

- Zutrittskontrolle mit Ausweiskarten und Überwachung von Sicherheitsereignissen
- Alarmanlagen und, wo angemessen, Videoüberwachung
- Schutz kritischer Standorte: Überspannungsschutz, Doppelböden, Klimatisierung, Brand- und Rauchmelder, Löschanlagen
- Vernichtung von Papierdokumenten

Zugangskontrolle:

Schutz vor unbefugter Systembenutzung:

- starke Authentifizierungs- und Autorisierungsverfahren
- zentrale Passwortverwaltung mit Vorgaben zu Länge, Komplexität und Ablauf
- VPN-Verschlüsselung für Fernzugriffe auf Unternehmensnetzwerke
- Virenschutz-Management, kontrollierter Zugang zu E-Mail und Internet

Zugriffskontrolle:

Zur Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems.

- rollenbasierte Zugriffsrechte, regelmäßig überprüft nach dem Prinzip der Funktionstrennung
- Zugriff auf Produktivumgebungen nur nach Rolle und Funktion
- Protokollierung von Zugriffen und Datenänderungen, zentrale Audit- und Sicherheitslogs

Trennungskontrolle:

- logische Trennung der Daten über rollenbasierte Zugriffsrechte
- Trennung nach Funktion (Test, Staging, Live)
- Pseudonymisierung und Datenminimierung in Anwendungs-, Debug- und Sicherheitslogs, definierte Aufbewahrungsfristen

Integrität

Weitergabekontrolle:

- Verschlüsselung der internen und externen Kommunikation mit starken kryptografischen Protokollen
- Verschlüsselung gespeicherter personenbezogener Daten (Datenbanken, freigegebene Verzeichnisse), Festplattenverschlüsselung auf Firmenrechnern
- Überwachung von Datenübertragungen auf Vollständigkeit und Richtigkeit

Eingabekontrolle:

- Change- und Release-Management mit Auswirkungsanalyse, Freigaben und Sicherheitsprüfungen

Verfügbarkeit und Belastbarkeit:

- unterbrechungsfreie Stromversorgung, redundante Hardware- und Netzwerksysteme
- Replikation bzw. Sicherung kritischer Daten (Cloud-Backups, Datenbankreplikation)
- Überwachung von Leistung und Verfügbarkeit, Failover-Alarme für kritische Dienste
- DDoS-Schutz, Last- und Stresstests
- geplante Wartung von Software und Infrastruktur inkl. Sicherheitsupdates

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung:

- Penetrationstests kritischer Netzwerke und Plattformen sowie regelmäßige Schwachstellenscans
- Incident-Response-Programm, Meldung von Sicherheitsvorfällen ohne unangemessene Verzögerung
- Vertraulichkeitsverpflichtung und regelmäßige Datenschutz- und Sicherheitsschulungen der Mitarbeiter*innen
- vertragliche Weisungsbindung und regelmäßige Datenschutzprüfungen von Dienstleistern
- regelmäßige Überprüfung der Wirksamkeit der technisch-organisatorischen Maßnahmen

ANLAGE 4
Captcha-Dienst
Leistungsbeschreibung und TOM

Leistungsbeschreibung

Der Auftragnehmer betreibt für den Auftraggeber einen Captcha-Dienst auf Basis der Open-Source-Software Cap (github.com/tiagozip/cap). Das Captcha-Widget auf der Website des Auftraggebers ruft vom Captcha-Server eine Rechenaufgabe ab, die der Browser der Besucher*innen selbstständig löst (Proof-of-Work). Der Captcha-Server prüft die Lösung und stellt ein einmalig gültiges Token aus, das die Website des Auftraggebers beim Absenden des Formulars serverseitig überprüft. Es werden weder Bilderrätsel angezeigt noch Inhalte an Dritte weitergegeben.

Verarbeitete Daten:

- IP-Adresse der Besucher*innen (technisch notwendig für die Verbindung sowie zur Missbrauchsabwehr und Ratenbegrenzung)
- Zeitstempel und technische Request-Daten (z. B. Browserkennung/User-Agent)
- Challenge- und Token-Daten (zufällig erzeugte Werte ohne Personenbezug)

Nicht verarbeitet bzw. nicht eingesetzt werden:

- Cookies, Local Storage oder vergleichbare Speichertechnologien zur Wiedererkennung
- Tracking, Browser-Fingerprinting oder Profilbildung
- Formularinhalte – diese werden ausschließlich an die Website des Auftraggebers übermittelt
- Weitergabe von Daten an Dritte oder Übermittlung in Drittländer

Speicherdauer:
Challenges und Tokens verlieren nach wenigen Minuten bzw. nach einmaliger Verwendung ihre Gültigkeit und werden automatisch gelöscht. Server-Logfiles werden nur kurzfristig zur Fehleranalyse und Missbrauchsabwehr aufbewahrt und anschließend gelöscht.

Infrastruktur

Der Captcha-Server ist ein virtueller Server, der vom Auftragnehmer angemietet und ausschließlich vom Auftragnehmer administriert wird:

Hostinger International Ltd.
61 Lordou Vironos Street
6023 Larnaca, Zypern
Serverstandort: Rechenzentrum in Frankreich (EU)

Mit Hostinger besteht eine Vereinbarung zur Auftragsverarbeitung gemäß Art 28 DSGVO. Die physische Sicherheit des Rechenzentrums (Zutrittskontrolle, Stromversorgung, Brandschutz, Netzwerk) richtet sich nach den technisch-organisatorischen Maßnahmen von Hostinger (Anlage 3).

Technisch-organisatorische Maßnahmen des Captcha-Servers

- Übertragung ausschließlich verschlüsselt (HTTPS/TLS)
- Administrativer Zugang ausschließlich für Mitarbeiter*innen des Auftragnehmers über verschlüsselte Verbindungen mit Schlüssel-Authentifizierung
- Firewall, nur die für den Dienst notwendigen Ports sind erreichbar
- regelmäßige Sicherheitsupdates von Betriebssystem und Software
- Validierung der Tokens nur mit geheimem, websitebezogenem Schlüssel
- Ratenbegrenzung zum Schutz vor Missbrauch
- Datenminimierung: keine dauerhafte Speicherung personenbezogener Daten