

AUFTRAGSVERARBEITUNGSVERTRAG

gem. Artikel 30 Abs. 2 DSGVO

Angaben zum Auftragsverarbeiter:

Online-Dienst Udo Breitbart
Projekt: my-GAESTEBUCH.de
Thüringer Straße 79
36208 Wildeck
Webseite: <https://my-gaestebuch.de>

Angaben zur Person des Datenschutzbeauftragten

Ein externer Datenschutzbeauftragter wurde gem. Artikel 37 DSGVO nicht bestellt.

Angaben zum Auftraggeber (bitte ausfüllen):

Gästebuch-ID:

Name:

Ggf. Organisation:

Straße / Nr.:

PLZ / Ort:

Land:

§1 - Vertragsgegenstand

Vertragsgegenstand ist das Bereitstellen eines Gästebuchs im Internet auf den Server des Auftragsverarbeiter und der damit verbundenen Erhebung, Verarbeitung und/oder Nutzung von persönlichen Daten. Dies erfolgt ausschließlich auf dem Gebiet der Europäischen Union (EU) und damit im Geltungsbereich der EU-Datenschutzgrundverordnung mit Beschluß des Europäischen Parlaments und des Rates vom 27. April 2016 und Geltendmachung ab 25. Mai 2018. Das Gästebuch selbst ist kostenfrei und wird mit Werbeeinblendungen finanziert. Optional kann die Werbung im Gästebuch kostenpflichtig abgeschaltet werden. Der Vertrag wird unbefristet geschlossen und endet mit dem Löschen des Gästebuches, was beide Seiten ohne Begründung jederzeit vornehmen können.

§2 - Angaben zur Datenverarbeitung

(Angaben gemäß Art. 30 Abs. 2 lit. b)

Wir führen für Sie im Auftrag folgende Verarbeitungskategorien durch:

- Speicherung der Vertragsdaten
- Hosting der Gästebücher
- Entwicklung und Wartung des Gästebuchs-Systems

§3 - Angaben zum Kreis der Betroffenen

(Angaben gemäß Art. 30 Abs. 2 lit. c)

Folgende Personenkreise sind von der Datenverarbeitung betroffen:

- Mitarbeiter
- Kunden/Auftraggeber
- Nutzer

§4 - Datenübermittlung an Dritte

(Angaben gemäß Art. 30 Abs. 2 lit. d+e)

Eine Datenübermittlung an Dritte findet nicht statt. Alle Daten der Gästebücher sind aber im Internet öffentlich sichtbar (was Sinn und Zweck ist).

§5 - Speicherdauer

(Angaben gemäß Art. 30 Abs. 2 lit. f)

Die Einträge im Gästebuch werden veröffentlicht, der Auftraggeber kann diese jederzeit im geschlossenen Bereich bearbeiten, editieren, kommentieren oder löschen.

Auf den Server fallen persönliche Daten durch die Serverdienste an, da beispielsweise IP-Adressen als persönliche Daten gelten. Diese werden zum Zwecke der Gefahrenabwehr, Fehlerbereinigung, Fehleranalyse und Strafverfolgung automatisiert bis zu 6 Monate + Backupzeitraum (i.d.R. 14 Tage, maximal 21 Tage) gespeichert und automatisch gelöscht.

Wir speichern Ihre Kontakt- und Vertragsdaten zu Abrechnungszwecken. Darin sind enthalten: Ihr Name, ggf. Firmenname/Organisation, Anschrift, ggf. Bankverbindung, ggf. USt-ID-Nr., ggf. Telefonnummer, ggf. Faxnummer, Emailadresse und eventuell die gebuchten Leistungen. Da die Lagerung dieser Daten durch die Vorschriften zur Finanzbuchhaltung beeinflusst werden, kann die Lagerung im Einzelfall bis zu 13 Jahre nach Beendigung des Vertragsverhältnisses andauern (nur bei Zahlungen an den Auftragsverarbeiter).

§6 - Technische und organisatorische Maßnahmen

1. Die technische und/oder organisatorische Maßnahmen sollen die Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie die Systembelastbarkeit im Zuge der Datenverarbeitung sicherstellen. Aus den angegebenen Maßnahmen muss ein angemessenes Sicherheitsniveau ableitbar sein. Der Auftragsverarbeiter hat den Verantwortlichen bei der Ergreifung technisch-organisatorischer Maßnahmen bestmöglich zu unterstützen.
2. Die TOM entsprechen dem Stand der Technik bei Vertragsschließung. Dieser kann sich im Zeitraum des Vertragsverhältnisses ändern. Dem Auftragsverarbeiter ist es gestattet die TOM durch aktuellere Maßnahmen zu ersetzen, die das Schutzniveau nicht senken.
3. Die TOM sind am Ende dieses Vertrags ausgeführt.

§7 - Vertraulichkeitsvereinbarung

Der Auftragsverarbeiter wird alle im Zuge seines Auftrags erlangten Informationen vertraulich behandeln, soweit andere gesetzliche Pflichten dies nicht verbieten.

§8 - Informationspflichten

(Angaben gemäß Art. 13 Abs. 2 lit. d)

1. Der Kunde/Auftraggeber hat das Recht, sich zwecks Beschwerde an die Datenschutzbehörde zu wenden.

§9 - Verantwortung & Risikoabschätzung

1. Die von uns erhobenen Daten sind im Allgemeinen nicht geeignet, schwere Risiken für Rechte und Freiheiten des Betroffenen darzustellen.
2. Der Auftragsverarbeiter verpflichtet sich, Datenschutzverstöße an die zuständigen Datenschutzbehörden zu melden, sofern diese ermittelbar sind.
3. Der Auftragsverarbeiter verpflichtet sich, dem Art. 24 und 28 der DSGVO zu genügen.
4. Dienstleister des Auftragsverarbeiters, die nicht direkt an der Auftragsdatenverarbeitung beteiligt sind, aber zur Erfüllung des Auftrags benötigt werden, sind von den Regelungen dieses Vertrags nicht betroffen.

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 Datenschutz-Grundverordnung EU 2018

Folgende technische und organisatorische Maßnahmen setzen wir und unsere Dienstleister zum Schutz Ihrer Daten ein:

Maßnahmen zur Vertraulichkeit der Daten

... im Hostway Rechenzentrum Hannover (wo der Server des Gästebuchs-Systems steht) ...

- ext. Gebäudesicherung durch Zäune
- Einlasskontrollsysteme & Personenkontrollen mit Vorlage des Personalausweises
- Türsicherungssysteme mit Chipkarten
- Unterbringung der Server in separaten Racks pro Kunde, jeweils zugangsgesichert mit Schlössern
- Alarmsysteme an den Gebäudeein- und -ausgängen
- Videoüberwachung der Serversäle
- Dokumentation der Zugänge
- Zugangsbeschränkung auf folgende Personengruppen:
 - Mitarbeiter und autorisierte Personen
 - autorisiertes Personal des Rechenzentrums
- Trennung von Serversystemen durch Einsatz von VMs

... in Servern ...

- Protokollierung der Zugriffe auf Server
- Zugriffsbeschränkungen von Administrativen Benutzern nur per SSH Schlüssel
- Zugriffsbeschränkungen von Administrativen Benutzern mit Passwort an der physikalischen Konsole des Servers
- Einsatz von Anti-Virensoftware
- Einsatz von Serverüberwachungssoftware
- Einsatz von Firewalls
- Softwareaktualisierung der Serversysteme alle 2 Stunden
- physikalische Trennung von Server und Backupsystem

... im Büro ...

- Festplattenverschlüsselung der Datenträger nach Stand der Technik
- Zugriffskontrollen auf PCs mit Passwörtern
- Einsatz von Firewalls
- Einsatz von Anti-Virensoftware
- Softwareaktualisierung der Computer
- Einsatz von Schreddern für die Entsorgung von Akten

... bei Dienstleistern/Lieferanten außerhalb des Rechenzentrums ...

- Vertragliche Einhaltung der DSGVO

Maßnahmen zur Integrität der Daten

- Datenübertragung per verschlüsselter Kommunikation bspw. SSH, HTTPS, SFTP, VPN, TLS
- Schutzmaßnahmen gegen Hackangriffe u.a. IDS, autom. Integritätsprüfung der eingesetzten Software, Separierung von System und Anwendungen

Maßnahmen zur Verfügbarkeit und Belastbarkeit

- Einsatz von RAID Systemen
- 24/7 Servermonitoring
- RZ seitiges Notstromaggregat
- Duale Stromversorgung
- Feuer- und Rauchmeldeanlagen
- regelmäßige Sicherung aller Serverdaten auf Backupserver

Maßnahmen zur Sicherung des Datenschutzniveaus

- Die Konzepte zur Absicherung der Server, PCs werden regelmäßig überdacht, sobald neue Techniken oder Sicherheitslücken bekannt werden.
- Schulung und Verpflichtung aller Mitarbeiter zur Einhaltung des Datenschutzes, der Regelungen dieses Vertrages und anderer gesetzlicher Pflichten.

Datum

Unterschrift (Auftraggeber/Kunde)

Datum

Unterschrift (Auftragsverarbeiter/Online-Dienst Breitbart)