Technische und organisatorische Maßnahmen (TOM) — crmbooster

Anlage zum Auftragsverarbeitungsvertrag (Art. 32 DSGVO) **Stoerkens GmbH**, Karl-Birzer-Str. 7, 85521 Ottobrunn, Deutschland Stand: 2026-07-20 · Version 1.0

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

Zutrittskontrolle. Die Systeme werden in Rechenzentren in Deutschland betrieben. Der physische Zutritt wird durch den Hosting-Dienstleister mit den branchenüblichen Maßnahmen (Zutrittsberechtigungen, Protokollierung, Bewachung) sichergestellt.

Zugangskontrolle. Zugriff auf Verwaltungs- und Portalfunktionen ist nur nach Authentifizierung möglich. Es gelten ein Rollen- und Rechtekonzept sowie starke Passwörter. Administrative Zugänge sind auf den erforderlichen Personenkreis beschränkt.

Zugriffskontrolle. Berechtigungen werden nach dem Prinzip der geringsten Rechte vergeben (Rollen im CMS/Backend). Zugangsdaten und Schlüssel (Secrets) werden ausschließlich in einem zentralen Secret-Vault vorgehalten und **nicht** im Quellcode oder in Konfigurationsdateien gespeichert.

Trennungskontrolle. Daten werden mandantenbezogen verarbeitet; Partner- und Kundendaten sind logisch getrennt und je Partner scope-isoliert. Test-/Demo-Umgebung und Produktivumgebung sind getrennt.

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

Weitergabekontrolle. Sämtliche Datenübertragungen erfolgen ausschließlich verschlüsselt über TLS/HTTPS. Zahlungsdaten werden über den PCI-DSS-zertifizierten Zahlungsdienstleister (Stripe) verarbeitet.

Eingabekontrolle. Wesentliche administrative Vorgänge und Änderungen werden protokolliert und sind nachvollziehbar.

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

Regelmäßige Datensicherungen, Betrieb in Deutschland, dokumentierte Wiederherstellungsverfahren sowie Monitoring und eine öffentliche Statusseite (crmbooster.io/status) gewährleisten Verfügbarkeit und Belastbarkeit der Systeme.

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

Eine automatisierte Ende-zu-Ende-Testsuite prüft die Kernfunktionen der Plattform. Änderungen durchlaufen einen definierten Bereitstellungs- und Rücksetzprozess. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) sind als Entwicklungsprinzip verankert (u. a. Auswahl nur der jeweils benötigten Datenfelder).

5. Auftragskontrolle

Mit Unterauftragsverarbeitern bestehen Verträge nach Art. 28 DSGVO. Die eingesetzten Unterauftragsverarbeiter sind in `subprozessoren.md` aufgeführt.

6. Hosting und Speicherung im Ruhezustand

Die Systeme werden bei der Hetzner Online GmbH in Rechenzentren in Deutschland betrieben; Hetzner ist nach ISO/IEC 27001 zertifiziert. Die Datenträger sind gespiegelt ausgelegt (RAID-1, Ausfallsicherheit). Der Zugriff auf Datenbank und Server ist auf authentifizierte Administratoren nach dem Prinzip der geringsten Rechte beschränkt; Zugangsdaten und Schlüssel werden ausschließlich in einem zentralen Vault vorgehalten. Eine vollständige Datenträger-/Volume-Verschlüsselung im Ruhezustand wird derzeit nicht eingesetzt; der Schutz ruhender Daten erfolgt über die vorstehenden Zutritts-, Zugangs- und Zugriffskontrollen. Die Übertragung erfolgt ausschließlich verschlüsselt (TLS/HTTPS, siehe Ziffer 2).

Technical and organisational measures (TOM) — crmbooster (English translation)

Annex to the Data Processing Agreement (Art. 32 GDPR) **Stoerkens GmbH**, Karl-Birzer-Str. 7, 85521 Ottobrunn, Germany · As of 2026-07-20 · Version 1.0 *The German version prevails.*

1. Confidentiality (Art. 32(1)(b) GDPR)

Physical access control. Systems are operated in data centres in Germany. Physical access is secured by the hosting provider with industry-standard measures (access authorisations, logging, security).

System access control. Access to administrative and portal functions requires authentication. A role and permission concept and strong

passwords apply. Administrative access is limited to the necessary group of persons.

Data access control. Permissions follow the least-privilege principle (CMS/backend roles). Credentials and secrets are stored exclusively in a central secret vault and **not** in source code or configuration files.

Separation control. Data is processed on a per-tenant basis; partner and customer data are logically separated and scope-isolated per partner. Test/demo and production environments are separated.

2. Integrity (Art. 32(1)(b) GDPR)

Transfer control. All data transfers occur exclusively encrypted via TLS/HTTPS. Payment data is processed via the PCI-DSS-certified payment service provider (Stripe).

Input control. Material administrative operations and changes are logged and traceable.

3. Availability and resilience (Art. 32(1)(b) GDPR)

Regular backups, operation in Germany, documented recovery procedures, monitoring and a public status page (crmbooster.io/status) ensure availability and resilience.

4. Regular review procedure (Art. 32(1)(d) GDPR)

An automated end-to-end test suite verifies the platform’s core functions. Changes go through a defined deployment and rollback process. Data protection by design and by default (Art. 25 GDPR) is embedded as a development principle (including selecting only the required data fields).

5. Commissioned-processing control

Contracts under Art. 28 GDPR are in place with sub-processors. The sub-processors used are listed in `subprozessoren.md`.

6. Hosting and storage at rest

The systems are operated at Hetzner Online GmbH in data centres in Germany; Hetzner is certified to ISO/IEC 27001. Storage is mirrored (RAID-1, for resilience). Access to the database and servers is limited to authenticated administrators under the least-privilege principle; credentials and keys are held exclusively in a central vault. Full disk/volume encryption at rest is not currently employed; data at rest is protected by the physical, system- and data-access controls above. Transmission is exclusively encrypted (TLS/HTTPS, see section 2).