# Technische und organisatorische Maßnahmen

## Präambel

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOMs) der inducio GmbH zur Erfüllung der Anforderungen aus Artikel 32 DSGVO.

## Überprüfung und Aktualisierung

Die hier dokumentierten Maßnahmen werden regelmäßig, mindestens jedoch einmal jährlich, sowie anlassbezogen bei wesentlichen Änderungen der Verarbeitungstätigkeiten, der eingesetzten Technologien, der Bedrohungslage oder der rechtlichen Anforderungen überprüft und fortgeschrieben.

## Abschnitt 5: Organisatorische Maßnahmen

### TOM 5.1 - Informationssicherheitspolitik und -richtlinien

Eine durch die Geschäftsführung der inducio GmbH verabschiedete Informationssicherheits-Leitlinie sowie themenbezogene Richtlinien (u. a. Zugangs-, Verschlüsselungs-, Datensicherungs-, Lieferanten-Richtlinie) sind dokumentiert, kommuniziert und werden mindestens jährlich sowie bei wesentlichen Änderungen überprüft.

### TOM 5.2 - Informationssicherheitsrollen und -verantwortlichkeiten

Rollen und Verantwortlichkeiten für die Informationssicherheit (u. a. Informationssicherheitsbeauftragte/r, Asset- und Risk-Owner) sowie für den Datenschutz (Siehe Informationen unserer Webseite) sind definiert, dokumentiert und den jeweiligen Personen formell zugewiesen.

### TOM 5.3 - Aufgabentrennung

Kollidierende Aufgaben und Verantwortungsbereiche werden funktional getrennt (z. B. Entwicklung vs. Betrieb, Beantragung vs. Genehmigung von Zugangsrechten, Buchung vs. Freigabe), um das Risiko unautorisierter oder missbräuchlicher Handlungen zu reduzieren.

### TOM 5.4 - Verantwortlichkeiten der Leitung

Die Geschäftsführung der inducio GmbH verpflichtet alle Mitarbeitenden und Auftragnehmer, die Informationssicherheit gemäß den festgelegten Richtlinien und Verfahren anzuwenden, und stellt die hierfür erforderlichen Ressourcen bereit.

### TOM 5.5 - Kontakt mit Behörden

Geeignete Kontakte zu relevanten Behörden sind etabliert. Zuständige Aufsichtsbehörde ist das Bayerisches Landesamt für Datenschutzaufsicht (BayLDA). Im Bedarfsfall (insb. bei Sicherheitsvorfällen und Datenschutzverletzungen) erfolgt zeitnahe Kontaktaufnahme.

### TOM 5.6 - Kontakt mit speziellen Interessengruppen

Die inducio GmbH unterhält Kontakte zu Sicherheits-Foren und Berufsverbänden, um über aktuelle Bedrohungen, Best Practices und Schwachstellen informiert zu bleiben.

TOM 5.7 - Informationen über die Bedrohungslage

Informationen zu aktuellen Bedrohungen werden aus internen und externen Quellen (Hersteller-Advisories, CERT-Bund, BSI-Lagebericht, einschlägige Fachpresse) systematisch ausgewertet und fließen in Risiko- und Schutzentscheidungen ein.

TOM 5.8 - Informationssicherheit im Projektmanagement

Informationssicherheit ist fester Bestandteil des Projektmanagements aller Projekttypen. Sicherheits- und Datenschutzanforderungen werden in jeder Projektphase identifiziert, bewertet und behandelt.

TOM 5.9 - Inventar der Informationen und anderer damit verbundener Werte

Ein Inventar der Informationen und damit verbundener Werte (Hardware, Software, Daten, Cloud-Dienste, Lizenzen) wird geführt, regelmäßig überprüft und enthält den jeweiligen Eigentümer (Asset-Owner).

TOM 5.10 - Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten

Regeln für die zulässige Nutzung sind festgelegt und kommuniziert. Die Nutzung privat beschaffter IT-Systeme zur Verarbeitung von personenbezogenen Daten ist untersagt.

TOM 5.11 - Rückgabe von Werten

Mitarbeitende und externe Nutzer geben alle überlassenen Werte (Hardware, Datenträger, Dokumente, Zugangstoken) bei Beendigung des Beschäftigungsverhältnisses oder Auftrags nachvollziehbar zurück.

TOM 5.12 - Klassifizierung von Informationen

Informationen werden nach gesetzlichen Anforderungen, Wert, Kritikalität und Schutzbedarf klassifiziert (z. B. öffentlich, intern, vertraulich, streng vertraulich). Personenbezogene Daten gelten mindestens als „vertraulich“.

TOM 5.13 - Kennzeichnung von Informationen

Verfahren zur Kennzeichnung von Informationen gemäß Klassifizierungsschema sind etabliert (z. B. Kopf-/Fußzeilen, Metadaten, Hinweise in E-Mail-Signaturen).

TOM 5.14 - Informationsübermittlung

Für jede Übermittlungsart (elektronisch, physisch, mündlich) bestehen Regeln. Personenbezogene Daten werden ausschließlich verschlüsselt bzw. über gesicherte Kanäle übermittelt.

TOM 5.15 - Zugangssteuerung

Regeln zur Steuerung des physischen und logischen Zugangs werden nach den Grundsätzen „need-to-know“ und „least privilege“ festgelegt und umgesetzt.

TOM 5.16 - Identitätsmanagement

Der gesamte Lebenszyklus von Identitäten (Eröffnung, Änderung, Sperrung, Löschung) wird zentral gesteuert. Gemeinsam genutzte Konten sind nur mit ausdrücklicher Genehmigung und nachvollziehbarer Zuordnung zulässig.

TOM 5.17 - Authentisierungsinformationen

Die Zuteilung und Verwaltung von Authentisierungsinformationen (Passwörter, Token, Schlüssel) erfolgen über kontrollierte Prozesse. Passwortqualität und -wechselregeln sind definiert. Geheime Informationen werden niemals im Klartext gespeichert oder übermittelt.

TOM 5.18 - Zugangsrechte

Zugangsrechte werden formal beantragt, genehmigt, dokumentiert, mindestens jährlich geprüft und bei Personalwechsel oder Aufgabenwechsel zeitnah angepasst oder entzogen.

TOM 5.19 - Informationssicherheit in Lieferantenbeziehungen

Verfahren zur Behandlung von Risiken aus Lieferantenbeziehungen sind definiert. Lieferanten und Dienstleister werden vor Beauftragung einer angemessenen Sicherheitsprüfung unterzogen.

TOM 5.20 - Behandlung von Informationssicherheit in Lieferantenvereinbarungen

Mit jedem Lieferanten werden risikoangemessene Sicherheitsanforderungen vertraglich vereinbart (insb. Auftragsverarbeitungsvertrag nach Art. 28 DSGVO, TOMs, Audit- und Meldepflichten).

TOM 5.21 - Umgang mit der Informationssicherheit in der IKT-Lieferkette

Risiken aus der IKT-Lieferkette (Unter-Auftragsverarbeiter, Software-Zulieferer, Cloud-Anbieter) werden bewertet und behandelt. Die aktuelle Liste der eingesetzten Unter-Auftragsverarbeiter ist veröffentlicht unter https://inducio-services.net/datenschutz/unterauftragsnehmer.

TOM 5.22 - Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen

Erbringung, Sicherheitsvorfälle und SLA-Einhaltung der Lieferanten werden regelmäßig ausgewertet. Änderungen am Leistungsumfang werden bewertet und nachgeführt.

TOM 5.23 - Informationssicherheit für die Nutzung von Cloud-Diensten

Vor der Nutzung eines Cloud-Dienstes wird eine Risikobewertung durchgeführt (u. a. Datenstandort, Verschlüsselung, Kontroll- und Audit-Möglichkeiten, Exit-Strategie). Ausstieg und Datenrückgabe sind in den Cloud-Verträgen geregelt.

TOM 5.24 - Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen

Prozesse, Rollen und Verantwortlichkeiten für die Vorfallbehandlung sind festgelegt, kommuniziert und werden regelmäßig geübt.

TOM 5.25 - Beurteilung und Entscheidung über Informationssicherheitsereignisse

Sicherheitsereignisse werden nach dokumentierten Kriterien (Schwere, Auswirkung, Eintrittswahrscheinlichkeit) bewertet und ggf. als Vorfall eingestuft.

TOM 5.26 - Reaktion auf Informationssicherheitsvorfälle

Auf Vorfälle wird gemäß dokumentierten Verfahren reagiert. Bei Datenschutzverletzungen erfolgen die Meldung an das Bayerisches Landesamt für Datenschutzaufsicht (BayLDA) innerhalb 72h (Art. 33 DSGVO) sowie die unverzügliche Information des Verantwortlichen.

TOM 5.27 - Erkenntnisse aus Informationssicherheitsvorfällen

Aus jeder Vorfallbehandlung werden Lessons-Learned dokumentiert und in Prozesse, Schulungen und technische Maßnahmen eingearbeitet.

TOM 5.28 - Sammeln von Beweismaterial

Verfahren zur forensisch verwertbaren Identifizierung, Sicherung und Erhaltung von Beweismaterial in Zusammenhang mit Sicherheitsereignissen sind etabliert.

TOM 5.29 - Informationssicherheit bei Störungen

Während Störungen wird die Informationssicherheit auf angemessenem Niveau aufrechterhalten (z. B. Notbetriebs- und Eingriffsverfahren mit definierten Sicherheitsleitplanken).

TOM 5.30 - IKT-Bereitschaft für Business-Continuity

Die IKT-Bereitschaft (Redundanzen, Notfall-, Wiederanlaufkonzepte) ist auf die definierten Geschäftskontinuitätsziele ausgerichtet und wird regelmäßig getestet.

TOM 5.31 - Juristische, gesetzliche, regulatorische und vertragliche Anforderungen

Relevante rechtliche und vertragliche Anforderungen (insb. DSGVO, BDSG, Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz, ggf. branchenspezifische Vorgaben) sind identifiziert, dokumentiert und werden aktuell gehalten.

TOM 5.32 - Geistige Eigentumsrechte

Verfahren zum Schutz geistiger Eigentumsrechte (eigene wie fremde) sind etabliert: Lizenzmanagement, ausschließliche Verwendung lizenzkonformer Software, Beachtung der Urheberrechte Dritter.

TOM 5.33 - Schutz von Aufzeichnungen

Aufzeichnungen werden vor Verlust, Zerstörung, Fälschung und unbefugtem Zugriff geschützt. Gesetzliche und vertragliche Aufbewahrungs- und Löschfristen werden eingehalten.

TOM 5.34 - Datenschutz und Schutz personenbezogener Daten

Die Anforderungen an den Datenschutz nach DSGVO und BDSG werden umgesetzt. Eine externe Datenschutzbeauftragte ist bestellt: RAin Irmengard Gromotka (datenschutz@inducio.de).

TOM 5.35 - Unabhängige Überprüfung der Informationssicherheit

Das Informationssicherheits-Konzept und dessen Umsetzung werden in geplanten Abständen sowie bei wesentlichen Änderungen unabhängig überprüft (interne Audits, ggf. externe Begutachtung).

TOM 5.36 - Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit

Die Einhaltung der Informationssicherheits-Richtlinie und themenbezogener Richtlinien wird regelmäßig durch Stichproben und Audits überprüft.

TOM 5.37 - Dokumentierte Betriebsabläufe

Betriebsabläufe für informationsverarbeitende Einrichtungen (z. B. Change-, Patch-, Backup-, Restore-Verfahren) sind dokumentiert und dem zuständigen Personal zugänglich.

## Abschnitt 6: Personelle Maßnahmen

### TOM 6.1 - Sicherheitsüberprüfung

Vor Beschäftigungsbeginn werden Bewerber angemessen überprüft (Vorlage Führungszeugnis bei sicherheitsrelevanten Funktionen, Identitätsprüfung, Referenzen) - unter Beachtung der gesetzlichen Vorgaben.

### TOM 6.2 - Beschäftigungs- und Vertragsbedingungen

Die Arbeits- und Werkverträge regeln die Verantwortlichkeiten für Informationssicherheit und Datenschutz.

### TOM 6.3 - Informationssicherheitsbewusstsein, -ausbildung und -schulung

Mitarbeitende der inducio GmbH werden mindestens jährlich zu Informationssicherheit und Datenschutz geschult und bei sicherheitsrelevanten Ereignissen erfolgen anlassbezogene Sensibilisierungen.

### TOM 6.4 - Maßregelungsprozess

Bei Verstößen gegen die Informationssicherheits-Richtlinien ist ein formaler Maßregelungsprozess vorgesehen und arbeitsrechtliche Konsequenzen können bis zur Kündigung reichen.

### TOM 6.5 - Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung

Bei Beendigung oder Wechsel der Beschäftigung werden Zugänge gesperrt, Assets zurückgegeben und der oder die Betroffene auf weiterhin geltende Geheimhaltungspflichten hingewiesen.

### TOM 6.6 - Vertraulichkeits- oder Geheimhaltungsvereinbarungen

Mit allen Mitarbeitenden, externen Beschäftigten und relevanten Vertragspartnern werden Vertraulichkeits- oder Geheimhaltungsvereinbarungen geschlossen und regelmäßig überprüft.

### TOM 6.7 - Remote-Arbeit

Beim Remote-Arbeiten sind technische und organisatorische Schutzmaßnahmen umgesetzt: VPN-Zugang, Multi-Faktor-Authentifizierung, Endpunkt-Verschlüsselung, Sichtschutz.

TOM 6.8 - Meldung von Informationssicherheitsereignissen

Mitarbeitende werden verpflichtet und befähigt, Sicherheitsereignisse oder -verdachtsmomente unverzüglich über etablierte interne Kanäle zu melden.

## Abschnitt 7: Physische Maßnahmen

### TOM 7.1 - Physische Sicherheitsperimeter

Die Räumlichkeiten der inducio GmbH (Standort Traunstein) sind durch definierte Sicherheitsperimeter geschützt (Gebäudeeingänge, separierte Server- und Archivbereiche).

### TOM 7.2 - Physischer Zutritt

Der Zutritt erfolgt personenbezogen und protokolliert. Zutrittsrechte sind dokumentiert und werden regelmäßig überprüft. Besucher werden empfangen und begleitet.

### TOM 7.3 - Sichern von Büros, Räumen und Einrichtungen

Büros, Räume und Einrichtungen werden physisch gesichert. Sensible Bereiche unterliegen zusätzlichen Schutzmaßnahmen.

### TOM 7.4 - Physische Sicherheitsüberwachung

Sensible Bereiche werden auf unautorisierten Zutritt überwacht (Alarmanlage, Videoüberwachung im rechtlich zulässigen Rahmen, Sicherheitspersonal).

### TOM 7.5 - Schutz vor physischen und umweltbedingten Bedrohungen

Schutz vor physischen und umweltbedingten Risiken (Brand, Wasser, Stromausfall, Klima) ist umgesetzt: Brandmelder, Feuerlöscher, USV für kritische Systeme, kontrollierte Raumtemperatur.

### TOM 7.6 - Arbeiten in Sicherheitsbereichen

Für Tätigkeiten in besonders geschützten Bereichen gelten zusätzliche Regeln (z. B. Foto- und Aufnahmeverbote, Begleitung externer Personen, Clear-Desk-Pflicht).

### TOM 7.7 - Aufgeräumte Arbeitsumgebung und Bildschirmsperren

Clear-Desk-Regeln (keine sensiblen Papiere/Datenträger frei liegend) und Clear-Screen-Regeln (automatische Bildschirmsperre bei Inaktivität, manuelle Sperrung beim Verlassen) sind festgelegt und werden durchgesetzt.

TOM 7.8 - Platzierung und Schutz von Geräten und Betriebsmitteln

Geräte und Betriebsmittel werden so platziert und geschützt, dass das Risiko unautorisierter Einsicht, Manipulation oder Beschädigung minimiert wird.

TOM 7.9 - Sicherheit von Werten außerhalb der Räumlichkeiten

Mobile Werte (Notebooks, Smartphones, Wechseldatenträger) sind durch Geräteverschlüsselung und Verhaltensregeln (Aufsichtspflicht, sichere Aufbewahrung) geschützt.

TOM 7.10 - Speichermedien

Speichermedien werden über ihren Lebenszyklus klassifiziert verwaltet. Datenträger mit sensiblen Inhalten werden sicher gelöscht oder physisch vernichtet.

TOM 7.11 - Versorgungseinrichtungen

Informationsverarbeitende Einrichtungen sind gegen Versorgungsausfälle abgesichert (USV für kritische Systeme und redundante Internet-Anbindung).

TOM 7.12 - Sicherheit der Verkabelung

Strom- und Datenverkabelung ist gegen Abhören, Störung und Beschädigung geschützt (Verkabelung in geschützten Trassen, Schutz aktiver Komponenten in Verteilerschränken).

TOM 7.13 - Instandhaltung von Geräten und Betriebsmitteln

Geräte werden gemäß Herstellervorgaben gewartet. Wartungs- und Reparaturvorgänge durch Externe werden begleitet und dokumentiert.

TOM 7.14 - Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

Vor Entsorgung oder Wiederverwendung von Geräten mit Speichermedien werden Daten nachweislich sicher entfernt oder die Datenträger physisch vernichtet.

## Abschnitt 8: Technologische Maßnahmen

### TOM 8.1 - Endpunktgeräte des Benutzers

Endpunktgeräte (Notebooks, Desktops, Mobilgeräte) sind durch Endpoint-Protection, Geräteverschlüsselung, aktuelle Patches und ggf. Mobile-Device-Management abgesichert.

### TOM 8.2 - Privilegierte Zugangsrechte

Privilegierte Zugangsrechte (z. B. Admin-Konten) sind separat von Standardkonten, namentlich zugeordnet, durch Multi-Faktor-Authentifizierung geschützt und protokolliert.

### TOM 8.3 - Informationszugangsbeschränkung

Der Zugang zu Anwendungen und Daten ist durch granulare Berechtigungen auf den notwendigen Umfang beschränkt. Berechtigungen werden bedarfsgerecht und überprüfbar vergeben.

### TOM 8.4 - Zugriff auf den Quellcode

Lese- und Schreibzugriff auf Quellcode, Build- und Entwicklungswerkzeuge erfolgen über eine Versionskontrolle mit Code-Review. Signierte oder verifizierbare Commits werden bei sicherheitsrelevanten Repositories verlangt.

### TOM 8.5 - Sichere Authentisierung

Sichere Authentisierungsverfahren werden eingesetzt. Für administrative Zugänge sowie alle aus dem Internet erreichbaren Konten ist Multi-Faktor-Authentifizierung verpflichtend.

### TOM 8.6 - Kapazitätssteuerung

Ressourcennutzung (Speicher, Rechenleistung, Bandbreite) wird überwacht. Kapazitäten werden den erwarteten Anforderungen angepasst und Engpässe rechtzeitig adressiert.

### TOM 8.7 - Schutz gegen Schadsoftware

Ein mehrstufiger Schutz gegen Schadsoftware ist umgesetzt (Endpoint-Schutz, E-Mail- und Web-Filterung, Software-Einschränkungen) und durch regelmäßige Sensibilisierung der Nutzer flankiert.

TOM 8.8 - Handhabung von technischen Schwachstellen

Informationen zu technischen Schwachstellen werden eingeholt, bewertet und durch Patches, Konfigurationsänderungen oder kompensierende Maßnahmen behandelt.

TOM 8.9 - Konfigurationsmanagement

Konfigurationen von Hardware, Software, Diensten und Netzwerken sind dokumentiert. Sicherheitsrelevante Härtungs-Baselines werden definiert, umgesetzt und überwacht.

TOM 8.10 - Löschung von Informationen

Informationen werden gelöscht, sobald sie nicht mehr benötigt werden oder gesetzliche bzw. vertragliche Aufbewahrungsfristen abgelaufen sind. Ein Löschkonzept ist etabliert.

TOM 8.11 - Datenmaskierung

Datenmaskierungsverfahren (Pseudonymisierung, Anonymisierung) werden eingesetzt, wo Test-, Analyse- oder Schulungszwecke keine echten personenbezogenen Daten erfordern.

TOM 8.12 - Verhinderung von Datenlecks

Maßnahmen zur Verhinderung von Datenlecks werden auf relevante Systeme angewendet (z. B. Einschränkung externer Datenträger, Ausgangsfilterung, Berechtigungen auf Cloud-Sync-Tools).

TOM 8.13 - Sicherung von Informationen

Sicherungskopien werden nach einer dokumentierten Datensicherungsstrategie regelmäßig erstellt, vor Manipulation geschützt und durch periodische Wiederherstellungstests verifiziert.

TOM 8.14 - Redundanz von informationsverarbeitenden Einrichtungen

Kritische informationsverarbeitende Einrichtungen sind redundant ausgelegt, soweit dies den Verfügbarkeitsanforderungen entspricht.

TOM 8.15 - Protokollierung

Sicherheitsrelevante Ereignisse werden protokolliert, manipulationsgeschützt gespeichert und zur Auswertung bereitgestellt. Datenschutzanforderungen werden eingehalten.

TOM 8.16 - Überwachung von Aktivitäten

Netzwerke, Systeme und Anwendungen werden auf anomales Verhalten überwacht (z. B. Anomalie-Erkennung, Alarmierung bei verdächtigen Aktivitäten).

TOM 8.17 - Uhrensynchronisation

Die Systemuhren aller relevanten Systeme werden mit einer vertrauenswürdigen Zeitquelle (NTP) synchronisiert, um Protokolldaten korrelierbar zu halten.

TOM 8.18 - Gebrauch von Hilfsprogrammen mit privilegierten Rechten

Hilfsprogramme, die Sicherheitsmechanismen umgehen könnten, sind nur einem eng begrenzten Personenkreis zugänglich und ihre Nutzung wird protokolliert.

TOM 8.19 - Installation von Software auf Systemen in Betrieb

Software wird ausschließlich aus vertrauenswürdigen Quellen und im Rahmen eines kontrollierten Prozesses installiert. Standardnutzer dürfen keine Software ohne Freigabe installieren.

TOM 8.20 - Netzwerksicherheit

Netzwerke und Netzwerkgeräte werden gesichert, verwaltet und überwacht (Firewalls, gehärtete Konfigurationen, ausschließlich autorisierte Protokolle).

TOM 8.21 - Sicherheit von Netzwerkdiensten

Sicherheitsmechanismen, Service-Levels und Verwaltungsanforderungen aller Netzwerkdienste sind identifiziert, umgesetzt und werden überwacht.

TOM 8.22 - Trennung von Netzwerken

Netzwerke sind nach Schutzbedarf und Nutzergruppen segmentiert (z. B. Produktiv-, Verwaltungs-, Gäste-, DMZ-Bereiche).

TOM 8.23 - Webfilterung

Der Zugriff auf externe Webinhalte wird gesteuert (Web-Proxy / URL-Filtering), um die Belastung durch bekannte schadhafte oder unzulässige Inhalte zu reduzieren.

TOM 8.24 - Verwendung von Kryptographie

Für Verschlüsselung und Schlüsselverwaltung gelten verbindliche Regeln.

TOM 8.25 - Lebenszyklus einer sicheren Entwicklung

Für die Entwicklung von Software und Systemen gelten Regeln einer sicheren Entwicklung (Secure-SDLC, Bedrohungsmodellierung, Sicherheit als Design-Grundsatz).

TOM 8.26 - Anforderungen an die Anwendungssicherheit

Bei der Entwicklung und Beschaffung von Anwendungen werden Informationssicherheitsanforderungen im jeweiligen GitLab-Projekt bzw. Beschaffungsvorgang erfasst. Identifikation und Spezifikation erfolgen durch den verantwortlichen Bearbeiter, die Freigabe durch den IT-Verantwortlichen über die in GitLab integrierten Review- und Approval-Mechanismen (Issues, Merge Requests). Eine darüber hinausgehende separate Dokumentation wird nicht geführt. Die Nachvollziehbarkeit ergibt sich aus der Historie der Entwicklungs- und Beschaffungssysteme.

TOM 8.27 - Sichere Systemarchitektur und Entwicklungsgrundsätze

Architektur- und Entwicklungsgrundsätze (z. B. Least Privilege und sichere Default-Konfigurationen) sind dokumentiert und werden konsequent angewendet.

TOM 8.28 - Sichere Codierung

Grundsätze sicherer Codierung werden umgesetzt (Vermeidung verbreiteter Schwachstellenklassen, Code-Reviews, statische und dynamische Code-Analyse).

TOM 8.29 - Sicherheitsprüfung bei Entwicklung und Abnahme

Sicherheitsprüfungen sind fester Bestandteil des Entwicklungsprozesses. Vor der Produktivnahme sicherheitskritischer Anwendungen erfolgen geeignete Tests (z. B. Penetrationstests).

TOM 8.30 - Ausgegliederte Entwicklung

Ausgelagerte Entwicklungstätigkeiten werden überwacht und überprüft. Sicherheitsanforderungen, Code-Übergaben und Abnahmen sind vertraglich geregelt.

TOM 8.31 - Trennung von Entwicklungs-, Test- und Produktionsumgebungen

Entwicklungs-, Test- und Produktionsumgebungen sind getrennt. Echte personenbezogene Daten werden in Test- und Entwicklungsumgebungen grundsätzlich nicht verwendet.

TOM 8.32 - Änderungssteuerung

Änderungen an informationsverarbeitenden Einrichtungen und Anwendungen folgen einem dokumentierten Change-Prozess (Antrag, Bewertung, Genehmigung, Test, Freigabe, Rückfallplan).

TOM 8.33 - Testdaten

Testdaten werden bewusst ausgewählt, geschützt und verwaltet. Personenbezogene Echtdaten in Testumgebungen sind nur pseudonymisiert bzw. anonymisiert zulässig.

TOM 8.34 - Schutz der Informationssysteme während Tests im Rahmen von Audits

Audits und Sicherheitsprüfungen produktiver Systeme werden geplant und mit der zuständigen Leitung abgestimmt, um Beeinträchtigungen des Betriebs zu minimieren.