

A photograph of a modern, multi-story office building with a prominent glass facade and a central tower. The building is set against a clear blue sky. A semi-transparent blue banner is overlaid on the lower left portion of the image, containing white text.

TÜV Rheinland.
Ihr Partner für Informationssicherheit.

2017

TÜV Rheinland i-sec. Informations- und IT-Sicherheit.

Führender unabhängiger Dienstleister
für Informationssicherheit in Deutschland

Beratungs- und Lösungskompetenz
in ganzheitlicher Informationssicherheit
– von der Steuerungsebene bis ins
Rechenzentrum inkl. betriebsunter-
stützender Leistungen

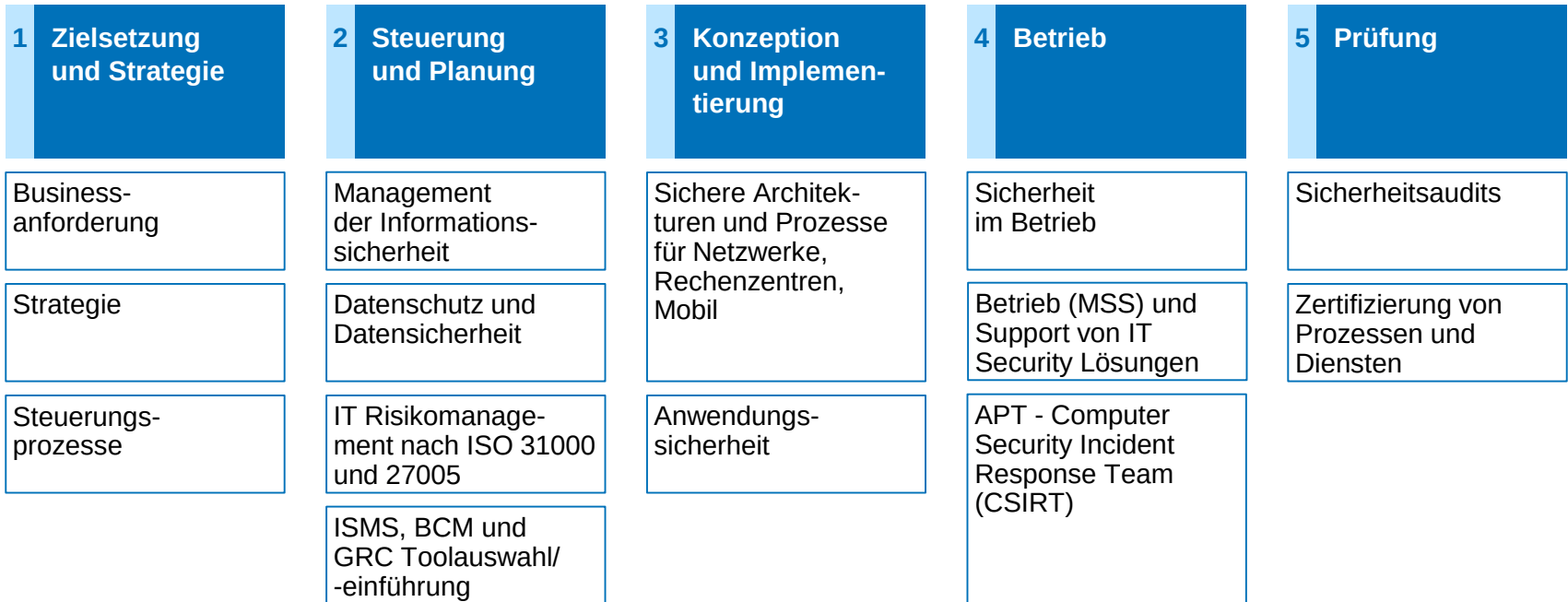
Exzellente Technologie-Expertise,
umfassendes Branchen-Know-how,
Partnerschaften mit Marktführern

International zählen wir im Verbund
mit unserer Schwestergesellschaft OpenSky
zu den wichtigsten unabhängigen Anbietern

Zertifiziert nach ISO 27001 und ISO 9001



Lösungskompetenz. Informations- und IT-Sicherheit.



Abkürzungsverzeichnis

ISMS = Information Security Management System
BCM = Business Continuity Management
GRC = Governance, Risk und Compliance
APT = Advanced Persistent Threat – gezielte Cyberangriffe
MSS = Managed Security Services



! Branchenlösungen, individuelle Konzepte, professionelle Beratung und stark in der Umsetzung.

A photograph of a modern, multi-story office building with a glass facade and a prominent glass pyramid structure. The building is set against a clear blue sky. A semi-transparent blue rectangle is overlaid on the left side of the image, containing the title text.

Risikoorientiertes Datenschutzmanagement nach EU-DSGVO

Roadshow, Mai 2017

Referenten

Thomas Werner

Funktion: Security Consultant, TÜV Rheinland

Fachgebiet: Datenschutzrecht



+49 221 567 832 86



thomas.werner@i-sec.tuv.com



Frank Kümpel

Funktion: Principal Consultant, TÜV Rheinland

Fachgebiet: Informationssicherheit und Datenschutz



+49 221 56783 281



frank.kuempel@i-sec.tuv.com



Eine Übersicht der Themen.

- 1 Datenschutz-Management-System: Pflichtbegründende Normen
- 2 Umfang eines Datenschutz-Management-Systems
- 3 Ziele eines Datenschutz-Management-Systems
- 4 Synergie-Effekte mit bestehenden Informationssicherheitssystemen

Datenschutz-Management-System: Woraus ergibt sich die gesetzliche Pflicht?

Wortlaut der Normen

Art. 5 II DSGVO:

Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Art. 24 I DSGVO:

Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

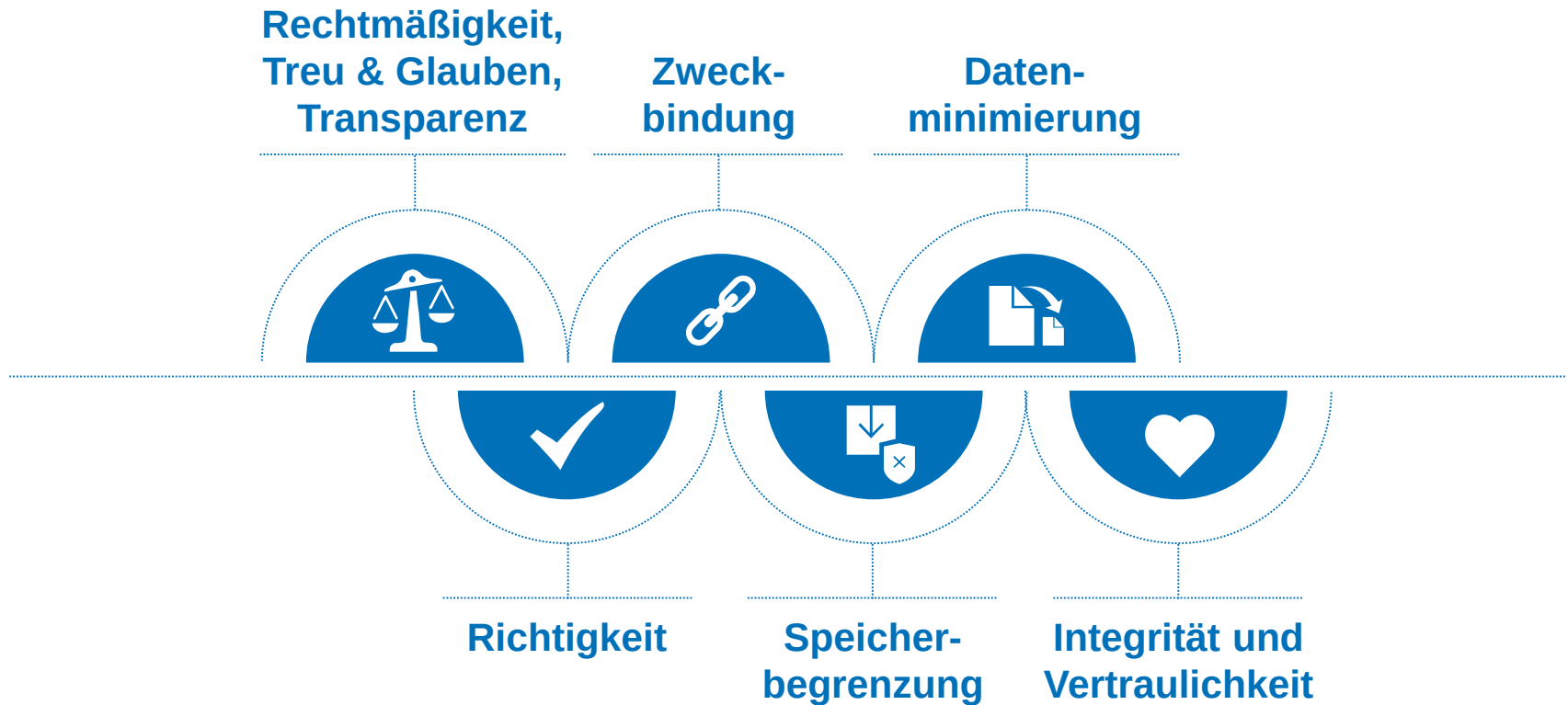


Weitere Normen zur Begründung von Compliance-Management:

§ 91 I AktG; § 43 GmbHG, § 130 I OWiG.

Umfang der Rechenschaftspflicht aus Art. 5 II DSGVO

Aus Art. 5 I DSGVO ergeben sich eine Vielzahl einzuhaltender Grundsätze



Muss das sein? Beispiele praktischer Datenschutz-Risiken

„Durch die Einhaltung des Datenschutzes verkaufen wir nicht ein Hemd mehr“

Häufige Gaps u. Verstöße aus der Praxis:

- Unrechtmäßige Verarbeitung
- Speicherung personenbezogener Daten auf Vorrat
- Fehlende Datenschutz-Folgenabschätzung und Vorabkontrolle
- Unzureichende Kontrolle von Auftragsdatenverarbeitern
- Verarbeitung der Daten in Ländern ohne ausreichendes Datenschutzniveau
- Verletzung des Transparenzgrundsatzes gegenüber Betroffenen und Aufsichtsbehörden
- Fehlende Dokumentation der Verfahren
- Verletzung der Meldepflicht gegenüber der Aufsichtsbehörde
- Unzureichende Erfüllung der Betroffenenrechte hinsichtlich Inhalt, Verständlichkeit und Fristigkeit
- Schadensersatzforderungen Betroffener

Datenschutz-Management mit PDCA-Zyklus

Plan-Do-Check-Act-Zyklus als implizite Vorgabe der DSGVO

Art. 32 I DSGVO

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: (...)

Art. 24 I DSGVO:



(...) Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.



Wer zuvor bereits mit Informationssicherheitsmanagement-Systemen gearbeitet hat, erkennt schon durch den Wortlaut der Norm die Anforderung, einen PDCA-Zyklus zu errichten um personenbezogene Daten systematisch zu schützen.

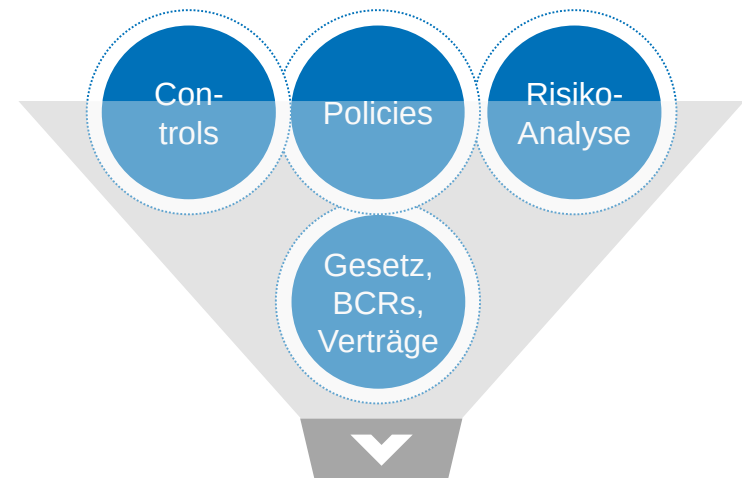
Datenschutz-Management: Essentielle Zutaten

Ziele

Compliance | Rücksicht auf die Grundrechte MA & Kunden | Image-Gewinn u. dadurch Wettbewerbsvorteil

Handlungsfelder

- Klare Delegation & Trennung von Pflichten
- Privacy-by-Design
- Awareness
- Vertragsmanagement (ADV-Dienstleister)
- Systematischer Umgang mit DS-Risiken
- Umfangreiches Dokumentationswesen
- Wahrung der Betroffenenrechte
- Berichtswesen



Datenschutz-Management

BCR: Binding Corporate Rules

Implementierung des Datenschutz-Management-Systems

1

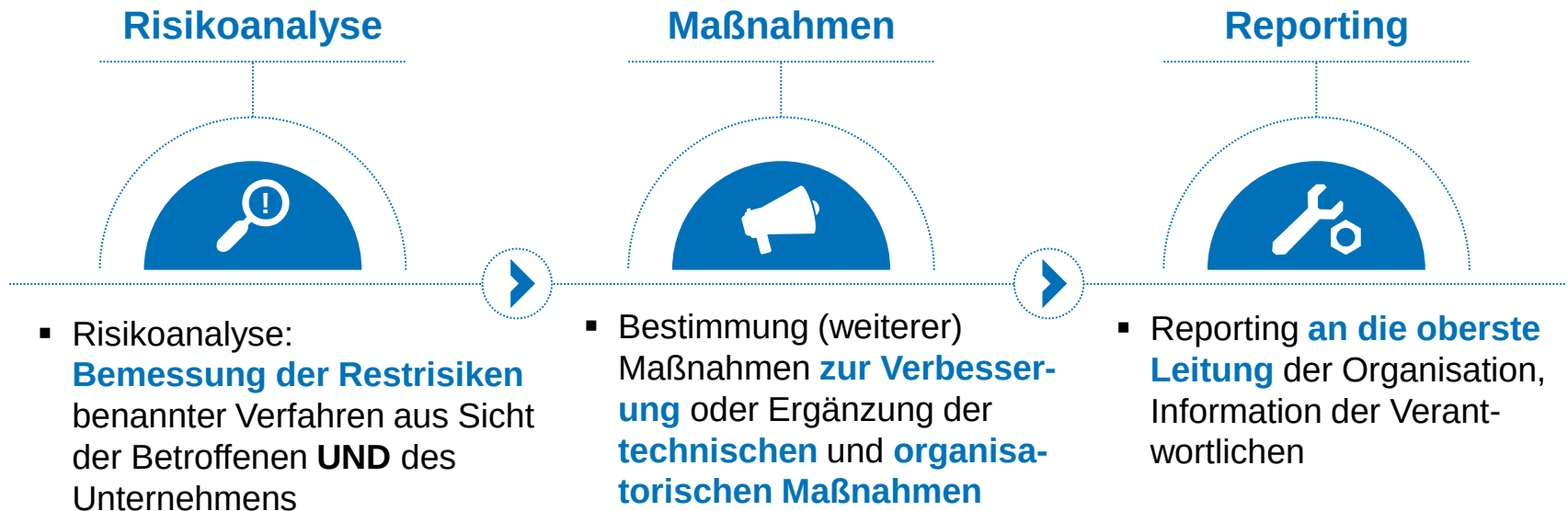
Schritte zur Implementierung eines Datenschutz-Management-Systems



Implementierung des Datenschutz-Management-Systems

2

Schritte zur Implementierung eines Datenschutz-Management-Systems



Datenschutz-Management-System: Drei Varianten

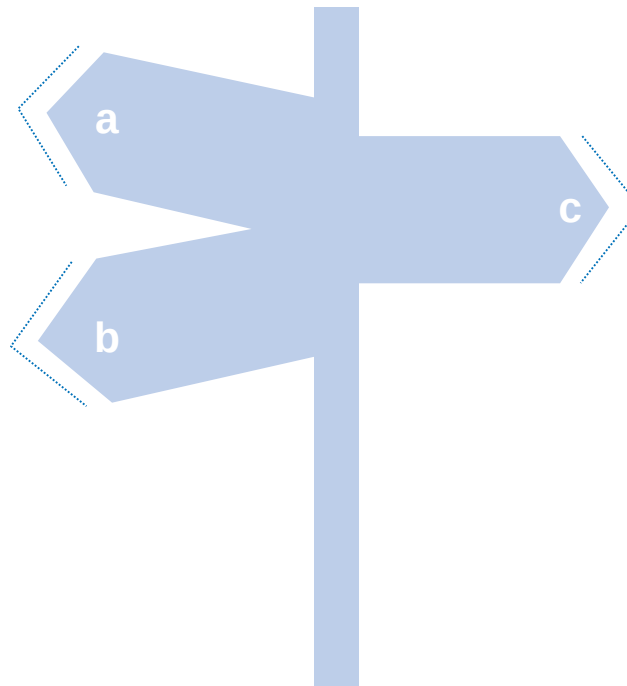
Sie haben die Wahl ...

Aufbau MS nur für PB Daten (Stand-Alone)

- Orientierung entlang ISO/IEC 27001
- Einschränkung auf Erfüllung der Ziele aus der EU-DSGVO & Öffnungsklauseln

Einbau in bestehendes ISMS

- Anpassen Kontext & Anwendungsbereich
- Ergänzung Datenschutz-Spezifika



Aufbau eines „vollen“ ISMS

- Berücksichtigung von Datenschutz-Spezifika direkt beim Aufbau



Eine Zertifizierung ist gesetzlich normiert (Art. 42,43 DSGVO)

Datenschutz-Management:

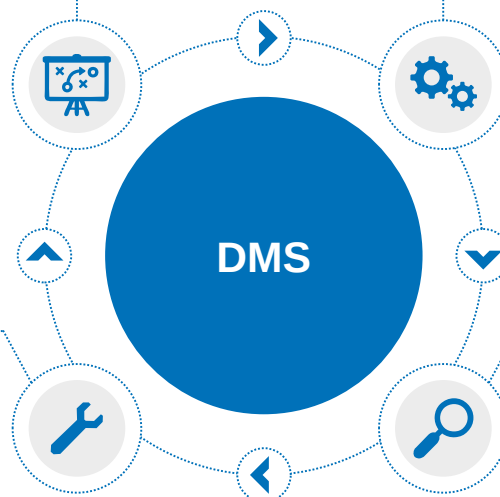
Stand-Alone Datenschutzmanagement

Planning

- Übersicht über Verfahren und Organisation
- Bestimmung des Schutzbedarfs
- Mapping von TOM auf Verfahren
- Ziele & Plan

Improvement

- Behandeln von Abweichungen
- Beseitigen der Ursachen von Abweichungen
- Risikobehandlung durch Implementierung und Verbesserung der TOM



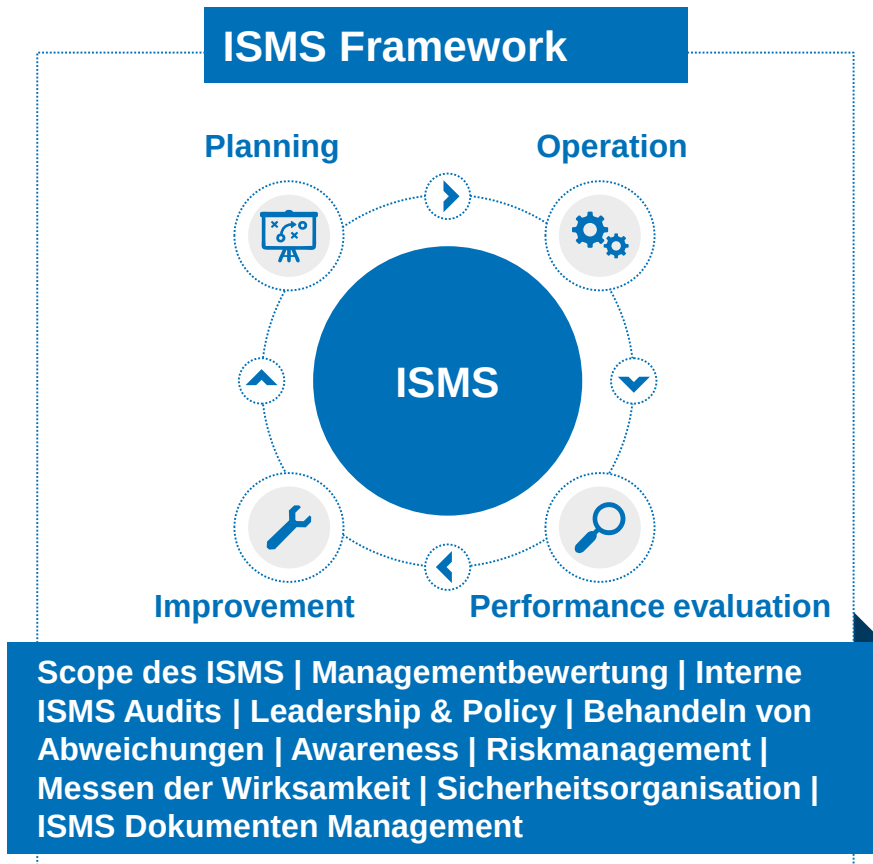
Operation

- Implementierung und Betrieb von TOM, Verfahren und Prozessen
- Datenschutz-Folgenabschätzung (risikobasiert), allg. Datenschutzrisiken
- Berichtswesen

Performance evaluation

- Messen der KPIs
- Überwachungsaudits
- Analyse und Bewertung
- Reporting

Datenschutz-Management: Integration der Datenschutzanforderungen in ein bestehendes ISMS



- Ein ISMS nach ISO 27001 erfüllt die Anforderungen nach PDCA-gestütztem Management der DSGVO ebenso
- Verfahren zur Verarbeitung personenbezogener Daten können in ein bestehendes System integriert werden
- Datenschutz-Spezifika werden in Leitlinien, Richtlinien, Verfahren und Methoden nachgepflegt
- Sofern ein Schutzobjekt des ISMS die Verarbeitung personenbezogener Daten aufweist, lässt sich dieses „flaggen“, mit der Folge, dass auch datenschutzrelevante Risiken oder Bedrohungen bewertet werden
- Maßnahmen lassen sich ISMS- u. datenschutzübergreifend implementieren, wodurch die Wirtschaftlichkeit erhöht wird

Datenschutz-Management: Aufbau eines umfassenden Management-Systems



Ist eine Anforderung der zahlreichen neuen Pflichten nach der DSGVO und eine Anforderung an die Informationssicherheit in der Organisation gegeben, empfiehlt sich der Aufbau eines umfassenden Managements-Systems (ISMS)

Es wird eine zertifizierbare Infrastruktur (organisatorisch, technisch) geschaffen, die einen PDCA-orientierten Umgang mit Informationssicherheitsrisiken, mithin auch Datenschutzrisiken, bescheinigt

Personenbezogene Daten nach DSGVO fallen daher in den Anwendungsbereich eines ISMS nach ISO/IEC 27001

Datenschutz-Management: Unterstützung durch Tools

Tool-Unterstützung erleichtert Dokumentationspflichten und Meldewege

Art. 17 I DSGVO

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden (...)

Art. 12 III DSGVO

Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn (...)

Art. 12 IV DSGVO

(...) so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang (...)

Art. 33 I DSGVO

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der (...) zuständigen Aufsichtsbehörde (...). Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Der Einsatz von GRC-Tools zur Unterstützung eines DMS/ISMS, z.B. Melde- und Berichtswesen, der sachgerechten Bearbeitung von Betroffenenansprüchen sowie der Datenschutz-Folgenabschätzung ist sehr zu empfehlen. (Audit- und Revisionsfestigkeit)

Fragen?

Frank Kümpel

Principal Consultant

TÜV Rheinland i-sec GmbH

Am Grauen Stein

51105 Köln

Tel: +49 221 56783 281

Fax: +49 221 806 1580

frank.kuempel@i-sec.tuv.com

www.tuv.com/informationssicherheit

Thomas Werner

Security Consultant

TÜV Rheinland i-sec GmbH

Am Grauen Stein

51105 Köln

Tel: +49 221 567 832 86

Fax: +49 221 806 1580

thomas.werner@i-sec.tuv.com

www.tuv.com/informationssicherheit



www.tuv.com/it-sicherheits-kongress

8. IT-Sicherheits-Kongress 2017

Cyber Security und Qualität in der digitalen Transformation

7. – 8. November in Frankfurt am Main