EXTRA Group | TRUST CENTER

DSGVO Dokumentation

Überblick zu Auftragsverarbeitung, TOMs und relevanten Verarbeitungsprozessen

EXTRA Group GmbH – Digital Innovation Studio

Version: 1.0
Stand: 12.11.2024
Geltungsbereich: EXTRA Group GmbH und verbundene Marken / Plattformen

1. Einordnung & Geltungsbereich

Die EXTRA Group GmbH entwickelt und betreibt Enterprise-fähige Plattformen, Community-Layer-Lösungen, AI-Automation und Digital Commerce Systeme. Dieses Dokument fasst unsere datenschutzrelevanten Rollen, Verarbeitungsprozesse und technischen sowie organisatorischen Maßnahmen (TOMs) konzernweit zusammen.

1.1 Unternehmen & Leistungsportfolio

- Kernfelder der EXTRA Group:
- Community-Layer-Lösungen und Live-Engagement
- AI Automation & Performance Systems
- Digitale Plattformen (Web/Apps)
- Digital Commerce & Media Technology

1.2 Zweck dieses Dokuments

- Dieses Dokument dient insbesondere folgenden Zwecken:
- Einordnung der Rolle der EXTRA Group nach DSGVO (Verantwortlicher / Auftragsverarbeiter)
- Überblick über zentrale Verarbeitungstätigkeiten
- Beschreibung der technischen und organisatorischen Maßnahmen (TOMs) gem. Art. 32 DSGVO
- Darstellung unserer Kern-Garantien zu Datenhoheit, Löschung, Verfügbarkeit und Exit-Szenarien

Hinweis: Dieses Dokument ergänzt die jeweils individuell abgeschlossenen Verträge (insb. Auftragsverarbeitungsverträge nach Art. 28 DSGVO) und ersetzt keine individuelle Rechtsberatung.

2. Rolle nach DSGVO

2.1 Verantwortlicher

Für die Verarbeitung personenbezogener Daten im Rahmen des Besuchs unserer Websites, der Kommunikation sowie eigener Marketing- und Vertriebsaktivitäten ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO:

EXTRA Group GmbH
Mathes-Deutsch-Weg 24B
84036 Landshut, Deutschland

2.2 Auftragsverarbeiter

Bei B2B-Kundenprojekten (z. B. Community Layer, AI Automation, Plattform- und Commerce-Lösungen) verarbeitet die EXTRA Group personenbezogene Daten im Auftrag ihrer Kunden und agiert damit als Auftragsverarbeiter nach Art. 28 DSGVO.

- Die Verarbeitung erfolgt dabei ausschließlich:
- zur Erbringung der vertraglich vereinbarten Leistungen,
- auf dokumentierte Weisung des Kunden,
- ohne Nutzung der Daten zu eigenen Werbe- oder Verkaufszwecken.

Die Details der Auftragsverarbeitung werden in einem Standard-AVV nach Art. 28 DSGVO geregelt (Gegenstand und Dauer der Verarbeitung, Kategorien betroffener Personen, TOMs, Subprozessoren, Audit- und Kontrollrechte, Löschung und Exit-Szenarien).

3. Infrastruktur & Ort der Datenverarbeitung

Die wesentlichen Eckpunkte der Infrastruktur sind:

- Produktive Systeme werden ausschließlich in zertifizierten Rechenzentren in Deutschland betrieben.
- Backups werden auf geo-redundanten Standorten in Deutschland/EU gespeichert.
- Die Entwicklung erfolgt in einem Netzwerk ISO-27001-zertifizierter Entwicklungspartner in Europa.
- Je nach Projekt kommen weitere zertifizierte Infrastruktur- und Servicepartner (z. B. SOC 2, PCI-DSS) zum Einsatz.

4. Grundsätze der Datenverarbeitung

4.1 Datenhoheit

- Unsere Kunden behalten zu jeder Zeit die volle Datenhoheit:
- Daten bleiben im Eigentum des Kunden.
- Keine Nutzung für eigene Werbezwecke und kein Verkauf an Dritte.
- Export in gängigen Formaten ist auf Anfrage möglich.
- Definierte Aufbewahrungs- und Löschfristen gemäß DSGVO und Kundenanforderung.
- Vollständige Löschung nach Vertragsende inkl. Backups gemäß dokumentierter Lösch-Policy.
- Unterstützung bei Exit-Szenarien ohne Vendor Lock-in.

4.2 Performance & Verfügbarkeit

- Je nach System und Paket können vereinbart werden:
- SLAs mit bis zu 99,9 % Verfügbarkeit.
- 24/7 Monitoring mit definierten Reaktionszeiten.
- Dokumentierter Disaster-Recovery-Plan mit regelmäßigen Tests.

5. Überblick über zentrale Verarbeitungsprozesse

Die nachfolgenden Prozesse bilden einen konzernweiten Rahmen. Konkrete Projekte können in separaten Anlagen detailliert werden (Verzeichnis von Verarbeitungstätigkeiten, projektspezifische TOM-Anhänge).

5.1 Websites & Kommunikation

Bereich	Inhalt
Zweck	Bereitstellung der Website, Stabilität und Sicherheit, Bearbeitung von Kontaktanfragen, ggf. Newsletter.
Datenkategorien	Verbindungs- und Nutzungsdaten, Kommunikationsdaten, Einwilligungsdaten.
Betroffene Personen	Besucher*innen der Website, Ansprechpersonen bei Interessenten, Partnern und Kunden.
Rechtsgrundlagen	Art. 6 Abs. 1 lit. f DSGVO, Art. 6 Abs. 1 lit. b DSGVO, Art. 6 Abs. 1 lit. a DSGVO.
Speicherdauern	Logdaten i. d. R. 14–30 Tage, Kontaktanfragen 6–24 Monate, Newsletterdaten bis Widerruf.

5.2 Community Layer & Live-Engagement

Bereich	Inhalt
Zweck	Bereitstellung von Live-Chat, Umfragen, Reaktionen, Q&A-Formaten und Community-Features.
Datenkategorien	Nutzerkontodaten, Inhaltsdaten, Nutzungsdaten.
Betroffene Personen	Endnutzer*innen der Kundenplattform, kundenseitige Administratoren und Moderatoren.
Rechtsgrundlagen	In der Regel Art. 6 Abs. 1 lit. b, f DSGVO auf Seiten des Kunden; EXTRA Group als Auftragsverarbeiter.
Besonderheiten	Verarbeitung ausschließlich gemäß Weisung des Kunden; keine Nutzung zu eigenen Zwecken.

5.3 AI Automation & Decision Support

Bereich	Inhalt
Zweck	Automatisierte Beantwortung von Anfragen, Content-Generierung, Unterstützung beim Auswerten von Nutzungs- und Performance-Daten.
Datenkategorien	Eingaben der Nutzer, Nutzer-IDs/Pseudonyme, technische Nutzungs- und Logdaten.
Betroffene Personen	Endnutzer*innen der Systeme unserer Kunden.
Besonderheiten	KI-Modelle werden nach dokumentierten Richtlinien betrieben; Entscheidungen bleiben nachvollziehbar und übersteuerbar.
Rolle der EXTRA Group	Auftragsverarbeiter nach Art. 28 DSGVO.

5.4 Digital Commerce & Transaktionssysteme

Bereich	Inhalt
Zweck	Abwicklung von Bestellungen, Zahlungsprozessen, Kundenkonten und Versandprozessen.
Datenkategorien	Kundenstammdaten, Bestell- und Zahlungsdaten, projektspezifische Zusatzdaten.
Betroffene Personen	Kund*innen der Commerce-Systeme unserer Kunden.
Besonderheiten	Zahlungsprozesse über PCI-DSS-zertifizierte Payment-Provider.
Rolle der EXTRA Group	Auftragsverarbeiter nach Art. 28 DSGVO.

6. Technische & organisatorische Maßnahmen (TOMs)

Die folgenden Maßnahmen bilden das konzernweite Sicherheits-Framework und werden regelmäßig überprüft und dokumentiert.

6.1 Vertraulichkeit

- Zutrittskontrolle:
- Betrieb in zertifizierten Rechenzentren in Deutschland mit physischer Zugangskontrolle und Protokollierung.
- Zugangskontrolle:
- Individuelle Benutzerkonten, starke Passwortrichtlinien, Multi-Factor-Authentifizierung für sensible Zugänge.
- Zugriffskontrolle:
- Rollen- und Berechtigungskonzepte (RBAC) auf Applikations-, Datenbank- und Infrastruktur-Ebene, regelmäßige Rezertifizierung.
- Weitergabekontrolle:
- Verschlüsselung von Daten in Transit und at Rest, Verträge mit Subprozessoren nach Art. 28 DSGVO, Vertraulichkeitsvereinbarungen.

6.2 Integrität

- Sichere Software-Entwicklung mit etablierten Secure-Coding-Standards.
- Code-Reviews und Vier-Augen-Prinzip für kritische Änderungen.
- Regelmäßige Sicherheitsüberprüfungen und automatisierte Schwachstellenscans.
- Schutzmaßnahmen gegen typische Angriffsvektoren (z. B. CSRF, XSS, Injection).

6.3 Verfügbarkeit & Belastbarkeit

- SLAs mit bis zu 99,9 % Uptime je nach System und Paket.
- 24/7 Monitoring mit definierten Reaktionszeiten.
- Regelmäßige Backups an geo-redundanten Standorten inkl. Test-Restores.
- Dokumentierter Disaster-Recovery-Plan mit Notfallprozessen.

6.4 Pseudonymisierung & Datenminimierung

- Einsatz von Pseudonymisierung, wo möglich (z. B. Nutzung von IDs statt Klarnamen in Logs).
- Konfiguration der Systeme nach dem Prinzip Privacy by Design & by Default.
- Keine produktiven personenbezogenen Daten in Entwicklungs- und Testumgebungen (Anonymisierung oder synthetische Daten).

6.5 Organisationsmaßnahmen

- Dokumentierte Richtlinien zu Informationssicherheit, Acceptable Use, Passworten und Zugriffsmanagement.
- Regelmäßige Mitarbeiterschulungen zu Datenschutz, Informationssicherheit und Security-Awareness.

- Regelmäßige Überprüfung von Prozessen und Dienstleistern, inkl. Zertifikats-Checks.

7. Transparenz & Ethik (AI, Green Coding, Open Source)

Ergänzend zu den TOMs gelten konzernweit folgende Prinzipien:

7.1 AI Ethics

- Minimierung von Verzerrungen (Bias) und dokumentierte Datengrundlagen.
- Entscheidungen bleiben nachvollziehbar; kritische Entscheidungen können jederzeit durch Menschen übersteuert werden.

7.2 Green Coding

- Ressourcenschonende Software-Architekturen und effizienter Code.
- Wo möglich Nutzung von Rechenzentren mit zertifizierter Ökostrom-Nutzung und optimierten Deployments.

7.3 Open Source Contribution

- Verantwortungsvolle Nutzung von Open-Source-Technologien.
- Beitrag zu Open-Source-Projekten (z. B. Bugfixes, Features), wo sinnvoll.

8. Rechte der betroffenen Personen

Betroffene Personen haben im Rahmen der gesetzlichen Voraussetzungen insbesondere folgende Rechte:

- Auskunft (Art. 15 DSGVO)
- Berichtigung (Art. 16 DSGVO)
- Löschung (Art. 17 DSGVO)
- Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Datenübertragbarkeit (Art. 20 DSGVO)
- Widerspruch (Art. 21 DSGVO)
- Widerruf erteilter Einwilligungen (Art. 7 Abs. 3 DSGVO)

9. Kontakt & Ansprechpartner

Verantwortliche Stelle:

EXTRA Group GmbH
Mathes-Deutsch-Weg 24B
84036 Landshut, Deutschland
Telefon: +49 871 9740 734-0
E-Mail: service@extra-group.com

Security / Compliance / Datenschutz

Security & Compliance Team – EXTRA Group GmbH
Kontakt über Kontaktformular oder service@extra-group.com

Zuständige Aufsichtsbehörde

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA), Promenade 18, 91522 Ansbach, Deutschland.