

# Compliance & Governance Assessment

## Best-of-Breed-Marketing-Automation mit Evalanche

Dieses Asset dient der frühen sicherheits-, datenschutz- und architekturbezogenen Einordnung einer Marketing-Automation-Lösung im Unternehmenskontext. Im Fokus steht die Frage, ob die Integration in bestehende System-, Sicherheits- und Governance-Architekturen tragfähig ist und ohne strukturelle Risiken erfolgen kann.

### Zielgruppe

CISOs sowie IT-Security-, Datenschutz- und Architekturverantwortliche, die die Integrationsfähigkeit einer Marketing-Automation-Lösung in komplexe Systemlandschaften bewerten möchten.

### Inhalt

1. Systemrolle & Architekturprinzip
2. Datenverarbeitung & Systemgrenzen
3. Tracking- und Datennutzungsmodelle
4. Datenschutz & DSGVO-Compliance
5. Zugriffskontrolle & Identity Management
6. Informationssicherheitsmodell
7. Betriebsmodell
8. Architektur- und Risikoeinordnung
9. Gesamtbewertung

# 1. Systemrolle & Architekturprinzip

---

Die Marketing-Automation-Plattform Evalanche ist als spezialisierte, funktional abgegrenzte Komponente innerhalb einer modularen Enterprise-Architektur konzipiert.

Sie ist nicht als Ersatz für bestehende Kernsysteme (z. B. CRM) vorgesehen, sondern als ergänzende Systemkomponente.

## Kernprinzipien

- lose gekoppelte Systemarchitektur (Best-of-Breed-Ansatz)
- Integration über definierte Schnittstellen (API-basiert)
- klare funktionale Trennung der Systemrollen
- keine zwingende Konsolidierung von Daten- oder Kernsystemen
- inkrementelle Einführung über klar definierte Use Cases

# 2. Datenverarbeitung & Systemgrenzen

---

Die Verarbeitung personenbezogener Daten erfolgt zweckgebunden innerhalb klar definierter Systemgrenzen.

## Typischer Datenfluss

- Bereitstellung von Daten aus Bestandssystemen (z. B. CRM)
- Verarbeitung innerhalb von Kampagnen- und Automationslogiken
- Erfassung von Interaktionen im Rahmen definierter Prozesse
- optionale Rückführung relevanter Ereignisdaten in Quellsysteme

## Leitprinzipien

- Datenminimierung
- Zweckbindung
- kontrollierte Schnittstellenkommunikation
- nachvollziehbare Datenflüsse über Systemgrenzen hinweg

## 3. Tracking- und Datennutzungsmodelle

---

Die Nutzung von Tracking-Funktionalitäten ist konfigurationsabhängig und organisatorisch zu steuern.

### 1. Personenbezogenes Tracking

- Verarbeitung mit Personenbezug
- nur bei wirksamer Einwilligung zulässig
- vollständige Individualauswertung möglich

### 2. Pseudonymisiertes Tracking

- keine direkte Personenidentifikation
- Auswertung nur aggregiert oder pseudonymisiert
- Einwilligung weiterhin erforderlich

### 3. Deaktiviertes Tracking

- keine Erhebung von Trackingdaten
- Nutzung ohne Verhaltensanalyse

## 4. Datenschutz & DSGVO-Compliance

---

Die Plattform ist auf eine DSGVO-konforme Nutzung ausgelegt und unterstützt zentrale Privacy-by-Design-Prinzipien.

### Zentrale Prinzipien

- Verarbeitung erfolgt zweckgebunden und auf Basis definierter Geschäftsprozesse
- Unterstützung von Privacy-by-Design- und Privacy-by-Default-Ansätzen
- Datenhaltung innerhalb der EU (Deutschland)
- Unterstützung von Einwilligungs- und Widerrufsmechanismen (Opt-in/Opt-out)
- Umsetzung von Datenminimierung und Speicherbegrenzung

**Bewertung:** Die Lösung ist für den Einsatz in regulierten Unternehmensumgebungen geeignet, sofern Governance- und Betriebsprozesse korrekt implementiert sind.

## 5. Zugriffskontrolle & Identity Management

---

Der Zugriff auf Systeme und Daten erfolgt über standardisierte Sicherheits- und Identitätsmechanismen:

- rollenbasierte Zugriffskontrolle (RBAC)
- Mandantenfähigkeit für komplexe Organisationsstrukturen
- Integration in bestehende Identity-Provider-Systeme (IdP) möglich
- Unterstützung von Multi-Faktor-Authentifizierung
- IP-basierte Zugriffsbeschränkungen möglich
- funktionale Trennung von Verantwortlichkeiten

## 6. Informationssicherheitsmodell

---

Die Plattform implementiert technische und organisatorische Sicherheitsmaßnahmen zum Schutz von Daten und Systemen.

### **Zentrale Sicherheitsmechanismen**

- Verschlüsselung ruhender Daten (AES-256)
- Verschlüsselte Datenübertragung
- Betrieb in ISO-27001-zertifizierter Infrastruktur
- Nutzen der Plattformen zertifizierter Rechenzentrums- und Infrastrukturpartner
- Unterstützung von Sicherheitsnachweisen (z. B. Audits, Penetrationstests)
- Zugriffsschutz durch technische Kontrollmechanismen (z. B. MFA, IP-Restriktionen)

## 7. Betriebsmodell

---

Die Verantwortlichkeiten sind zwischen Anbieter und Unternehmen klar getrennt:

### Plattformanbieter

- Betrieb der technischen Infrastruktur
- Umsetzung von Sicherheitsmechanismen
- Sicherstellung der Systemverfügbarkeit und Plattformsecurity

### Unternehmen

- Governance der Nutzung
- Verwaltung von Benutzerrechten und Rollen
- Definition von Datenflüssen und Integrationen
- Einhaltung interner Compliance- und Datenschutzrichtlinien

## 8. Architektur- und Risikoeinordnung

---

Der Best-of-Breed-Ansatz führt zu einer modularen, steuerbaren Systemlandschaft:

- Spezialisierung einzelner Plattformen nach Funktionsdomäne
- Reduktion von Abhängigkeiten zwischen Kernsystemen
- klare Verantwortungs- und Kontrollstrukturen
- inkrementelle Weiterentwicklung der Gesamtarchitektur

Im Vergleich zu monolithischen Plattformansätzen entsteht eine flexiblere, jedoch governance-intensivere Architekturstruktur.

## 9. Gesamtbewertung

---

Die Lösung ist grundsätzlich geeignet für eine weiterführende technische, sicherheitsbezogene und datenschutzrechtliche Detailprüfung.

### Relevante Bewertungskriterien

- Betrieb in zertifizierter EU-/Deutschland-Infrastruktur
- verschlüsselte und kontrollierte Datenverarbeitung
- konfigurierbare Tracking- und Datennutzungsmodelle
- integrierbare Identity- und Zugriffskontrollmechanismen
- klar definierte Verantwortungsmodelle zwischen Anbieter und Unternehmen
- Einbindung in bestehende Governance- und Security-Frameworks

**Schlussfolgerung:** Die Architektur ist für regulierte Unternehmensumgebungen geeignet, sofern Integration, Governance und Betriebsmodell organisationsseitig konsistent umgesetzt werden.

## Möchtest du weitere Informationen zur Skalierbarkeit einer Best-of-Breed-Architektur über mehrere Organisationseinheiten hinweg?

Im Fokus stehen Architekturzusammenhänge zwischen Governance, Systemarchitektur und organisatorischer Steuerung zur Bewertung der Skalierbarkeit über Organisationseinheiten hinweg – inklusive klarer Trennung, Kontrollierbarkeit und Erweiterbarkeit.

➔ [Zur Compliance Checkliste Skalierung](#)

### Kontakt

Evalanche (SC-Networks GmbH)  
Würmstr. 4  
82319 Starnberg  
Deutschland  
Telefon: +49 8151 555 16-0  
E-Mail: [info@evalanche.com](mailto:info@evalanche.com)  
Web: [www.evalanche.com](http://www.evalanche.com)

Die Inhalte dieses Whitepapers wurden mit größter Sorgfalt erstellt. Für die Richtigkeit, Vollständigkeit und Aktualität können wir jedoch keine Gewähr übernehmen.

© SC-Networks GmbH, 2026

Alle Rechte vorbehalten – einschließlich derer, welche die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung der Inhalte dieses Dokumentes oder Teile davon außerhalb der Grenzen des Urheberrechts betreffen. Handlungen in diesem Sinne bedürfen der schriftlichen Zustimmung durch SC-Networks. SC-Networks behält sich das Recht vor, Aktualisierungen und Änderungen der Inhalte vorzunehmen. Sämtliche Daten und Inhalte, die auf Screenshots, Grafiken und weiterem Bildmaterial sichtbar sind, dienen lediglich zur Demonstration. Für den Inhalt dieser Darstellung übernimmt SC-Networks keine Gewähr.