					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P29S					Dokumenttitel: **Richtlinie für Testdaten und Testumgebungen**							
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/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 6.1, 8	
ISO/IEC 27002:2022	Maßnahmen 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
EU-DSGVO	Artikel 5(1)(c), 25, 32	
EU-NIS2	Artikel 21(2)(e), (h)	
EU-DORA	Artikel 9	
COBIT 2019	BAI07, DSS	

1. Zweck

1.1 Diese Richtlinie legt fest, wie Testdaten und Testumgebungen zu verwalten sind, um unbeabsichtigte Offenlegungen, Datenschutzverletzungen oder Betriebsstörungen während von Testaktivitäten zu verhindern.

1.2 Sie stellt sicher, dass echte Kundendaten bei Software- oder Systemtests niemals unzulässig verwendet werden und dass Testumgebungen logisch und technisch von Produktivsystemen getrennt sind.

1.3 Diese Richtlinie dient dazu, KMU bei der Erfüllung der Anforderungen für eine ISO/IEC-27001-Zertifizierung sowie einschlägiger Datenschutzgesetze zu unterstützen und dabei für Organisationen ohne dediziertes IT-Team praktikabel und durchsetzbar zu bleiben.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle Testumgebungen (z. B. Staging-Server, Sandbox-Systeme, Entwicklungs-Testumgebungen)

2.1.2 alle Testdaten, unabhängig davon, ob sie manuell erstellt, generiert oder aus Produktivdaten abgeleitet wurden

2.1.3 sämtliches Personal, das an Testaktivitäten beteiligt ist, einschließlich Mitarbeitender, Auftragnehmer, Freelancer und IT-Dienstleister

2.1.4 sämtliche Tests, die Auswirkungen auf kundenbezogene Plattformen, interne Geschäftssysteme oder Dienste Dritter haben können

2.2 Sie umfasst sowohl technische Umgebungen als auch Prozesse zur Unterstützung von:

2.2.1 der Entwicklung von Websites, Anwendungen und Werkzeugen

2.2.2 Systemaktualisierungen, Konfigurationstests und Integrationstests

2.2.3 automatisierten und manuellen funktionalen Tests sowie Sicherheitstests

3. Ziele

3.1 Verhinderung der Nutzung echter, identifizierbarer Kundendaten in Tests, sofern diese nicht anonymisiert und ausdrücklich genehmigt wurden.

3.2 Aufrechterhaltung einer strikten Trennung zwischen Test- und Produktivsystemen, um unbeabsichtigte Datenoffenlegungen oder Beeinträchtigungen des Betriebs zu vermeiden.

3.3 Schutz von Testsystemen und Testdaten vor unbefugtem Zugriff, versehentlicher Offenlegung oder Wiederverwendung über Umgebungen hinweg ohne geeignete Kontrollen.

3.4 Einhaltung relevanter Datenschutzvorschriften (z. B. DSGVO, NIS2), indem sichergestellt wird, dass alle Testdaten rechtmäßig, nach Treu und Glauben und sicher verarbeitet werden.

3.5 Unterstützung der Auditbereitschaft der Organisation für externe Audits und die ISO/IEC-27001-Zertifizierung durch dokumentierte Testpraktiken und die Durchsetzung konsistenter Schutzmaßnahmen.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführer (GM)

4.1.1 Trägt die Gesamtverantwortung für den Schutz von Testdaten und die Sicherheit von Testsystemen.

4.1.2 Genehmigt jede Nutzung echter Daten in Tests, nachdem geeignete Schutzmaßnahmen (z. B. Anonymisierung oder Maskierung) bestätigt wurden.

4.1.3 Verifiziert, dass Testaktivitäten ordnungsgemäß dokumentiert sind und dieser Richtlinie entsprechen.

4.2 Projektverantwortlicher

4.2.1 Koordiniert die Gestaltung und Durchführung der Testprozesse.

4.2.2 Stellt sicher, dass alle Teammitglieder diese Richtlinie verstehen und einhalten.

4.2.3 Bestätigt, dass Testsysteme sicher konfiguriert sind, bevor Tests beginnen.

4.2.4 Meldet alle Vorfälle im Zusammenhang mit Testumgebungen oder Datenabfluss an den GM.

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

9. Überprüfungs- und Aktualisierungsanforderungen

9.1 Planmäßige Überprüfungen

9.1.1 Diese Richtlinie ist mindestens einmal jährlich durch den Geschäftsführer (GM) zu überprüfen. Die Überprüfung stellt sicher, dass die Richtlinie aktuell bleibt in Bezug auf:

9.1.1.1 Änderungen bei Werkzeugen, Plattformen oder Umgebungen für die Softwareentwicklung

9.1.1.2 aktualisierte rechtliche Verpflichtungen, einschließlich Anforderungen an Datenschutz oder digitale Resilienz

9.1.1.3 die Zertifizierungsfähigkeit von KMU und die Auditbereitschaft nach ISO/IEC 27001

9.2 Auslösende Ereignisse für außerplanmäßige Überprüfungen

9.2.1 Zusätzliche Überprüfungen müssen erfolgen nach:

9.2.1.1 jedem Vorfall mit Datenoffenlegung oder Kompromittierung in Testumgebungen

9.2.1.2 jeder Nutzung echter Daten in Tests, auch wenn diese anonymisiert wurden

9.2.1.3 der Einführung neuer Testmethoden, Systeme oder Lieferanten

9.2.1.4 regulatorischen Änderungen, die die Datenverarbeitung während von Tests betreffen

9.3 Änderungsmanagement und Kommunikation

9.3.1 Der GM ist verantwortlich für:

9.3.1.1 die Aktualisierung dieser Richtlinie und die Dokumentation aller Änderungen in der Versionshistorie

9.3.1.2 die Benachrichtigung von Mitarbeitenden, Entwicklern und relevanten Dienstleistern über Aktualisierungen

9.3.1.3 die Bestätigung, dass sämtliches testbezogenes Personal die aktuellen Vorgaben versteht und anwendet

9.3.1.4 die Pflege einer zugänglichen Fassung der aktuellen Richtlinie für Prüfungs- und Audit-Zwecke

9.4 Audit und Dokumentation

9.4.1 Aufzeichnungen über alle Richtlinienüberprüfungen, Genehmigungen für die Nutzung echter Daten und Begründungen für Ausnahmen müssen:

9.4.1.1 sicher für Audit-Zwecke aufbewahrt werden

9.4.1.2 auf Anfrage bei internen Audits oder Audits durch Dritte verfügbar sein

9.4.1.3 jährlich überprüft werden, um die Übereinstimmung mit den Testpraktiken sicherzustellen

10. Verwandte Richtlinien und Verknüpfungen

10.1 Diese Richtlinie ist in Abstimmung mit den folgenden SME-Richtlinien anzuwenden, um Sicherheit und Einhaltung während von Testaktivitäten sicherzustellen:

10.1.1 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Definiert, wer für die Aufsicht über Entwicklung, Tests und Verantwortlichkeiten zur Systemtrennung rechenschaftspflichtig ist.

10.1.2 P4S – Richtlinie zur Zugriffskontrolle: Regelt die Zuweisung, Verwaltung und Entfernung von Zugangsdaten für Testsysteme.

10.1.3 P8S – Richtlinie zur Sensibilisierung und Schulung zur Informationssicherheit: Stellt sicher, dass Mitarbeitende die Risiken von Testdaten, sichere Handhabungspraktiken und die ordnungsgemäße Trennung von Umgebungen verstehen.

10.1.4 P13S – Richtlinie zur Datenklassifizierung und Kennzeichnung: Unterstützt die eindeutige Klassifizierung von Testdaten und gibt Vorgaben für Anonymisierungs- oder Maskierungsstrategien.

10.1.5 P17S – Richtlinie zu Datenschutz und Privatsphäre: Steht im Einklang mit den Verpflichtungen aus der DSGVO, einschließlich Schutzmaßnahmen für die Verarbeitung und Speicherung personenbezogener Daten, auch in Testumgebungen.

10.1.6 P24S – Richtlinie zur sicheren Softwareentwicklung: Legt die allgemeinen Sicherheitserwartungen für Entwicklungsteams fest, einschließlich der sicheren Verwendung von Daten während von Testphasen.

10.1.7 P30S – Richtlinie zur Reaktion auf Informationssicherheitsvorfälle: Legt dar, wie auf Verletzungen oder Probleme zu reagieren ist, die in einer Testumgebung festgestellt werden oder durch unsachgemäße Handhabung von Testdaten verursacht werden.

10.2 Diese Richtlinien bilden ein einheitliches Sicherheitsrahmenwerk zur Unterstützung der Integrität von Tests, der Datenminimierung und der vollständigen Ausrichtung an ISO/IEC 27001 über Entwicklungs- und Qualitätssicherungsaktivitäten hinweg.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 6.1 – Erfordert Risikoanalyse und Maßnahmen zur Risikobehandlung, einschließlich testbezogener Risiken.

11.1.2 Klausel 8.1 – Verlangt die Planung und Steuerung operativer Prozesse, einschließlich des Aufbaus von Testsystemumgebungen.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 8.28 – Erfordert, dass Organisationen Testdaten schützen und sicherstellen, dass diese keine sensiblen oder produktiven Echtzeitdaten enthalten.

11.2.2 Maßnahme 8.29 – Verlangt eine klare Trennung von Entwicklungs-, Test- und Produktivumgebungen.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – Umfasst Kontrollanforderungen für Entwicklung und Tests.

11.3.2 SA-12 – Behandelt Risiken bei Tests in der Lieferkette und Sicherheitsbewertungen.

11.3.3 SC-32 – Erfordert die Trennung von Umgebungen und Schutzmaßnahmen für die Vertraulichkeit und Integrität von Testdaten.

11.4 Datenschutz-Grundverordnung der EU (DSGVO)

11.4.1 Artikel 5(1)(c) – Verlangt Datenminimierung, einschließlich der Verwendung nur solcher Daten, die für Tests erforderlich sind.

11.4.2 Artikel 25 – Verlangt Datenschutz durch Technikgestaltung, was auch Kontrollen für Testumgebungen einschließt.

11.4.3 Artikel 32 – Verlangt eine sichere Verarbeitung personenbezogener Daten in allen Systemen, einschließlich Nicht-Produktivumgebungen.

11.5 EU-NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(e), (h) – Verlangt sichere Entwicklung und sichere Systemtests, insbesondere dort, wo digitale Dienste Cyberrisiken ausgesetzt sind.

11.6 EU-DORA (2022/2554)

11.6.1 Artikel 9 – Betont die Bedeutung digitaler operationeller Resilienz, einschließlich sicherer Tests von IKT-Systemen durch KMU im Finanzsektor.

11.7 COBIT 2019

11.7.1 BAI07 – Manage Change Acceptance and Transitioning: Umfasst Testkontrollen zur Validierung neuer Systeme und der Datenverarbeitung.

11.7.2 DSS05 – Sicherheitsdienste verwalten: Verlangt Test- und Entwicklungspraktiken, die Missbrauch oder Offenlegung geschäftlicher Daten verhindern.