					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P37					Dokumenttitel: **Richtlinie zur rechtlichen und regulatorischen Compliance**							
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**

1. Zweck

1.1 Diese Richtlinie legt den verbindlichen Rahmen für die Identifizierung, Steuerung und Einhaltung aller rechtlichen, regulatorischen und vertraglichen Verpflichtungen fest, die für die Informationssicherheit, den Datenschutz und die operativen Funktionen der Organisation relevant sind.

1.2 Ziel ist es, Verstöße gegen Compliance-Anforderungen zu verhindern, die zu Bußgeldern, rechtlicher Haftung, Betriebsstörungen, Reputationsschäden oder behördlichen Durchsetzungsmaßnahmen führen könnten.

1.3 Diese Richtlinie unterstützt die Integration von Compliance-Verpflichtungen in Governance, Risikomanagement, operative Prozesse, Projektlebenszyklen und die Systemarchitektur.

1.4 Sie stellt sicher, dass alle relevanten Verpflichtungen – über Rechtsordnungen, Branchen und regulatorische Geltungsbereiche hinweg – innerhalb der Organisation klar dokumentiert, bewertet, überwacht und durchgesetzt werden.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Abteilungen, Funktionen, Geschäftsbereiche und Personen, die im Namen der Organisation handeln, einschließlich:

2.1.1 unbefristet und befristet beschäftigter Mitarbeitender

2.1.2 Auftragnehmer, Berater und Praktikanten

2.1.3 Drittanbieter, Auftragsverarbeiter oder Partner, die Daten, Systeme oder regulatorische Verantwortlichkeiten der Organisation verarbeiten

2.1.4 aller Geschäftsprozesse, Projekte oder Initiativen, die rechtlichen oder regulatorischen Vorgaben unterliegen

2.2 Die von dieser Richtlinie erfassten Compliance-Bereiche umfassen unter anderem:

2.2.1 Anforderungen an Informationssicherheit und Cybersicherheit (z. B. ISO/IEC 27001, NIS2, DORA)

2.2.2 datenschutzrechtliche und privatsphärenbezogene Rechtsvorschriften (z. B. DSGVO, branchenspezifische Datenschutzgesetze)

2.2.3 sektorspezifische Regelwerke (z. B. Finanzwesen, Medizin, Automobilindustrie, Verteidigung)

2.2.4 vertragliche Verpflichtungen aus Geheimhaltungsvereinbarungen (NDAs), Service-Level-Agreements (SLAs) oder Vereinbarungen zur Verarbeitung durch Dritte

2.2.5 rechtliche Anforderungen im Zusammenhang mit Vorfallmeldungen, der Zusammenarbeit mit Strafverfolgungsbehörden und internationalen Datenübermittlungen

3. Ziele

3.1 Sicherzustellen, dass alle anwendbaren Gesetze, Vorschriften, Standards und vertraglichen Verpflichtungen organisationsweit identifiziert, dokumentiert, ausgelegt und umgesetzt werden.

3.2 Rechtliche und regulatorische Anforderungen in das Informationssicherheitsmanagementsystem (ISMS), die Risikomanagementprozesse, Lieferantenvereinbarungen sowie die Gestaltung von Produkten und Services zu integrieren.

3.3 Einen Mechanismus zur proaktiven Überwachung regulatorischer Änderungen und zur entsprechenden Aktualisierung von Kontrollen und Dokumentation bereitzustellen.

3.4 Klare Verantwortlichkeiten für die Überwachung der Compliance, die Eskalation von Verstößen, das Management von Ausnahmen und die externe Berichterstattung festzulegen.

3.5 Auditierbarkeit und belastbare Nachweisführung zur rechtlichen und regulatorischen Situation der Organisation bei Inspektionen, Untersuchungen oder Zertifizierungsaudits sicherzustellen.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung

4.1.1 Trägt die strategische Gesamtverantwortung für die rechtliche und regulatorische Ausrichtung im gesamten Unternehmen.

4.1.2 Prüft und genehmigt Compliance-Entscheidungen mit hohem Risiko, einschließlich Risikoakzeptanz und Rechtsstreitigkeiten.

4.2 Compliance-Beauftragter / General Counsel / Rechtsabteilung

4.2.1 Pflegt das Register der Compliance-Verpflichtungen, in dem alle anwendbaren Gesetze, Standards, Zertifizierungen und Vertragsklauseln aufgeführt sind.

4.2.2 Führt rechtliche Folgenabschätzungen für neue Services, Märkte oder Datenflüsse durch.

4.2.3 Gibt verbindliche Auslegungen von Gesetzen und Standards vor.

[... 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 Jährliche Richtlinienüberprüfung

9.1.1 Diese Richtlinie muss mindestens einmal pro Kalenderjahr überprüft werden, um:

9.1.1.1 die fortlaufende Ausrichtung an aktualisierten Gesetzen, Branchenstandards und regulatorischen Rahmenwerken sicherzustellen

9.1.1.2 die operative Wirksamkeit anhand von Auditfeststellungen und der Vorfallhistorie zu validieren

9.1.1.3 organisatorische Änderungen abzubilden (z. B. neue Rechtsordnungen, Systeme oder Geschäftsbereiche)

9.2 Anlassbezogene Überprüfungen

9.2.1 Zwischenprüfungen müssen eingeleitet werden, wenn:

9.2.2 eine neue rechtliche oder regulatorische Anforderung in Kraft tritt oder aktualisiert wird

9.2.3 ein Compliance-Vorfall oder ein Audit Mängel der Richtlinie aufdeckt

9.2.4 die Organisation einen neuen Markt oder eine neue Service-Linie erschließt, die einem eigenständigen Compliance-Rahmen unterliegt

9.2.5 Durchsetzungstrends oder Leitlinien von Aufsichtsbehörden auf Veränderungen im Risikoprofil hindeuten

9.3 Eigentümerschaft und Genehmigung

9.3.1 Die Rechtsabteilung und der Compliance-Beauftragte tragen gemeinsam die Verantwortung für die Koordination des Überprüfungsprozesses.

9.3.2 Endgültige Überarbeitungen dieser Richtlinie müssen durch die Geschäftsleitung genehmigt und mit zugehörigen Referenzen zur Änderungssteuerung sowie Kommunikationsplänen im Register für Richtlinienänderungen protokolliert werden.

9.4 Versionskontrolle und Kommunikation

9.4.1 Jede aktualisierte Version dieser Richtlinie muss:

9.4.1.1 eine Zusammenfassung der wesentlichen Änderungen enthalten

9.4.1.2 über offizielle Kanäle erneut verteilt werden (z. B. Richtlinienportal, LMS, interne Newsletter)

9.4.1.3 eine Bestätigung durch betroffene Mitarbeitende verlangen, insbesondere durch Personen in rechtlichen, operativen, sicherheitsbezogenen und lieferantenbezogenen Rollen

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie gilt in Verbindung mit den folgenden Richtlinien innerhalb des ISMS der Organisation und ergänzt diese:

10.1.1 P1 – Richtlinie zur Informationssicherheit: Legt die grundlegenden Governance-Prinzipien fest, die sicherstellen, dass alle Richtlinien zur Informationssicherheit – einschließlich Compliance – an strategischen Geschäfts- und Regulierungsanforderungen ausgerichtet sind.

10.1.2 P2 – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Definiert Entscheidungsbefugnisse, einschließlich der rechtlichen und compliancebezogenen Rollen für regulatorische Aufsicht und Rechenschaftspflicht.

10.1.3 P6 – Risikomanagement-Richtlinie: Unterstützt die Bewertung, Verantwortlichkeit und Minderung rechtlicher und regulatorischer Compliance-Risiken im gesamten Unternehmen.

10.1.4 P8 – Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit: Stellt sicher, dass sämtliches Personal über Compliance-Verantwortlichkeiten informiert ist und rollengerechte Schulungen erhält.

10.1.5 P12 – Richtlinie zum Asset-Management: Verstärkt rechtliche Verpflichtungen zur Verwaltung und zum Schutz regulierter oder vertraglich gebundener Assets, einschließlich solcher mit personenbezogenen Daten und kritischer Infrastruktur.

10.1.6 P30 – Incident-Response-Richtlinie: Regelt verpflichtende rechtliche Meldungen (z. B. DSGVO Artikel 33) und Eskalationsverfahren im Fall eines Compliance-Verstoßes oder regulatorischen Ereignisses.

10.1.7 P33 – Richtlinie zur Audit- und Compliance-Überwachung: Stellt strukturierte Sicherstellungsaktivitäten bereit – einschließlich Kontrolltests und der Sammlung von Nachweisen –, die für die interne und externe Verifizierung der Compliance erforderlich sind.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Abschnitt 4.2 – Verständnis der Erfordernisse und Erwartungen interessierter Parteien: Fordert die Identifizierung und Integration rechtlicher und regulatorischer Anforderungen in das ISMS.

11.1.2 Abschnitt 5.1 – Führung und Verpflichtung: Verlangt Rechenschaftspflicht der Führungsebene für die Einführung und Aufrechterhaltung rechtlicher Compliance in der gesamten Organisation.

11.1.3 Abschnitt 5.3 – Rollen, Verantwortlichkeiten und Befugnisse in der Organisation: Stellt klare Rollen für rechtliche Aufsicht und regulatorische Compliance sicher.

11.1.4 Anhang A Maßnahme 5.36 – Einhaltung rechtlicher und vertraglicher Anforderungen: Legt die Anforderung fest, Verpflichtungen aus Gesetzen, Vorschriften und Verträgen zu identifizieren und zu erfüllen.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 5.36: Beschreibt Umsetzungsleitlinien zur Pflege eines Registers der Compliance-Verpflichtungen, zur Validierung regulatorischer Anforderungen und zur Sicherstellung einer strukturierten Aufbewahrung von Nachweisen.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Richtlinie und Verfahren zur Sicherheitsplanung: Fordert, dass Compliance-Verpflichtungen in Governance-Strukturen und Dokumentation verankert werden.

11.3.2 PM-1 – Plan für das Informationssicherheitsprogramm: Verlangt regulatorische Kontrollen als Bestandteil des übergeordneten Sicherheitsprogramms.

11.3.3 CA-7 – Kontinuierliche Überwachung: Unterstützt die Überwachung der Kontrollwirksamkeit bei der Erfüllung rechtlicher und richtlinienbezogener Anforderungen.

11.3.4 AU-9 – Schutz von Audit-Informationen: Stellt sicher, dass Auditprotokolle und Compliance-Aufzeichnungen geschützt und für Prüfungen verfügbar sind.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 5 – Grundsätze für die Verarbeitung: Verlangt rechtmäßige Verarbeitung, Transparenz und Rechenschaftspflicht.

11.4.2 Artikel 6 – Rechtmäßigkeit der Verarbeitung: Verlangt geeignete Rechtsgrundlagen für alle Datenverarbeitungstätigkeiten.

11.4.3 Artikel 24 – Verantwortung des Verantwortlichen: Begründet die unmittelbare Rechenschaftspflicht zur Sicherstellung regulatorischer Compliance.

11.4.4 Artikel 32 – Sicherheit der Verarbeitung: Verlangt die Umsetzung geeigneter technischer und organisatorischer Maßnahmen.

11.4.5 Artikel 33 – Meldung von Verletzungen des Schutzes personenbezogener Daten: Verlangt, dass Datenschutzverletzungen innerhalb von 72 Stunden an die zuständigen Behörden gemeldet werden.

11.5 EU NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 20–21: Verlangen von wesentlichen und wichtigen Einrichtungen die Umsetzung dokumentierter Governance, rechtlicher Compliance-Strategien und einer fortlaufenden Überprüfung rechtlicher Risiken.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 5(2) – Rahmenwerk für das Management von IKT-Risiken: Verlangt die Integration rechtlicher Compliance in übergreifende Risikomanagement- und Überwachungsfunktionen.

11.6.2 Artikel 19 – IKT-Drittparteienrisiko: Begründet spezifische rechtliche Anforderungen für die Steuerung vertraglicher und regulatorischer Verpflichtungen im Zusammenhang mit externen Lieferanten und Plattformen.

11.7 COBIT 2019

11.7.1 APO12 – Risiken managen: Berücksichtigt rechtliche und regulatorische Compliance als kritische Bestandteile der unternehmensweiten Risiko-Governance.

11.7.2 MEA03 – Überwachung der Einhaltung externer Anforderungen: Definiert die fortlaufende Überwachung, das Ausnahmenmanagement und die Auditbereitschaft für alle Formen regulatorischer Verpflichtungen.