					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P37S					Dokumenttitel: **Richtlinie zur Einhaltung gesetzlicher und regulatorischer Anforderungen**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

Ausgerichtet an Standards und Vorschriften

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clauses 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Maßnahme 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
EU GDPR	Articles 5, 6, 32, 33	
EU NIS2	Articles 21(2)(a), 21(2)(f), 23	
EU DORA	Articles 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Zweck

1.1 Diese Richtlinie legt den Ansatz der Organisation zur Identifizierung, Einhaltung und zum Nachweis der Einhaltung gesetzlicher, regulatorischer und vertraglicher Verpflichtungen fest.

1.2 Sie definiert klare Verantwortlichkeiten und konkrete Maßnahmen, damit das Unternehmen seine Compliance-Verpflichtungen erfüllen kann, einschließlich datenschutzrechtlicher Anforderungen, Cybersicherheitsrahmenwerken, Kundenvereinbarungen und Zertifizierungsstandards.

1.3 Sie stellt sicher, dass das Unternehmen auch ohne dediziertes Compliance-Team einen rechtssicheren Betrieb aufrechterhält, angemessen auf Vorfälle reagiert und eine durchgehende Auditbereitschaft sicherstellt.

1.4 Diese Richtlinie ist wesentlich, um eine Zertifizierung nach ISO/IEC 27001:2022 zu ermöglichen und externe Erwartungen von Kunden, Aufsichtsbehörden und Partnern zu erfüllen.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle Mitarbeitenden, Auftragnehmer, Freelancer und Drittanbieter

2.1.2 alle Services, Betriebsabläufe, Systeme und Datenverarbeitungstätigkeiten, bei denen die Organisation gesetzliche oder vertragliche Anforderungen erfüllen muss

2.1.3 alle Standorte und Geräte, die zur Verarbeitung geschäftlicher Informationen genutzt werden, unabhängig davon, ob diese lokal, remote oder cloudbasiert sind

2.2 Diese Richtlinie umfasst:

2.2.1 Datenschutzgesetze wie die DSGVO

2.2.2 Cybersicherheitsvorschriften wie NIS2

2.2.3 branchenspezifische Verpflichtungen, soweit anwendbar

2.2.4 Kundenverträge, Vertraulichkeitsvereinbarungen und Auditklauseln

2.2.5 freiwillige Zertifizierungen (z. B. ISO 27001) und interne Richtlinien, deren Einhaltung sichergestellt werden muss

3. Ziele

3.1 Rechenschaftspflicht schaffen: Eindeutige Verantwortlichkeiten für die Überwachung, Aktualisierung und Durchsetzung gesetzlicher, regulatorischer und vertraglicher Verpflichtungen festlegen.

3.2 Das Unternehmen schützen: Das Risiko von Rechtsverstößen, Bußgeldern, Datenschutzverletzungen und Reputationsschäden minimieren.

3.3 Auditbereitschaft sicherstellen: Nachvollziehbare Aufzeichnungen führen, die belegen, wie die Organisation ihre Compliance-Verpflichtungen erfüllt.

3.4 Integration in Richtlinien unterstützen: Sicherstellen, dass gesetzliche und regulatorische Pflichten in allen Richtlinien und Prozessen konsistent umgesetzt werden.

3.5 Ausnahmen transparent steuern: Sicherstellen, dass Ausnahmen von Compliance-Verpflichtungen dokumentiert, begründet und genehmigt werden, um Haftungsrisiken zu vermeiden.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführer (GM)

4.1.1 Trägt die Gesamtverantwortung für die Einhaltung gesetzlicher und regulatorischer Anforderungen in der Organisation.

4.1.2 Führt das Compliance-Register und stellt sicher, dass es aktuell bleibt.

4.1.3 Prüft Kundenverträge und stellt sicher, dass spezifische Verpflichtungen nachverfolgt und umgesetzt werden.

4.1.4 Genehmigt Ausnahmen von Compliance-Verpflichtungen nur, wenn diese rechtlich vertretbar sind und risikomindernde Maßnahmen bestehen.

4.2 Externe Berater (z. B. Rechts-, IT- oder Compliance-Berater)

4.2.1 Unterstützen den GM bei der Identifizierung anwendbarer Gesetze, Zertifizierungen und Verpflichtungen (z. B. DSGVO, NIS2, ISO 27001).

4.2.2 Beraten bei der Auslegung neuer Vorschriften oder Änderungen bestehender Gesetze.

4.2.3 Können bei Richtlinienaktualisierungen, Audits oder der Reaktion auf Verstöße unterstützen, wenn rechtliche Risiken bestehen.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Anforderungen an Überprüfung und Aktualisierung

9.1 Planmäßige jährliche Überprüfung

9.1.1 Diese Richtlinie muss alle 12 Monate durch den GM überprüft werden.

9.1.2 Die Überprüfung muss bestätigen:

9.1.2.1 die Relevanz im aktuellen gesetzlichen und vertraglichen Kontext

9.1.2.2 die zutreffende Berücksichtigung von Kundenvereinbarungen und Serviceverpflichtungen

9.1.2.3 die Ausrichtung am Compliance-Register und an anderen Richtlinien

9.2 Ereignisgesteuerte Aktualisierungen

9.2.1 Eine sofortige Überprüfung ist erforderlich, wenn:

9.2.1.1 ein neues Gesetz oder eine neue Vorschrift anwendbar wird (z. B. eine neue Datenschutzregelung)

9.2.1.2 ein Kunde komplexe Compliance-Vorgaben in seine Vereinbarung aufnimmt

9.2.1.3 ein Compliance-Verstoß oder Vorfall der Nichteinhaltung auftritt

9.2.1.4 das Unternehmen in einen regulierten Markt oder Sektor expandiert

9.3 Genehmigung von Aktualisierungen und Versionskontrolle

9.3.1 Alle Aktualisierungen müssen dokumentiert, versioniert und vom GM genehmigt werden.

9.3.2 Historische Versionen müssen zu Audit- und Rechtszwecken aufbewahrt werden.

9.4 Kommunikation von Änderungen

9.4.1 Mitarbeitende und Auftragnehmer müssen innerhalb von 5 Geschäftstagen nach Genehmigung über Richtlinienänderungen informiert werden.

9.4.2 Betroffene Lieferanten müssen aktualisierte Bedingungen ebenfalls bestätigen, bevor die Leistungserbringung fortgesetzt wird.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie wird durch die folgenden SME-Richtlinien unterstützt und durchgesetzt:

10.1.1 P3S – Richtlinie zur zulässigen Nutzung: Verhindert Verhaltensweisen, die gegen gesetzliche oder vertragliche Bedingungen verstoßen können (z. B. nicht autorisierte Dateifreigabe)

10.1.2 P8S – Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit: Schult Mitarbeitende zu Compliance-Verpflichtungen und dazu, wie Verstöße vermieden werden können

10.1.3 P14S – Richtlinie zur Datenaufbewahrung und Entsorgung: Stellt rechtmäßige Praktiken im Umgang mit Daten über den gesamten Datenlebenszyklus sicher

10.1.4 P17S – Richtlinie zu Datenschutz und Privatsphäre: Erfüllt Anforderungen der DSGVO und kundenseitige Anforderungen an die Datenverarbeitung

10.1.5 P30S – Incident-Response-Richtlinie: Legt fest, wie auf Datenschutzverletzungen oder Nichteinhaltung zu reagieren ist, einschließlich Meldefristen

10.1.6 P36S – Richtlinie zu Social Media und externer Kommunikation: Stellt sicher, dass öffentliche Kommunikation keine gesetzlichen oder regulatorischen Verpflichtungen verletzt

10.2 Jede verknüpfte Richtlinie setzt einen Teil des Rahmens zur rechtlichen Einhaltung um und muss abgestimmt mit den anderen angewendet werden.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Abschnitt 6.1 – Maßnahmen zum Umgang mit Risiken und Chancen: Umfasst Compliance-Risiken

11.1.2 Abschnitt 8.1 – Operative Planung und Steuerung: Verlangt die Durchführung von Prozessen, die gesetzliche und vertragliche Anforderungen erfüllen

11.2 ISO/IEC 27002

11.2.1 Maßnahme 5.36 – Gibt der Organisation Leitlinien für die Führung von Aufzeichnungen über Verpflichtungen und zur Sicherstellung angemessener Reaktionen auf gesetzliche und regulatorische Anforderungen

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Richtlinie und Verfahren: Verlangt formale Richtlinien zur Einhaltung

11.3.2 PM-1 – Plan für das Informationssicherheitsprogramm: Verlangt die Integration rechtlicher Einhaltung in die Sicherheitsplanung

11.3.3 CA-1 – Bewertung, Autorisierung und Überwachung

11.3.4 AU-1 – Audit-Richtlinie: Verlangt die Aufrechterhaltung von Nachweisen der Einhaltung

11.4 EU GDPR

11.4.1 Artikel 5 – Grundsätze der Datenverarbeitung einschließlich Rechenschaftspflicht

11.4.2 Artikel 6 – Rechtsgrundlage der Verarbeitung

11.4.3 Artikel 32 – Sicherheit der Verarbeitung

11.4.4 Artikel 33 – Meldung von Verstößen innerhalb von 72 Stunden

11.5 EU-NIS2-Richtlinie

11.5.1 Artikel 21(2)(a) und (f) – Interne Richtlinien für Risiko- und Compliance-Steuerung

11.5.2 Artikel 23 – Durchsetzung und Sanktionen bei Verstößen gegen Compliance-Verpflichtungen

11.6 EU-DORA-Verordnung

11.6.1 Artikel 5(2) – Aufsicht über das Management von IKT-Risiken

11.6.2 Artikel 9(1) – Interne Governance der Compliance

11.6.3 Artikel 17 – Vertragliche Vereinbarungen mit IKT-Dienstleistern

11.7 COBIT 2019

11.7.1 APO12 – Managed Risk: Stellt sicher, dass Compliance-Risiken nachverfolgt und behandelt werden

11.7.2 APO13 – Managed Security: Umfasst die risikobasierte Durchsetzung regulatorischer und vertraglicher Compliance

11.7.3 DSS01 – Managed Operations: Verlangt operative Bereitschaft zur Erfüllung gesetzlicher Verpflichtungen