

11. TOLERANT Whitepaper

Zukunftssichere Compliance Prozesse für Mittel- und Großunternehmen

Von Dipl.-Math. Klaus-Dieter Sedlacek



TOLERANT Software

Unternehmen stehen heute unter dem gleichzeitigen Druck wachsender regulatorischer Anforderungen, steigender Datenmengen, komplexer Liefer- und Partnernetzwerke sowie zunehmender Erwartung an Geschwindigkeit und Transparenz. In diesem Umfeld wird Compliance nicht mehr als isolierte Kontrollfunktion verstanden, sondern als integraler Bestandteil von Unternehmenssteuerung, Risikomanagement und digitaler Transformation.

Dieses Whitepaper zeigt, warum Compliance by Design, Data Governance, Datenqualität und systemübergreifende Prozessautomatisierung zu strategischen Erfolgsfaktoren geworden sind. Es erläutert, wie Organisationen mit belastbaren Prüfprozessen für KYC, AML, Sanktionsprüfung und PEP-Prüfung regulatorische Anforderungen effizient erfüllen, Risiken reduzieren und operative Exzellenz erreichen können.

Der zentrale Befund lautet: Unternehmen, die Compliance, Governance und Technologie integriert denken, schaffen nicht nur Rechtssicherheit, sondern auch messbaren Geschäftswert. Sie erhöhen die Nachvollziehbarkeit, verbessern die Auditfähigkeit, beschleunigen Entscheidungen und stärken ihre Widerstandsfähigkeit gegenüber Markt- und Regulierungsänderungen.

Die Anforderungen an moderne Organisationen haben sich grundlegend verändert. Regulatorische Vorgaben werden komplexer, Prüfpflichten nehmen zu, und die Erwartung an dokumentierte Nachvollziehbarkeit steigt in nahezu allen Branchen. Gleichzeitig müssen Unternehmen ihre Prozesse digitalisieren, Kosten kontrollieren und schneller auf Marktveränderungen reagieren. Daraus entsteht ein Spannungsfeld, das nur mit einer klaren Governance-, Daten- und Prozessarchitektur beherrschbar ist.

Besonders relevant ist dies in Bereichen mit hoher regulatorischer Exponierung, etwa im Bankwesen, Versicherungswesen, in der Fertigung mit globalen Lieferketten sowie im öffentlichen Sektor. Hier reichen manuelle Kontrollen, isolierte Fachlösungen und fragmentierte Datenbestände nicht mehr aus. Gefragt sind integrierte Plattformen, standardisierte Workflows und eine Governance-Struktur, die Compliance, Risikomanagement und operative Effizienz miteinander verbindet.

Ein zukunftsfähiges Unternehmen betrachtet Compliance daher nicht als Kostenfaktor, sondern als Enabler für Vertrauen, Skalierbarkeit und nachhaltiges Wachstum. Die Fähigkeit, regulatorische Anforderungen systematisch, automatisiert und nachvollziehbar umzusetzen, wird zunehmend zu einem Differenzierungsmerkmal im Wettbewerb.



1. Aktuelle Herausforderungen

> **Regulatorische Dynamik und steigende Komplexität**

Unternehmen sehen sich einer wachsenden Zahl an Vorschriften gegenüber, die sich häufig parallel auf nationale, europäische und globale Anforderungen beziehen. Dazu zählen unter anderem Vorgaben zu Geldwäscheprävention, Sanktionsprüfung, KYC, PEP-Prüfung, Datenschutz, Aufbewahrungspflichten, internen Kontrollsystemen und branchenspezifischen Meldepflichten. Die Herausforderung besteht nicht nur in der Einhaltung einzelner Regeln, sondern in ihrer konsistenten Umsetzung über Prozesse, Systeme und Organisationseinheiten hinweg.

> **Fragmentierte Datenlandschaften**

In vielen Organisationen liegen relevante Informationen in unterschiedlichen Kernsystemen, Fachanwendungen, Excel-Dateien oder Dokumentenablagen vor. Diese Fragmentierung erschwert die Identifikation von Kunden, Geschäftspartnern, Lieferanten und Transaktionen. Ohne systemübergreifende Datenintegration entstehen Medienbrüche, doppelte Pflege und inkonsistente Ergebnisse. Gerade bei KYC-, AML- und Sanktionsprüfungen führt dies zu erhöhten Fehlalarmen, längeren Bearbeitungszeiten und unnötigen Eskalationen.

> **Manuelle Prozesse und begrenzte Skalierbarkeit**

Manuelle Prüf- und Freigabeprozesse sind fehleranfällig, schwer skalierbar und nur begrenzt auditierbar. Wenn Prüfungen per E-Mail koordiniert, Ergebnisse manuell zusammengeführt und Entscheidungen nicht strukturiert dokumentiert werden, steigt das operationelle Risiko erheblich. Dies gilt insbesondere bei wachsendem Transaktionsvolumen, internationaler Expansion oder häufigen regulatorischen Änderungen.

> **Unzureichende Datenqualität**

Datenqualität ist eine Grundvoraussetzung für wirksame Compliance. Unvollständige Stammdaten, veraltete Informationen, Dubletten oder uneinheitliche Schreibweisen beeinträchtigen die Trefferqualität und erzeugen False Positives oder False Negatives. Die Folge sind entweder unnötige Prüfaufwände oder das Risiko, relevante Sachverhalte zu übersehen. Datenqualität ist daher kein technisches Randthema, sondern ein Kernbestandteil von Risikomanagement und Governance.

> **Steigende Anforderungen an Nachvollziehbarkeit**

Aufsichtsbehörden, interne Revision, Wirtschaftsprüfer und externe Stakeholder erwarten belastbare Nachweise darüber, wie Entscheidungen zustande kommen. Unternehmen müssen Prüfpfade, Freigaben, Eskalationen und Ausnahmen lückenlos dokumentieren können. Ohne strukturierte Nachvollziehbarkeit wird jede Prüfung zum potenziellen Reputations- und Haftungsrisiko.



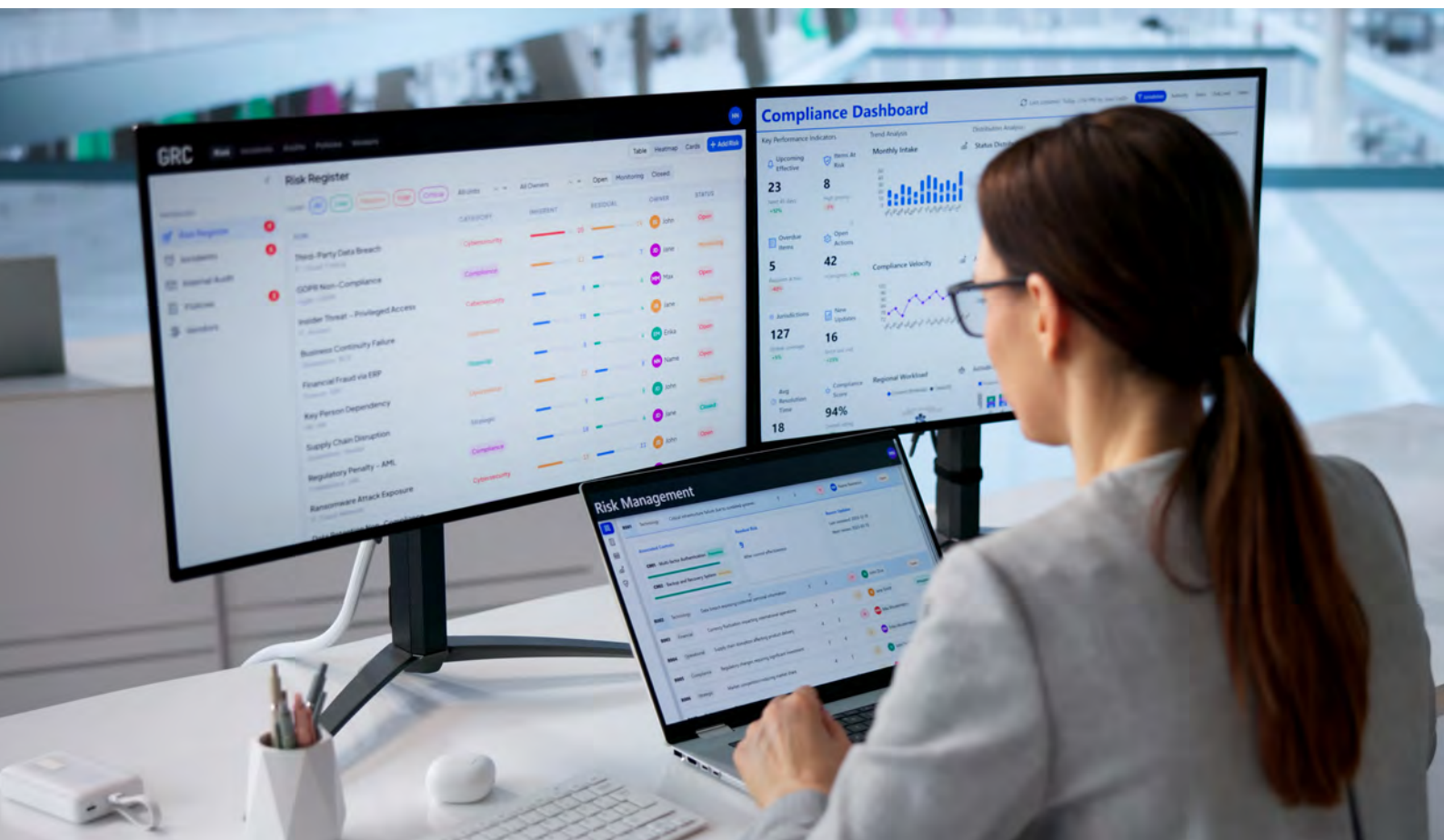
2. Strategische Bedeutung für Organisationen

Compliance, Governance und Datenmanagement sind heute strategische Steuerungsinstrumente. Sie beeinflussen nicht nur die Einhaltung von Vorschriften, sondern auch die Geschwindigkeit von Geschäftsprozessen, die Qualität von Entscheidungen und die Fähigkeit zur Skalierung. Unternehmen, die diese Themen professionell aufsetzen, schaffen eine belastbare Grundlage für Wachstum und Transformation.

Compliance by Design bedeutet, regulatorische Anforderungen bereits in der Prozess- und Systemarchitektur zu berücksichtigen. Dadurch werden Kontrollen nicht nachträglich ergänzt, sondern von Beginn an in Abläufe integriert. Das reduziert Reibungsverluste, senkt Implementierungskosten und erhöht die Wirksamkeit der Kontrollen.

Data Governance sorgt dafür, dass Verantwortlichkeiten, Datenstandards, Qualitätsregeln und Freigabeprozesse klar definiert sind. Sie stellt sicher, dass Daten nicht nur vorhanden, sondern auch vertrauenswürdig, konsistent und nutzbar sind. Für Führungskräfte ist dies von zentraler Bedeutung, weil strategische Entscheidungen nur so auf einer verlässlichen Informationsbasis getroffen werden können.

Risikomanagement profitiert unmittelbar von integrierten Prüf- und Steuerungsmechanismen. Wenn Risiken frühzeitig erkannt, klassifiziert und automatisiert überwacht werden, können Unternehmen schneller reagieren und Eskalationen vermeiden. Dies gilt besonders in regulierten Branchen, in denen Fehlentscheidungen erhebliche finanzielle, rechtliche und reputative Folgen haben können.



3. Geschäftliche Vorteile und Wertschöpfung

> **Effizienzsteigerung und Kostensenkung**

Automatisierte Compliance-Prozesse reduzieren den manuellen Aufwand in Prüfung, Freigabe und Dokumentation. Dadurch sinken Bearbeitungszeiten, Fachbereiche werden entlastet und Ressourcen können auf wertschöpfende Tätigkeiten konzentriert werden. In Banken kann dies etwa die Onboarding-Zeit für Firmenkunden verkürzen. In Versicherungen lassen sich Partner- und Vermittlerprüfungen effizienter gestalten. In der Fertigung profitieren Einkauf und Lieferantenmanagement von schnelleren Sanktions- und Risikoabgleichen.

> **Höhere Entscheidungsqualität**

Wenn Datenqualität, Transparenz und Nachvollziehbarkeit gewährleistet sind, verbessern sich die Grundlagen für Entscheidungen erheblich. Führungskräfte erhalten belastbare Informationen über Risiken, Ausnahmen und Prozessengpässe. Dies ermöglicht eine präzisere Steuerung von Compliance-Programmen, Investitionen und operativen Maßnahmen.

> **Skalierbarkeit und Wachstum**

Unternehmen mit standardisierten, digitalisierten Prüfprozessen können neue Märkte, Geschäftsmodelle oder Partner schneller integrieren. Ein skalierbares Compliance-Framework verhindert, dass Wachstum durch manuelle Kontrollen ausgebremst wird. Gerade bei internationaler Expansion ist dies entscheidend, da unterschiedliche regulatorische Anforderungen konsistent abgebildet werden müssen.

> **Reputationsschutz und Vertrauensaufbau**

Vertrauen ist ein zentraler immaterieller Vermögenswert. Organisationen, die regulatorische Anforderungen professionell erfüllen und ihre Entscheidungen nachvollziehbar dokumentieren, stärken das Vertrauen von Kunden, Aufsichtsbehörden, Investoren und Geschäftspartnern. Dies gilt besonders in Branchen mit hoher öffentlicher Sichtbarkeit oder sensiblen Datenbeständen.

Beispiele aus der Praxis

Im **Bankwesen** kann eine integrierte Plattform für KYC, AML, Sanktionsprüfung und PEP-Prüfung dazu beitragen, neue Kunden schneller und regelkonform zu onboarden. Gleichzeitig werden Treffer systematisch priorisiert und Prüfpfade revisionssicher dokumentiert.

Im **Versicherungswesen** lassen sich Vermittler-, Makler- und Geschäftspartnerprüfungen standardisieren. Dadurch sinkt das Risiko unvollständiger Due-Diligence-Prozesse, und die Governance über Vertriebs- und Kooperationsnetzwerke wird gestärkt.

In der **Fertigung** unterstützt eine systemübergreifende Datenintegration die Prüfung von Lieferanten, Subunternehmern und Handelsbeziehungen. So können Sanktionsrisiken, Embargoverstöße und ESG-bezogene Risiken frühzeitig erkannt werden.

Im **öffentlichen Sektor** verbessern automatisierte Prüf- und Freigabeprozesse die Transparenz bei Fördermitteln, Vergaben und Bürgerdiensten. Gleichzeitig steigt die Auditfähigkeit gegenüber Rechnungshöfen, Innenrevision und parlamentarischer Kontrolle.

4. Perspektiven zu Governance, Compliance und Risiken

- > **Unternehmensweite Governance**
Wirksame Governance erfordert klare Rollen, Verantwortlichkeiten und Eskalationswege. Fachbereiche, Compliance, IT, Risikomanagement und Data Governance müssen gemeinsam agieren. Ohne ein abgestimmtes Betriebsmodell entstehen Zuständigkeitslücken, die die Wirksamkeit von Kontrollen mindern.
- > **Regulatorische Anforderungen & Prüfpflichten**
Organisationen müssen in der Lage sein, regulatorische Anforderungen nicht nur zu interpretieren, sondern operational umzusetzen. Dazu gehören dokumentierte Kontrollen, definierte Schwellenwerte, Freigaberegeln, Ausnahmemanagement und regelmäßige Wirksamkeitsprüfungen. Besonders relevant sind Anforderungen an Aufbewahrung, Revisionssicherheit, Datenschutz und Nachweisführung.
- > **Risikominderung durch Automatisierung**
Automatisierung reduziert nicht nur Kosten, sondern auch Risiken. Standardisierte Prüfregeln minimieren subjektive Entscheidungen, erhöhen die Konsistenz und verbessern die Reaktionsgeschwindigkeit. Gleichzeitig müssen automatisierte Entscheidungen kontrollierbar bleiben. Ein wirksames Modell kombiniert Regelautomatisierung mit fachlicher Eskalation für komplexe oder risikobehaftete Fälle.
- > **Compliance by Design als Governance-Prinzip**
Compliance by Design bedeutet, dass Kontrollen, Dokumentationspflichten und Freigabemechanismen bereits in der Architektur berücksichtigt werden. Dies betrifft Datenmodelle, Schnittstellen, Workflows, Rollenmodelle und Berechtigungskonzepte. Unternehmen, die diesen Ansatz konsequent verfolgen, vermeiden spätere Nachrüstungen und schaffen eine stabile Governance-Basis.
- > **Risiken bei Nichtbeachtung**
Wer Compliance, Datenqualität und Governance vernachlässigt, riskiert Bußgelder, Sanktionen, Reputationsschäden, operative Störungen und Haftungsfragen. Hinzu kommen ineffiziente Prozesse, hohe manuelle Aufwände und eine geringe Anpassungsfähigkeit an neue regulatorische Anforderungen. In kritischen Fällen kann dies zu Geschäftsunterbrechungen oder zum Verlust von Markt- und Kundenvertrauen führen.

5. Auswirkungen auf Prozesse und Organisation

> **Prozessstandardisierung**

Ein zukunftsfähiges Compliance-Setup beginnt mit standardisierten End-to-End-Prozessen. Vom Dateneingang über die Prüfung bis zur Entscheidung und Archivierung müssen definierte Prozessschritte existieren. BPM-Plattformen können dabei helfen, diese Abläufe transparent zu modellieren, zu steuern und kontinuierlich zu verbessern.

> **Organisatorische Verankerung**

Compliance darf nicht ausschließlich in einer zentralen Fachabteilung verankert sein. Vielmehr braucht es ein Zusammenspiel aus zentraler Steuerung und dezentraler Verantwortung. Fachbereiche müssen ihre Rolle im Kontrollsystem kennen, während Compliance und Data Governance Standards, Kontrollen und Monitoring vorgeben.

> **Rollen und Kompetenzen**

Die Umsetzung erfordert neue Kompetenzen in den Bereichen Prozessmanagement, Datenmanagement, Regulatorik und Technologie. Unternehmen sollten Rollen wie Process Owner, Data Owner, Control Owner und Compliance Analyst klar definieren. Schulungen und Awareness-Programme sind notwendig, um die Akzeptanz und Wirksamkeit der Maßnahmen sicherzustellen.

> **Auditfähigkeit und Prüfpfade**

Jede relevante Entscheidung sollte mit einem nachvollziehbaren Prüfpfad versehen sein. Dazu gehören Eingabedaten, verwendete Regeln, Trefferbewertungen, Freigaben, Ausnahmen und Zeitstempel. Diese Transparenz erleichtert interne und externe Prüfungen und stärkt die regulatorische Bereitschaft der Organisation.



6. Überlegungen zu Technologie und Integration

- > **Systemübergreifende Datenintegration**

Eine wirksame Compliance-Architektur benötigt integrierte Datenflüsse zwischen Kernsystemen, Fachanwendungen, Datenplattformen und externen Informationsquellen. Nur so lassen sich Kunden-, Lieferanten- und Transaktionsdaten konsistent prüfen. Schnittstellen, APIs und Datenmodelle sollten standardisiert und governancekonform gestaltet sein.
- > **Prozessautomatisierung und BPM-Plattformen**

BPM-Plattformen ermöglichen die Modellierung, Steuerung und Überwachung komplexer Compliance-Prozesse. In Verbindung mit Regelwerken, Workflow-Engines und Entscheidungslogik lassen sich Prüfungen automatisieren und Eskalationen gezielt steuern. Dies ist besonders relevant für KYC, AML, Sanktionsprüfung und PEP-Prüfung, aber auch für Lieferantenfrequenzen, Berechtigungsprozesse oder Fördermittelkontrollen.
- > **Qualitäts- und Kontrollmechanismen**

Technologie allein löst keine Governance-Probleme. Es braucht Validierungsregeln, Datenqualitätskontrollen, Monitoring, Protokollierung und Berechtigungskonzepte. Systeme sollten so gestaltet sein, dass Fehler früh erkannt, Ausnahmen dokumentiert und Korrekturen nachvollziehbar vorgenommen werden können.
- > **Architekturprinzipien**

Empfohlen werden modulare, skalierbare und interoperable Architekturen. Offene Schnittstellen, klare Datenverantwortung und eine Trennung von Fachlogik und technischer Umsetzung erhöhen die Zukunftsfähigkeit. Unternehmen sollten vermeiden, neue Insellösungen zu schaffen, die langfristig die Komplexität erhöhen.
- > **Digitale Transformation als Enabler**

Digitale Transformation ist dann erfolgreich, wenn sie nicht nur Prozesse digitalisiert, sondern Governance und Compliance mitdenkt. Automatisierte Prüfungen, zentrale Transparenz und standardisierte Datenflüsse schaffen die Grundlage für resiliente Geschäftsmodelle. In diesem Sinne ist Compliance ein wesentlicher Bestandteil der digitalen Unternehmensarchitektur.

7. Best Practices

- > Compliance, Risiko und Data Governance gemeinsam steuern statt isoliert organisieren.
- > Regulatorische Anforderungen früh in Prozessdesign und Systemarchitektur integrieren.
- > Einheitliche Datenstandards, Referenzdaten und Qualitätsregeln definieren.
- > Prüfungen für KYC, AML, Sanktionsprüfung und PEP-Prüfung zentral standardisieren.
- > Ausnahmen, Eskalationen und Freigaben revisionssicher dokumentieren.
- > BPM-Plattformen für durchgängige Workflows und Monitoring einsetzen.
- > Regelmäßige Wirksamkeitsprüfungen und Kontrollen etablieren.
- > Klare Rollen für Data Owner, Process Owner und Control Owner festlegen.
- > Dashboards für Risiko, Durchlaufzeiten, Trefferquoten und Bearbeitungsstände nutzen.
- > Kontinuierliche Verbesserung als festen Bestandteil des Betriebsmodells verankern.

8. Häufige Fallstricke

- > Einführung einzelner Tools ohne übergreifende Governance.
- > Unklare Verantwortlichkeiten zwischen Fachbereich, Compliance und IT.
- > Unterschätzung der Datenqualität als Erfolgsfaktor.
- > Zu starke Abhängigkeit von manuellen Prüfungen und E-Mail-Freigaben.
- > Fehlende Dokumentation von Entscheidungen und Ausnahmen.
- > Insellösungen ohne systemübergreifende Integration.
- > Automatisierung ohne ausreichende Kontroll- und Eskalationsmechanismen.
- > Zu geringe Berücksichtigung regulatorischer Änderungen im Betriebsmodell.
- > Fehlende Schulung der Mitarbeitenden und mangelnde Akzeptanz im Fachbereich.
- > Projekte ohne messbare Zielgrößen, Governance-KPIs und Betriebsverantwortung.



9. Zukünftige Trends und Marktentwicklungen

Die Zukunft von Compliance und Governance wird durch stärkere Automatisierung, intelligenteren Datenverarbeitung und höhere Transparenz geprägt sein. Unternehmen werden verstärkt auf integrierte Plattformen setzen, die Prüfungen, Workflows, Datenqualität und Reporting in einem konsistenten Betriebsmodell vereinen.

Ein zentraler Trend ist der Einsatz von KI-gestützten Assistenzfunktionen zur Priorisierung von Treffern, zur Mustererkennung und zur Unterstützung von Fallbearbeitungen. Gleichzeitig wird der Bedarf an erklärbarer, auditierbarer Automatisierung steigen. Organisationen werden nachweisen müssen, warum ein System eine bestimmte Entscheidung vorgeschlagen oder getroffen hat.

Ein weiterer Trend ist die stärkere Verzahnung von Compliance mit ESG-, Lieferketten- und Drittparteienrisiken. Sanktionsprüfung, PEP-Prüfung und Due Diligence werden zunehmend in umfassendere Risiko- und Governance-Programme eingebettet. Auch im öffentlichen Sektor werden digitale Nachweis- und Prüfprozesse an Bedeutung gewinnen.

Darüber hinaus wird sich die Bedeutung von Echtzeit- oder Near-Realtime-Prüfungen erhöhen. Unternehmen erwarten künftig schneller verfügbare Ergebnisse, insbesondere bei Onboarding, Zahlungen, Lieferantenfreigaben und Transaktionskontrollen. Dies setzt leistungsfähige Datenarchitekturen, BPM-Plattformen und integrierte Kontrollmechanismen voraus.



10. Empfehlungen für Entscheider

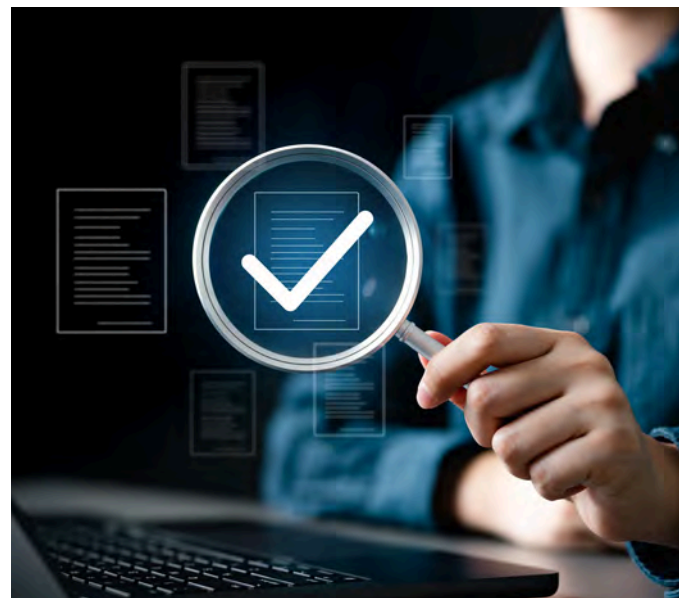
- > Behandeln Sie Compliance als strategische Managementaufgabe und nicht als isolierte Pflicht.
- > Verankern Sie Data Governance, Datenqualität und Nachvollziehbarkeit in der Unternehmensarchitektur.
- > Priorisieren Sie Prozesse mit hohem Risiko- und Volumenpotenzial, etwa KYC, AML und Sanktionsprüfung.
- > Setzen Sie auf Compliance by Design statt auf nachträgliche Kontrollen.
- > Investieren Sie in BPM-Plattformen und systemübergreifende Integration, um Medienbrüche zu vermeiden.
- > Definieren Sie klare Verantwortlichkeiten, Eskalationswege und Kontrollpunkte.
- > Nutzen Sie Automatisierung zur Risikominderung, aber behalten Sie fachliche Kontrolle über Ausnahmen.
- > Messbare KPIs für Qualität, Durchlaufzeit, Trefferquote und Auditfähigkeit etablieren.
- > Führen Sie regelmäßige Reviews zu regulatorischen Änderungen, Datenqualität und Prozesswirksamkeit durch.
- > Planen Sie Governance und Compliance als festen Bestandteil der digitalen Transformation.

11. Schlussfolgerung

Unternehmen, die in einem dynamischen regulatorischen Umfeld erfolgreich bleiben wollen, benötigen mehr als punktuelle Kontrollen oder einzelne Softwarelösungen. Sie brauchen eine integrierte Architektur aus Governance, Datenqualität, Prozessautomatisierung und nachvollziehbarer Entscheidungslogik. Genau diese Verbindung schafft regulatorische Bereitschaft, operative Effizienz und strategische Resilienz.

Compliance by Design, unternehmensweite Data Governance und systemübergreifende Integration sind keine optionalen Verbesserungen, sondern zentrale Voraussetzungen für nachhaltige Wettbewerbsfähigkeit. Wer diese Themen konsequent umsetzt, reduziert Risiken, stärkt das Vertrauen von Stakeholdern und schafft die Grundlage für skalierbares Wachstum.

Die Zukunft gehört Organisationen, die Compliance nicht als Bremse, sondern als Enabler verstehen. Sie nutzen Transparenz, Automatisierung und belastbare Governance, um schneller, sicherer und widerstandsfähiger zu handeln. Damit wird Compliance zu einem echten Werttreiber der digitalen Transformation.



Verzeichnis der TOLERANT Softwareprodukte

Die TOLERANT Software GmbH bietet eine Reihe von hochentwickelten Tools an, die darauf ausgelegt sind, Unternehmen in verschiedenen Aspekten des Datenmanagements zu unterstützen. Diese Produkte ermöglichen eine verbesserte Datenqualität, Compliance mit regulatorischen Anforderungen und effizientere Geschäftsprozesse. Im Folgenden wird eine Übersicht über die Kernprodukte von TOLERANT und ihre spezifischen Funktionen gegeben.

1. **TOLERANT Match**

Funktion: Dieses Tool dient der Identifikation und Zusammenführung von Duplikaten innerhalb von Datenbeständen. Es ermöglicht eine effiziente und präzise Datenbereinigung, was die Grundlage für zuverlässige Analysen und Geschäftsentscheidungen bildet.

2. **TOLERANT Post**

Funktion: TOLERANT Post gewährleistet die Korrektheit und Vollständigkeit von Adressdaten. Es unterstützt die Standardisierung und Bereinigung von Adressinformationen, was nicht nur die Kundenkommunikation optimiert, sondern auch die Zustellbarkeit von postalischen Sendungen verbessert.

3. **TOLERANT Bank**

Funktion: TOLERANT Bank prüft Bankdaten wie Kontonummer und Bankleitzahl und korrigiert diese gegebenenfalls. BIC und IBAN werden automatisch ermittelt.

4. **TOLERANT MPM (Marketing Permission Management)**

Funktion: TOLERANT MPM verwaltet die Einwilligungen und Berechtigungen für Marketingaktivitäten und stellt sicher, dass alle Kundenkommunikationen den gesetzlichen Vorgaben und den Wünschen der Kunden entsprechen.

5. **TOLERANT PEP**

Funktion: Ein spezialisiertes Tool zur Identifizierung politisch exponierter Personen (PEPs) in Kunden- und Geschäftspartnerdaten. Es hilft Unternehmen, Compliance-Anforderungen wie die Anti-Geldwäsche-Richtlinien (AML) zu erfüllen.

6. **TOLERANT Name**

Funktion: TOLERANT Name strukturiert Namensbestandteile und generiert daraus korrekte Briefanreden, so dass Kunden stets richtig angesprochen werden.

7. **TOLERANT Sanction**

Funktion: Dieses Tool überprüft Personen und Unternehmen gegen nationale und internationale Sanktionslisten. Es ist entscheidend für die Einhaltung von Compliance-Vorschriften und verhindert Geschäftsbeziehungen mit sanktionierten Einheiten.

8. **TOLERANT Move**

Funktion: TOLERANT Move ermittelt Umzugsdaten von unbekannt verzogenen Empfängern und erkennt verstorbene Personen im Adressbestand.

Diese Produktreihe von TOLERANT deckt ein breites Spektrum an Funktionen ab, von der Datenbereinigung über Compliance-Überwachung bis hin zum Management von Kundenberechtigungen, und bietet damit umfassende Unterstützung für das Datenmanagement in modernen Unternehmen.

