

UMFASSENDE LEITFADEN:

Compliance sichern, Effizienz steigern, Datenaustausch zentral lösen.

Wie Sie mit nur einer Plattform mehrere Vorgaben erfüllen
— von ISO 27001 und DSGVO bis NIS-2, TISAX®, DORA und CRA.

Inhaltsverzeichnis.

- 1 EXECUTIVE SUMMARY.
- 2 DIE HERAUSFORDERUNG: STEIGENDE COMPLIANCE-ANFORDERUNGEN.
- 3 DIE WICHTIGSTEN REGULARIEN IM ÜBERBLICK.
- 4 SCHNITTMENGEN UND SYNERGIEN — DER SCHLÜSSEL ZUR EFFIZIENZ.
 - | Gemeinsame Anforderungen auf einen Blick
 - | Wie Unternehmen die Synergien nutzen können
- 5 BRANCHEN UND IHRE ANFORDERUNGEN.
 - | Unternehmen
 - | Ämter und Behörden
 - | Gesundheitswesen
 - | Finanz- und Versicherungsunternehmen
- 6 EFFIZIENZ DURCH KONSOLIDIERUNG: SO HILFT FTAPI.
- 7 FAZIT UND HANDLUNGSEMPFEHLUNGEN.

Executive Summary.

Datenschutz, Cybersicherheit, Resilienz und Nachvollziehbarkeit sind für Unternehmen und Behörden nicht mehr optional — sie sind gesetzlich verankerte Pflicht. Richtlinien und Verordnungen wie **ISO 27001**, **DSGVO**, **NIS-2**, **DORA**, **TISAX®** oder **CRA** prägen die operative Realität — von der Industrie über das Gesundheitswesen bis zur öffentlichen Verwaltung.

Mit steigenden Anforderungen wachsen auch die Herausforderungen: Wie lassen sich die Pflichten effizient, nachhaltig und ohne übermäßige Ressourcen umsetzen?

Die gute Nachricht: Viele Regularien überschneiden sich in ihren Anforderungen. Wer diese Schnittmengen erkennt und gezielt nutzt, kann mit einer Lösung gleich mehrere Compliance-Vorgaben erfüllen — und dabei **Prozesse vereinfachen**, statt sie umständlicher zu machen.

Hier setzt FTAPI an: Als **Plattform für sicheren und automatisierten Datenaustausch** hilft FTAPI, regulatorische Vorgaben umzusetzen — schnell, wirtschaftlich und sicher. Compliance wird beim Datenaustausch dann nicht zur Bremse, sondern zum Katalysator digitaler Effizienz.

Dieser Leitfaden zeigt,

- was die aktuellen Regularien von welchen Branchen in Sachen Datensicherheit fordern,
- welche Schnittmengen sich ergeben,
- wie Unternehmen mehrere Anforderungen mit einer **zentralen Plattformlösung effizient und zukunftsicher erfüllen können.**



Die Herausforderung: Steigende Compliance-Anforderungen.

In nahezu allen Branchen nimmt der regulatorische Druck spürbar zu. Industrieunternehmen, Krankenhäuser, Versicherungen und Behörden müssen neue oder verschärfte Vorgaben umsetzen, die tief in IT-Systeme, Geschäftsprozesse und Sicherheitsarchitekturen eingreifen.

Der erste Eindruck ist dabei ein unübersichtliches **Netz an Vorschriften**:

- Die **Datenschutz-Grundverordnung (DSGVO)** stellt hohe Anforderungen an den Umgang mit personenbezogenen Daten.
- **ISO 27001** verlangt den Aufbau eines umfassenden Informationssicherheitsmanagementsystems (ISMS).
- Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** stellt besondere Anforderungen an den **Schutz kritischer Infrastrukturen (KRITIS)**.
- Die **NIS-2-Richtlinie** weitet die Cybersicherheitsvorgaben der NIS-Richtlinie 2016 von KRITIS-Unternehmen auf mehr Branchen und Unternehmensgrößen aus.
- **DORA (Digital Operational Resilience Act)** verpflichtet Finanz- und Versicherungsunternehmen zu digitaler Resilienz und Cybersicherheit.
- **TISAX®** adressiert Sicherheitsstandards in der Automobilzulieferkette.
- Der **Cyber Resilience Act (CRA)** bringt neue Pflichten für Hersteller digitaler Produkte, unter anderem in Bezug auf Secure-by-Design und Schwachstellenmanagement.
- **BSI C5** definiert Anforderungen für die geprüfte Sicherheit von Cloud-Diensten und wird in Ausschreibungen zunehmend vorausgesetzt.

So unterschiedlich die Regelungen auch sind — ihr Ziel ist dasselbe: **Vertrauen schaffen durch Sicherheit, Transparenz und Nachvollziehbarkeit im digitalen Raum.**

Die Realität in vielen Organisationen sieht jedoch anders aus: Zwischen dem Wunsch nach Automatisierung und Effizienz einerseits und den komplexen Compliance-Vorgaben andererseits entstehen Spannungsfelder. Besonders im Mittelstand oder im öffentlichen Sektor fehlen häufig Ressourcen, Fachwissen oder IT-Kapazitäten.

Viele reagieren mit Insellösungen: ein Tool für den sicheren E-Mail-Versand, ein weiteres zur Verwaltung von Zugriffsrechten, ein drittes für Dokumentation und Nachweispflichten. Das Resultat sind redundante Prozesse, fragmentierte Sicherheitsstrukturen — und Risiken im Fall von Störungen oder Prüfungen.

Die Folgen unzureichender Umsetzung reichen von Bußgeldern und Reputationsverlusten über Projekt- und Lieferkettenrisiken bis hin zu strategischen Nachteilen bei Ausschreibungen oder Zertifizierungen. Gleichzeitig verursachen ineffiziente Prozesse unnötige Betriebskosten und beeinträchtigen die digitale Wettbewerbsfähigkeit.

Die **Lösung** liegt in einem integrierten, ganzheitlichen Ansatz: Wer **Compliance als Bestandteil effizienter digitaler Prozesse** denkt, erreicht beides — Rechtssicherheit und Zukunftsfähigkeit.



Die wichtigsten Regularien im Überblick.

Der folgende Überblick fasst die **wichtigsten Regularien** kompakt zusammen. Dabei liegt der Fokus nicht auf juristischen Details, sondern auf den Zielen, Schnittmengen (dazu später noch mehr) und relevanten Branchen:

Richtlinie	Ziel	Branchen	Schnittmengen mit
ISO 27001	Informationssicherheitsmanagementsystem (ISMS) einführen	Alle	DSGVO, TISAX® (basiert auf ISO 27001) DORA, NIS-2
DSGVO	Schutz personenbezogener Daten, Transparenz und Zweckbindung bei der Verarbeitung	Alle	ISO 27001, TISAX®, DORA, KRITIS
NIS-2	Cybersicherheit in kritischen und wichtigen Sektoren	KRITIS, größere Unternehmen, Verwaltung, digitale Dienste	ISO 27001, DORA, KRITIS
DORA	Digitale Betriebsstabilität in der Finanzbranche	Finanzunternehmen, Versicherungen & relevante IT-Dienstleister	ISO 27001, DSGVO, NIS-2, TISAX®
TISAX®	Einheitliche Informationssicherheit in der Automobilbranche	Automobilhersteller, Zulieferer	ISO 27001 (Grundlage von TISAX®), DSGVO, CRA (softwaregestützte Komponenten)
CRA	Cybersicherheit für digitale Produkte	Hersteller, Entwickler, Softwareanbieter	ISO 27001, DSGVO, TISAX®
KRITIS (BSI)	Schutz kritischer Infrastrukturen durch Mindeststandards, Meldesysteme und Auditpflichten	Energie, Wasser, Gesundheit, Ernährung, Finanzen, Verwaltung	NIS-2, ISO 27001, DSGVO
BSI C5 (kein Gesetz, aber oft gefordert)	Nachweisbare Sicherheit in Cloud-Umgebungen durch standardisierte Kontrollanforderungen	Cloud-Anbieter, Softwareanbieter, IT-Dienstleister	ISO 27001, DSGVO, KRITIS, teilweise NIS-2

Obwohl der **C5-Katalog des BSI** kein Gesetz ist, spielt er in der Praxis eine zentrale Rolle: Er gilt als anerkannter Prüfstandard für Cloud-Dienste — und ist oft Pflicht in öffentlichen Ausschreibungen sowie zunehmend auch in der Privatwirtschaft. Der **Katalog** basiert größtenteils auf ISO 27001, ergänzt um cloudspezifische Anforderungen wie Zugriffskontrollen, Datenlöschung und Protokollierung. Eine erfolgreiche C5-Prüfung erfüllt damit viele Vorgaben aus ISO 27001, DSGVO oder NIS-2 — und schafft Vertrauen bei Kunden und Behörden.



US-Anbieter unterliegen zusätzlich dem **CLOUD Act** — sie können verpflichtet werden, Daten an US-Behörden herauszugeben, selbst wenn diese auf Servern in der EU gespeichert sind. Um die hohen Anforderungen an Datenschutz und Informationssicherheit zu erfüllen, zählt daher neben dem Serverstandort auch die **rechtliche Kontrolle über die Infrastruktur**. Nur europäische Anbieter mit Hosting und Hauptsitz in der EU gewährleisten echte Datensouveränität.

Schnittmengen und Synergien — der Schlüssel zur Effizienz.

Die zentralen Richtlinien und Verordnungen haben mehr gemeinsam, als es auf den ersten Blick scheint. Wer sie strukturiert betrachtet, erkennt **zahlreiche Schnittmengen** — und damit die Chance, mehrere Vorschriften effizient zu erfüllen.

Gemeinsame Anforderungen auf einen Blick

Die Vorschriften bauen auf **ähnlichen Grundprinzipien** auf. In vielen Fällen handelt es sich um strukturell gleichartige Anforderungen mit leicht abweichender Ausprägung.

Hier sind die wichtigsten **Gemeinsamkeiten der Regularien im Überblick:**

Anforderung	ISO 27001	DSGVO	NIS-2	DORA	TISAX®	CRA	KRITIS (BSI)	BSI C5
Informationssicherheitsmanagement (ISMS)	✓	●	✓	✓	✓	●	✓	✓
Zugriffskontrolle & Berechtigungen	✓	✓	✓	✓	✓	✓	✓	✓
Datenschutz & Vertraulichkeit	●	✓	✓	✓	✓	✓	✓	✓
Datenverschlüsselung	✓	✓	✓	✓	✓	✓	✓	✓
Auditierbarkeit & Protokollierung	✓	✓	✓	✓	✓	●	✓	●***
Meldepflicht bei Sicherheitsvorfällen	●	✓*	✓**	✓**	●	✓	✓	✓
Schwachstellen- & Risikomanagement	✓	●	✓	✓	✓	✓	✓	✓
Sichere Kommunikation & Datentransfer	✓	✓	✓	✓	✓	●	✓	✓
Business Continuity & Notfallplanung	✓	●	✓	✓	✓	●	✓	✓
Lieferanten- & Drittanbietersteuerung	✓	✓	✓	✓	✓	●	●	●
Technische & organisatorische Maßnahmen (TOMs)	✓	✓	✓	●	✓	✓	✓	✓

Legende:

- ✓ = explizit geregelt / Kernanforderung
- = implizit enthalten oder ergänzend relevant

* Max. 72h-Meldepflicht nach DSGVO Art. 33 bei Datenpannen mit Personenbezug

** Max. 24h-Meldepflicht nach DORA und NIS-2

*** C5 enthält keine eigene Meldepflicht — ergibt sich aus gesetzl. Vorgaben (z. B. DSGVO)

| Wie Unternehmen die Synergien nutzen können

Unternehmen können durch **ganzheitliche Maßnahmen mehrere Regularien parallel bedienen** — und so Compliance und Effizienz steigern.

1 | Auf einheitliche Sicherheitsplattform statt Insellösungen setzen:

Mit einer umfassenden Plattformlösung wie FTAPI lassen sich zentrale Sicherheitsanforderungen (z. B. Zugriff, Verschlüsselung, Nachvollziehbarkeit) systematisch und organisationsweit erfüllen — statt isoliert in einzelnen Teams oder Tools.

2 | Nachweisdokumentation automatisieren:

Protokolle, Zugriffslisten, Transferlogs und Audit-Trails sind für viele Vorschriften Pflicht. Eine integrierte Lösung spart hier viel manuelle Dokumentationsarbeit und minimiert Fehlerquellen.

3 | Meldepflichten effizient umsetzen:

Ein zentrales Incident-Management inklusive Eskalationsketten, Nachverfolgung und Reporting sorgt dafür, dass gesetzlich vorgeschriebene Reaktionszeiten (24 Stunden bei NIS-2 und DORA, 72 Stunden bei Datenpannen nach DSGVO) eingehalten werden.

4 | Sensible Daten einheitlich schützen:

Ob Patientendaten oder Schadendokumente — werden Daten grundsätzlich klassifiziert und über eine abgesicherte Plattform verwaltet und versendet, lassen sich zentrale Anforderungen wie Verschlüsselung, Zugriffskontrolle und Protokollierung gleichzeitig erfüllen.

5 | Synergien bei Audits und Zertifizierungen nutzen:

Wer ISO 27001-konforme Prozesse aufsetzt, erfüllt beispielsweise bereits einen großen Teil der Anforderungen aus TISAX® oder NIS-2. Einmalige Vorbereitung, mehrfacher Nutzen.

Branchen und ihre Anforderungen.

Regulatorische Anforderungen unterscheiden sich von Branche zu Branche — aber in der Umsetzung zeigen sich viele Gemeinsamkeiten: Zugriffskontrolle, Verschlüsselung, Dokumentation, Incident Response und Prozesssicherheit sind fast überall gefordert.

Dieses Kapitel zeigt pro Zielgruppe, **welche Vorschriften entscheidend sind, wo sie sich überschneiden** — und **welche Herausforderungen in der Praxis immer wieder auftreten**.

Unternehmen

Wichtige Regelwerke:

ISO 27001, DSGVO, NIS-2, TISAX® (bei OEM-Nähe), CRA (bei digitalen Produkten)

Typische Herausforderungen:

Unternehmen stehen vor der Aufgabe, gleichzeitig wachsenden regulatorischen Anforderungen und dem Wettbewerbsdruck gerecht zu werden. Gerade im Mittelstand fehlt es häufig an spezialisierten Ressourcen für Datenschutz, Informationssicherheit und Prozess-Governance. In vielen Fällen wurden technische Lösungen historisch gewachsen implementiert — was zu isolierten Tools, redundanten Workflows und fehlender Nachvollziehbarkeit führt.

Zentrale Schnittmengen:

Nahezu alle relevanten Standards verlangen von Unternehmen:

- Zugriffskontrolle auf sensible Daten (ISO 27001, DSGVO, TISAX®)
- Protokollierung & Nachvollziehbarkeit bei Dateiaktionen (ISO 27001, DORA)
- Business Continuity (ISO 27001, DORA, KRITIS, NIS-2)

Typischer Umsetzungsfehler:

Um die Anforderungen zu erfüllen, setzen viele Unternehmen auf Einzeltools, zum Beispiel ein Produkt für E-Mail-Verschlüsselung, ein anderes für Zugriffsverwaltung. Dadurch entstehen Schnittstellenprobleme, unvollständige Audit Trails und hoher Verwaltungsaufwand — was letztlich sowohl Sicherheit als auch Produktivität beeinträchtigt und unnötige Kosten verursacht.

Praxisbeispiel:

Ein Zulieferer verarbeitet technische Konstruktionsdaten für einen Original Equipment Manufacturer (OEM). Gleichzeitig enthält die Kommunikation personenbezogene Daten (z. B. Bewerbungen, Projektverantwortliche). Gefordert sind:

- TISAX®-konformer Schutz von Entwicklungsdaten
- DSGVO-konformer Umgang mit personenbezogenen Daten
- Nachweisbare Zugriffskontrolle & Dokumentation nach ISO 27001

Ein integrierter Ansatz, der alle relevanten Anforderungen systematisch zusammenführt, kann hier den Unterschied machen — technisch wie organisatorisch.

Ämter und Behörden

| Wichtige Regelwerke:

DSGVO, KRITIS (BSI), ISO 27001, CRA (bei digitalen Verwaltungsdiensten)

| Typische Herausforderungen:

Öffentliche Verwaltungen verarbeiten hochsensible Bürgerdaten, stehen unter Digitalisierungsdruck und sind oft mit veralteter IT-Infrastruktur konfrontiert. Gleichzeitig fehlt es an Personal, Budget und standardisierten Prozessen für Informationssicherheit und Datenschutz. Besonders in föderalen Strukturen entstehen uneinheitliche Umsetzungsmuster — mit erhöhtem Risiko für Sicherheitsvorfälle. Bei Nutzung externer Cloud-Dienste verlangen viele Stellen zudem einen C5-Nachweis — etwa im Rahmen öffentlicher Ausschreibungen.

| Zentrale Schnittmengen:

- Zugriffskontrolle und rollenbasierte Berechtigungssysteme (ISO 27001, KRITIS, DSGVO)
- Verschlüsselung und sichere Kommunikation bei Datentransfers (DSGVO, ISO 27001, KRITIS)
- Revisionssichere Protokollierung und Nachvollziehbarkeit (ISO 27001, C5, teilweise KRITIS)
- C5-Nachweis bei Nutzung externer Cloud-Dienste (ISO 27001, DSGVO)

| Typischer Umsetzungsfehler:

Viele Behörden verlassen sich weiterhin auf unverschlüsselte E-Mails oder ungeschützte Dateifreigaben. Daten werden über unterschiedliche Systeme transportiert, ohne zentrale Dokumentation oder Zugriffskontrolle. Die Folge sind Intransparenz, ineffiziente Prozesse und hohe Prüfrisiken.

| Praxisbeispiel:

Eine Stadtverwaltung digitalisiert das Antragswesen für soziale Leistungen. Formulare mit Personen- und Gesundheitsdaten werden eingereicht, weitergeleitet und bearbeitet. Dabei greifen mehrere Abteilungen und externe Partner auf die Daten zu. Erforderlich ist:

- DSGVO-konformer Umgang mit personenbezogenen Daten
- Nachvollziehbarer Zugriff und automatisierte Weiterleitung
- Nachweisbare Prozesskette zur Auditfähigkeit (KRITIS)

Nur mit einer integrierten, standardisierten Umsetzung lassen sich diese Anforderungen effizient und rechtssicher erfüllen.

Gesundheitswesen

| Wichtige Regelwerke:

DSGVO, KRITIS (BSI), ISO 27001

| Typische Herausforderungen:

Krankenhäuser, Labore und Gesundheitseinrichtungen arbeiten mit besonders schützenswerten personenbezogenen Daten, sind oft KRITIS-relevant und müssen gleichzeitig Versorgungssicherheit und Datenschutz garantieren. Dazu kommen hohe Dokumentationspflichten, Fachkräftemangel und ein fragmentiertes Zusammenspiel aus Klinik-IT, Partnern und Drittsystemen.

| Zentrale Schnittmengen:

- Schutz besonderer Datenkategorien nach Art. 9 DSGVO
- Zugriffsbeschränkung und rollenbasierte Systemnutzung (KRITIS, ISO 27001)
- Technisch-organisatorische Maßnahmen für Verarbeitung, Speicherung, Übertragung (DSGVO, NIS-2)
- Notfallkonzepte und Business Continuity Management (KRITIS, ISO 27001)

| Typischer Umsetzungsfehler:

Medizinische Daten werden häufig über unsichere Kanäle wie Fax oder in TLS-verschlüsselten E-Mails geteilt. Systeme sind nicht zentral verknüpft, Protokollierung fehlt oder ist nur teilautomatisiert. Das erschwert Audits, verursacht Mehraufwand und birgt erhebliche Datenschutzrisiken.

| Praxisbeispiel:

Ein Krankenhaus versendet radiologische Befunde an externe Fachärzte und verarbeitet personenbezogene Anamnesedaten in internen Systemen. Gleichzeitig muss es auf Cybervorfälle vorbereitet sein. Umgesetzt werden muss:

- Verschlüsselte Übertragung und Zugriffsnachweis (DSGVO, ISO 27001)
- KRITIS-konformes Notfallmanagement & Kommunikationsfähigkeit
- Schutz bei Datenweitergabe an Partner & externe Dienste

Ein einheitlicher, dokumentierter und revisionssicherer Datenfluss ist hier die Basis für Sicherheit und Versorgungskontinuität.

Finanz- und Versicherungsunternehmen

Wichtige Regelwerke:

DORA, DSGVO, ISO 27001

Typische Herausforderungen:

Versicherer und Finanzdienstleister verfügen über hoch digitalisierte Prozesse, große Datenmengen und komplexe Dienstleisterketten. Die Anforderungen an digitale Resilienz, revisionsfähige Abläufe und Datenschutz steigen rasant — insbesondere durch DORA, das branchenweit neue Maßstäbe für ICT-Risikomanagement setzt.

Zentrale Schnittmengen:

- ICT-Risikomanagement und technische Sicherheitsmaßnahmen (DORA, ISO 27001)
- Datenschutz durch Technik und Protokollierung personenbezogener Daten (DSGVO)
- Zugriffssteuerung und Nachweisbarkeit (ISO 27001, DORA)
- Meldepflichten bei Vorfällen (DORA, DSGVO)

Typischer Umsetzungsfehler:

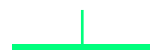
Schadendokumente oder Vertragsdaten werden über E-Mail, Fileserver oder Drittportale ausgetauscht — ohne klare Zugriffskontrolle oder vollständige Protokollierung. Im Notfall fehlen definierte Kommunikationswege — was die Einhaltung der 24-Stunden-Meldepflichten nach DORA gefährdet.

Praxisbeispiel:

Eine Versicherung verarbeitet große Mengen personenbezogener Daten im Rahmen digitaler Schadenabwicklung. Dokumente werden mit Dienstleistern, Partnern und Gutachtern ausgetauscht. Gleichzeitig müssen Incident-Response-Prozesse DORA-konform dokumentiert und automatisiert ausführbar sein. Gefordert sind:

- DSGVO-konformer, verschlüsselter Dokumentenaustausch
- Notfallkommunikation und Meldekette im Sinne von DORA
- Rollenbasierter Zugriff und revisionsfähige Ablage (ISO 27001)

Ein systematischer, zentral steuerbarer Ansatz minimiert Risiken, steigert Nachvollziehbarkeit und reduziert den Aufwand bei Prüfungen.



Diese Beispiele zeigen: **Die Anforderungen mögen unterschiedlich benannt sein — doch inhaltlich überschneiden sie sich oft stark.** Genau hier liegt das Potenzial, mit einem zentralen System gleich mehrere Anforderungen zu erfüllen — effizient, nachvollziehbar und ohne doppelte Arbeit.

Wie das konkret funktioniert, zeigt das nächste Kapitel.

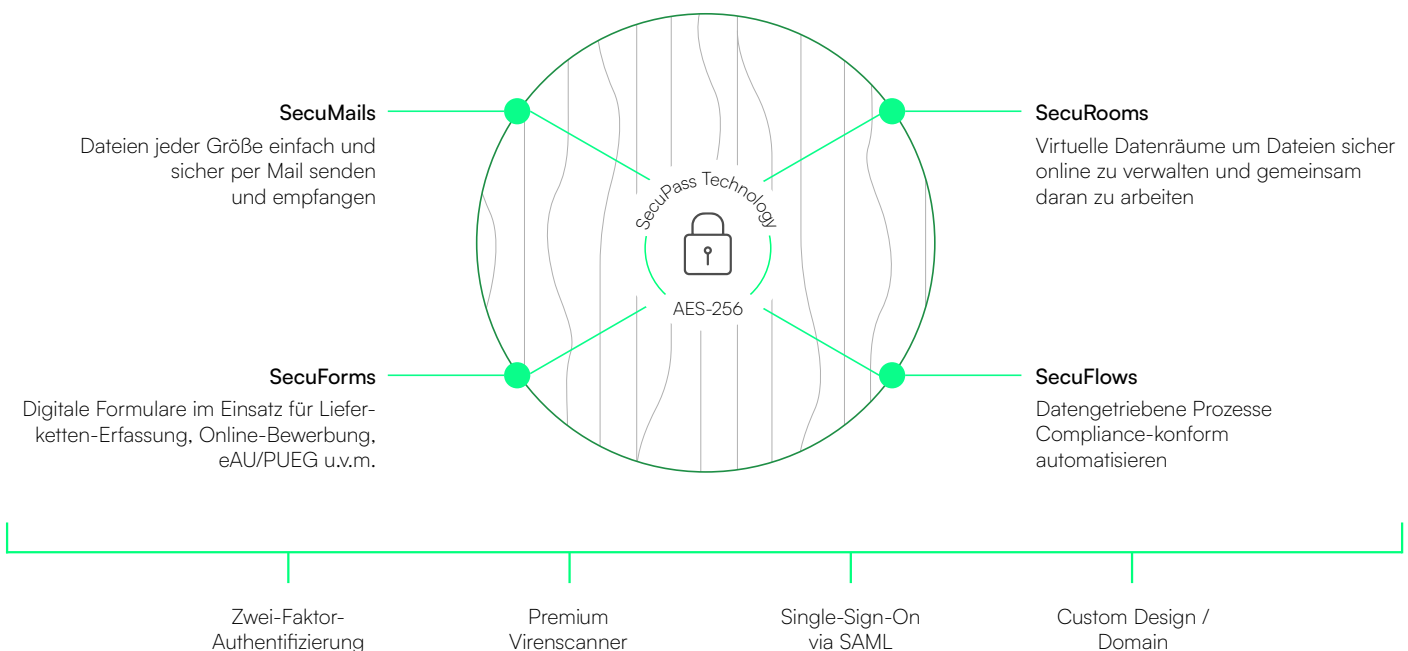
Effizienz durch Konsolidierung: So hilft FTAPI.

Regulatorische Anforderungen umzusetzen ist meist kein technisches, sondern ein organisatorisches Problem: zu viele parallele Systeme, zu wenig Integration, zu viel manuelle Arbeit. Genau hier setzt FTAPI an — als **zentrale Lösung für strukturierte, gesicherte Kommunikationsprozesse**. Die Plattform vereint:

- Ende-zu-Ende-verschlüsselten Datentransfer via E-Mail
- Sichere Datenräume mit granularer Rechtevergabe
- Formularbasierte Uploads für standardisierte Anfragen und Prozesse
- Automatisierte Datenworkflows, z. B. mit Freigabe-, Prüf- oder Transferlogik
- Zentrale Auditierung und Protokollierung

Plus: **FTAPI ist erfolgreich nach dem BSI C5 Typ 2 Standard testiert** — durch die renommierte deutsche Wirtschaftsprüfungsgesellschaft HKKG.

So können Unternehmen und Behörden verschiedenste Anforderungen abdecken — **mit einer einheitlichen Plattform**, bestehend aus vier Lösungen und ausgewählten Add-ons, die sich nahtlos in vorhandene Infrastrukturen einfügen.



Beispiele: So löst FTAPI zentrale Compliance-Anforderungen

Hier sehen Sie, wie sich zentrale regulatorische Anforderungen mit FTAPI effizient, revisionssicher und benutzerfreundlich umsetzen lassen.

1

Sichere Notfallkommunikation & Business Continuity

Vorgaben: ISO 27001, DORA, NIS-2

Was Sie damit lösen: Handlungsfähigkeit bei Cyberangriffen, Ausfällen oder Krisensituationen sicherstellen — inkl. dokumentierter Reaktionsprozesse.

Das bietet FTAPI:

(SecuFlows • SecuMails)

- Ausfallsichere Kommunikation über extern gehostete Plattform
- Zugriff über Browser und mobile Geräte — unabhängig von der internen IT
- Prozessmodellierung und Vorfallmanagement nach BPMN 2.0
- Revisionssichere Protokolle für Prüfbehörden

Vorteil: Ihre Business Continuity ist gesichert und Sie bleiben auch im Ernstfall reaktionsfähig — unabhängig von der lokalen Infrastruktur.

2

Datenverschlüsselung & Datensouveränität

Vorgaben: DSGVO, ISO 27001, NIS-2, KRITIS (BSI)

Was Sie damit lösen: Vertraulichkeit von Daten sicherstellen — bei Erfassung, Speicherung und Übertragung.

Das bietet FTAPI:

(SecuMails • SecuRooms • SecuForms • SecuFlows)

- Ende-zu-Ende-Verschlüsselung mit Zero-Knowledge-Prinzip
- Kein Zugriff durch Admins/Drittparteien — auch nicht FTAPI
- Formulare sicher senden, inkl. Captcha und Authentifizierung
- Made & hosted in Germany — für maximale Datensouveränität
- Verschlüsselter Austausch über Mail, Datenräume oder Workflows
- Löscho- und Rückruffunktionen für volle Kontrolle

Vorteil: Datenschutz auf höchstem Niveau — nachvollziehbar und manipulationssicher.

3

Zugriffskontrolle & Berechtigungen

Vorgaben: ISO 27001, TISAX®, DORA, DSGVO

Was Sie damit lösen: Rechts- und auditkonforme Steuerung von Nutzerrechten, Datenzugriffen und Rollen — intern wie extern

Das bietet FTAPI:

(SecuRooms • SecuMails)

- Gruppenbasierte Rechtevergabe & Benutzerrollen (inkl. AD-Integration)
- Nachvollziehbarer Zugriff in Datenräumen und Mail-Verkehr
- Individuelle Löschrregeln und Datei-Klassifikation
- Zugriffs- und Downloadprotokolle für Prüfungen & Audits

Vorteil: Klare Zugriffskonzepte sorgen für Nachvollziehbarkeit und Revisionssicherheit.

4

Sichere Kommunikation & Datentransfer

Vorgaben: DSGVO, ISO 27001, TISAX®, KRITIS (BSI)

Was Sie damit lösen: Sicherer Austausch sensibler Daten — ohne Medienbrüche oder Schatten-IT

Das bietet FTAPI:

(SecuMails • SecuRooms)

- Verschlüsselter Dateiversand via Outlook oder Browser (bis 100 GB)
- Dateiversand per sicherem Link mit Zugriffskontrolle und Fristen
- Externe Kommunikation ohne IT-Integration
- Revisionssichere Datenräume für projektbezogenen Datenaustausch
- Mobile Zugriffsmöglichkeiten und moderne Benutzerführung

Vorteil: Maximaler Schutz mit minimalem Aufwand — sicherer Austausch ohne Medienbrüche.

Fazit und Handlungsempfehlungen.

Die Umsetzung regulatorischer Anforderungen ist für Organisationen längst kein Randthema mehr — sie ist fester Bestandteil operativer und strategischer Entscheidungen. Gleichzeitig steigen Komplexität, Dokumentationspflichten und die Erwartung, mit bestehenden Ressourcen auszukommen.

Der Schlüssel liegt nicht in zusätzlichen Einzellösungen, sondern in einem **integrierten Ansatz**: Wer die inhaltlichen Schnittmengen der verschiedenen Regelwerke erkennt, kann **technische und organisatorische Maßnahmen gezielt bündeln** — und mehrere Anforderungen effizient erfüllen.

Eine **zentrale Plattform für sicheren Datenaustausch, klare Zugriffsstrukturen und automatisierte Protokollierung** kann dabei helfen, Komplexität zu reduzieren, Nachweispflichten effizient zu erfüllen und Risiken zu minimieren.

Organisationen sollten jetzt:

- prüfen, **welche regulatorischen Anforderungen** sie aktuell betreffen — und welche in Zukunft relevant werden,
- analysieren, **wo sich Anforderungen überschneiden** und heute bereits doppelt oder manuell umgesetzt werden,
- ihre bestehende **Systemlandschaft auf Medienbrüche und redundante Tools** hinterfragen,
- und identifizieren, **welche Prozesse sich zentral, sicher und nachvollziehbar bündeln lassen** — etwa beim Datentransfer, bei der Zugriffskontrolle oder bei Meldepflichten.



Bereit für den nächsten Schritt?

Lassen Sie uns gemeinsam herausfinden, wie Sie Ihre Compliance-Anforderungen effizienter lösen können.

Unverbindliches Gespräch vereinbaren

FTAPI Software GmbH

Steinerstr. 15f
81369 München

T: +49 89 230 6954 0
F: +49 89 230 6954 10
info@ftapi.com

ftapi.com

HINWEIS

Dieser Guide stellt keine rechtliche Beratung dar. Alle Inhalte wurden mit größtmöglicher Sorgfalt erstellt, erheben jedoch keinen Anspruch auf Vollständigkeit oder rechtliche Verbindlichkeit.

TISAX® ist eine eingetragene Marke der ENX Association. Die FTAPI Software GmbH steht in keiner geschäftlichen Beziehung zu ENX. Mit der Nennung der Marke TISAX® ist keine Aussage des Markeninhabers zur Geeignetheit der hier beworbenen Leistungen verbunden.