

Marketing-Workflows effizienter gestalten – vom CRM bis zur Kampagne

Diese Checkliste richtet sich an Entscheidungsverantwortliche aus den Bereichen Recht, Informationssicherheit und Enterprise-Architektur, die Marketing-Automation-Lösungen für den Einsatz in komplexen Multi-Unit- und Enterprise-Organisationen bewerten möchten.

Sie dient der systematischen Einordnung, ob eine Plattform den Betrieb über mehrere Länder, Business Units und Organisationseinheiten hinweg unterstützt.

Im Fokus steht die Frage, wie gut die Lösung den Aufbau und Betrieb einer skalierbaren System- und Organisationsarchitektur ermöglicht, in der:

- Governance zentral definiert und lokal umgesetzt wird
- Daten und Zugriffe kontrolliert und abgegrenzt bleiben
- mehrere Organisationseinheiten parallel und unabhängig arbeiten können
- regulatorische Anforderungen in der Architektur verankert sind

Die Bewertung erfolgt auf architektonischer Ebene und ist unabhängig von konkreten Marketing- oder Kampagnenanwendungen.

Inhalt

1. Entscheidungsübersicht
2. Multi-Unit-Architekturprinzip
3. Mandantenfähigkeit & organisatorische Trennung
4. Governance-Modell
5. Rollen, Rechte & Zugriffskontrolle
6. Identity & Zugriff (SSO/MFA)
7. Datenstruktur & Mandantentrennung
8. Datenlebenszyklus & DSGVO-Prozesse
9. Mandantenübergreifende Steuerung & Datenaustausch
10. Audit, Nachvollziehbarkeit & Kontrollfähigkeit
11. Skalierungsfähigkeit über Organisationseinheiten hinweg
12. Fazit

1. Entscheidungsübersicht

Multi-Unit Governance

- ✓ zentrale Steuerung + lokale Umsetzung möglich

Mandantenfähigkeit

- ✓ klare logische Trennung von Organisationseinheiten

Datenkontrolle

- ✓ nach Units getrennte Datenhaltung

Zugriffssteuerung

- ✓ differenzierbare Rollen- und Rechtekonzepte
- ✓ Möglichkeit, zusätzliche technische Zugriffskontrollen einzurichten (z. B. 2FA, IP-Restriktionen)

Identity Integration

- ⚠ Abhängigkeit der SSO-Funktionalität von externer Integration (z. B. SAML/OIDC)
- ✓ Unterstützung von MFA (z. B. hardwarebasierte Sicherheits-Keys wie UB Key)

Audit & Nachvollziehbarkeit

- ✓ vollständige Nachvollziehbarkeit von Prozessen
- ✓ Verfügbarkeit von Nachweisen und Audit-Dokumentation (z. B. Sicherheitskonzept, Auditberichte)

Skalierung

- ✓ Erweiterbarkeit um neue Einheiten – ohne Architekturbruch

Compliance/DSGVO

- ✓ Erfüllung grundlegender Prinzipien (Privacy-by-Design, kontrollierte Verarbeitung, Datenlokation in der EU/in Deutschland)

2. Multi-Unit-Architekturprinzip

Multi-Unit-Komplexität entsteht primär durch unklare Verantwortlichkeiten, unstrukturierte Daten und uneinheitliche Entscheidungslogiken.

Eine skalierbare Architektur basiert auf:

- **zentraler Governance:** Definition von Standards, Prozessen und Richtlinien
- **lokaler Umsetzung:** operative Durchführung innerhalb definierter Rahmenbedingungen
- **struktureller Trennung:** klare Abgrenzung zwischen Organisationseinheiten, Datenräumen und Verantwortlichkeiten

Ziel ist eine Architektur, die Wachstum ermöglicht und gleichzeitig Kontrollverlust sowie ein Aufweichen der Governance verhindert.

3. Mandantenfähigkeit & organisatorische Trennung

Unter Mandantenfähigkeit versteht man die Möglichkeit, mehrere Organisationseinheiten innerhalb eines Systems logisch getrennt abzubilden und zu verwalten.

Architektonische Eigenschaften

- logisch getrennte Organisationseinheiten innerhalb eines Systems
- separierte Daten-, Prozess- und Konfigurationsräume
- unabhängige Steuerbarkeit der einzelnen Einheiten
- gemeinsame Nutzung definierter Standards

Wirkung

- Vermeidung von Datenvermischung
- eindeutige Zuordnung von Verantwortlichkeiten
- Parallelbetrieb unterschiedlicher Organisationseinheiten

Prüffokus

- Sind Organisationseinheiten eindeutig voneinander getrennt?
- Lassen sich Einheiten unabhängig voneinander verwalten?
- Bleibt Governance über alle Einheiten konsistent steuerbar?

4. Governance-Modell

Governance definiert die Steuerungslogik über alle Organisationen hinweg.

Struktur

- zentrale Definition von Standards und Prozessen
- Ableitung auf lokale Einheiten
- kontrollierte Umsetzung innerhalb definierter Steuerungsrahmen

Wesentliche Elemente

- Prozess- und Richtlinienstandards
- KPI- und Reporting-Logiken
- Freigabe- und Kontrollmechanismen
- organisationsübergreifende Regelwerke

Prüffokus

- Lassen sich Standards zentral definieren und verbindlich umsetzen?
- Wie wird Konsistenz über alle Einheiten sichergestellt?
- Gibt es überprüfbare Kontrollmechanismen?

5. Rollen, Rechte & Zugriffskontrolle

Zugriffskontrolle umfasst rollenbasierte Berechtigungen sowie technische Schutzmechanismen zur Absicherung sensibler Daten und Systeme.

Anforderungen

- rollenbasierte Zugriffskontrolle
- Differenzierung nach Organisationseinheiten
- granulare Berechtigungssteuerung
- Trennung von zentralen und lokalen Verantwortlichkeiten
- technische Zugriffssicherungen (z. B. IP-Restriktionen, 2FA)

Prüffokus

- Ist es möglich, Rechte pro Rolle und Einheit differenziert zu steuern?
- Ist eine klare Trennung von Verantwortlichkeiten abbildbar?
- Sind Zugriffsrechte konsistent überprüfbar?

6. Identity & Zugriff (SSO/MFA)

Enterprise-Architekturen erfordern die Integration in bestehende Identity-Infrastrukturen.

Zu Prüfendes

- Unterstützung von SSO (z. B. SAML/OIDC)
- Unterstützung von Multi-Factor Authentication (hardwarebasierte Sicherheits-Keys)
- Nutzung unternehmensweiter Sicherheitsrichtlinien
- zentrale Verwaltung von Benutzeridentitäten

Prüffokus

- Wie erfolgt die Integration in bestehende Identity-Architekturen?
- Lassen sich unternehmensweite Sicherheitsrichtlinien durchsetzen?
- Ist eine zentrale Benutzerverwaltung realisierbar?

7. Datenstruktur & Mandantentrennung

Datenorganisation ist ein elementarer Bestandteil der Multi-Unit-Architektur.

Anforderungen

- nach Organisationseinheiten logisch getrennte Daten
- eindeutige Zuordnung von Daten zu Verantwortlichkeiten
- kontrollierte Datenflüsse zwischen Einheiten
- Unterstützung von globalen und lokalen Datenstrukturen
- flexible Anwendung von Datenklassifikationen (global oder mandantenspezifisch)

Wirkung

- Vermeidung unkontrollierter Datenverteilung
- trennscharfe Datenhoheit pro Einheit
- strukturierte Nutzung gemeinsamer Datenbasis

Prüffokus

- Ist die Datenhoheit eindeutig je Mandant definiert?
- Können Daten kontrolliert zwischen Einheiten bewegt werden?
- Ist die Trennung von Daten systemweit einheitlich und konsequent umgesetzt?

8. Datenlebenszyklus & DSGVO-Prozesse

Regulatorische Anforderungen betreffen den gesamten Lebenszyklus von Daten.

Relevante Aspekte

- zweckgebundene Datenverarbeitung
- Speicherung innerhalb definierter Regionen (EU/Deutschland)
- Unterstützung von Datenschutzprinzipien wie Privacy-by-Design
- Umsetzung organisatorischer Vorgaben für Löschung, Auskunft und Datenminimierung

Prüffokus

- Sind Lösch- und Aufbewahrungsrichtlinien technisch abbildbar?
- Ist es möglich, die Datenverarbeitung zweckgebunden zu steuern?
- Lassen sich DSGVO-Prozesse organisatorisch umsetzen?

9. Mandantenübergreifende Steuerung & Datenaustausch

In Multi-Unit-Architekturen ist der kontrollierte Datenfluss zwischen Einheiten entscheidend.

Anforderungen

- kontrollierter Datenaustausch zwischen Organisationseinheiten
- Definition von Freigabe- oder Transfermechanismen
- Vermeidung unkontrollierter Datenbewegungen
- Steuerung von Datenflüssen auf Governance-Ebene

Prüffokus

- Ist die Datenübertragung zwischen Mandanten kontrollierbar?
- Lassen sich Freigaben strukturiert steuern?
- Bleibt die Datenkontrolle jederzeit erhalten?

10. Audit, Nachvollziehbarkeit & Kontrollfähigkeit

Entscheidend ist die Möglichkeit, System- und Prozessverhalten systematisch nachzuvollziehen.

Das bedeutet:

- Aktionen innerhalb des Systems sind eindeutig zuordenbar
- Änderungen an Daten und Prozessen sind dokumentiert
- Freigaben sind lückenlos nachvollziehbar
- Prozesse lassen sich intern und extern überprüfen

Prüffokus

- Sind sicherheits- und governance-relevante Aktivitäten nachvollziehbar dokumentiert?
- Lassen sich Änderungen eindeutig den jeweiligen Verantwortlichen zuordnen?
- Ist Auditierbarkeit systemseitig gewährleistet?

11. Skalierungsfähigkeit über Organisationseinheiten hinweg

Unter Skalierung ist die Integration neuer Organisationseinheiten ohne Anpassung der bestehenden Architektur zu verstehen.

Architektonische Anforderungen

- standardisierte Anbindung neuer Organisationseinheiten
- wiederverwendbare Governance- und Prozessmodelle
- Erweiterung ohne strukturelle Änderungen
- konsistente Anwendung über alle Einheiten hinweg

Prüffokus

- Ist es möglich, neue Länder oder Units über ein standardisiertes Modell zu integrieren?
- Bleibt die Systemsteuerung bei Wachstum stabil?
- Ist die Architektur auf langfristige Skalierung ausgelegt?

12. Fazit

Für Multi-Unit-Organisationen ist entscheidend, dass die Systemarchitektur folgende Fähigkeiten unterstützt:

- klare Trennung von Organisationseinheiten (Mandantenfähigkeit)
- zentrale Governance bei lokaler Umsetzung
- rollenbasierte und technisch abgesicherte Zugriffskontrolle
- eindeutig definierte Datenorganisation und Datenlokation

- kontrollierte Prozesse mit operativer DSGVO-Unterstützung
- Integration in bestehende Identity- und Sicherheitslandschaften
- Auditierbarkeit inklusive bereitgestellter Nachweise (z. B. ISO-Zertifizierungen)
- Skalierbarkeit ohne Kontrollverlust

Eine Architektur, die diese Prinzipien erfüllt, ist für den Betrieb über Länder, Business Units und Marken hinweg geeignet und unterstützt nachhaltige Organisations- und Systemskalierung.

Möchtest du weitere Informationen zur sicherheits-, datenschutz- und architekturbezogenen Einordnung einer Best-of-Breed-Architektur?

Spezialisierte Systemkomponenten werden in eine modular integrierte Enterprise-Architektur eingebettet – mit klar definierten Systemgrenzen, kontrollierter Datenverarbeitung, API-basierter Integration sowie Berücksichtigung von Governance-, Sicherheits- und DSGVO-Anforderungen.

➔ **Zur Compliance Checkliste Best-of-Breed**

Kontakt

Evalanche (SC-Networks GmbH)

Würmstr. 4

82319 Starnberg

Deutschland

Telefon: +49 8151 555 16-0

E-Mail: info@evalanche.com

Web: 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.