secianus

Datenschutz und Informationssicherheit
Partner? Konkurrenten? Gegner?

Vortrag im Rahmen des GDD-Anwendertreffens in Nürnberg

Zertifizierungen und Mitgliedschaften

Horst Pittner
Qualifikationen und Erfahrungen

Ausbildung:

- Technikinformatiker
- Seit 1985 in der EDV
- Programmierung – Netzwerktechnik – SAP
- Seit 2001 in der IT-Sicherheit
- Seit 2003 als Auditor
- Seit 2005 in der Informationssicherheit
- Seit 2005 als Datenschutzberater und DSB

Schwerpunkte:

- Behörden
- Industrie
- Telekommunikation
- ISO 27001 auf Basis IT-Grundschutz
- SAP R/3 – SAP4HANA

Qualifikationen:

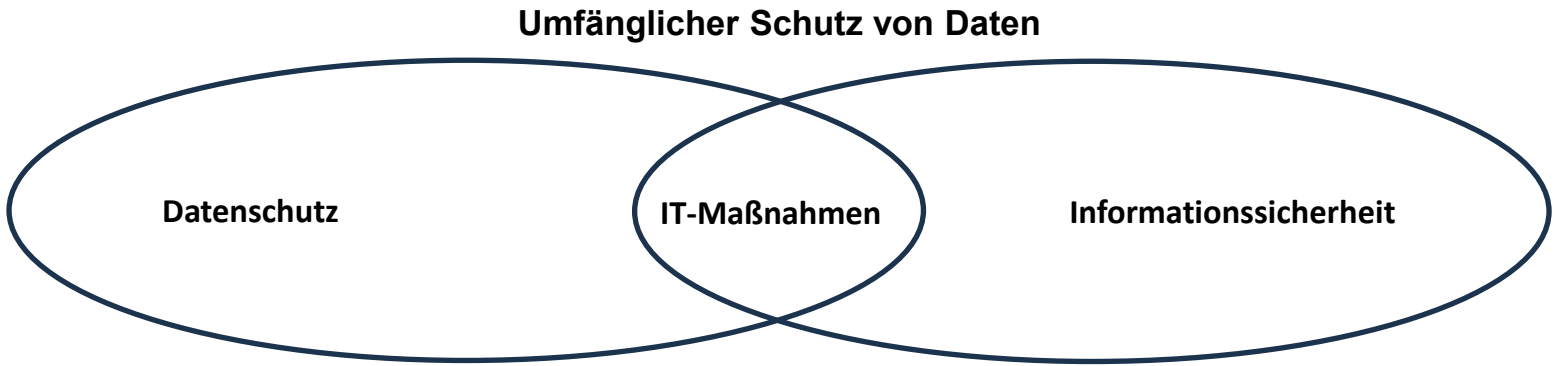
Vom Bundesamt für Sicherheit in der Informationstechnik zertifizierter

- Lead-Auditor für ISO 27001 auf Basis IT-Grundschutz (BSI-ZIG-0020-2023)
- IS-Revisor (BSI-ZISR-0018-2023)
- Prüfverfahrenskompetenz für Prüfungen nach § 8a BSIG

SAP SE zertifizierter

- SAP R/3 Application Consultant

Informationssicherheit im Zusammenspiel von Datenschutz und IT-Sicherheit



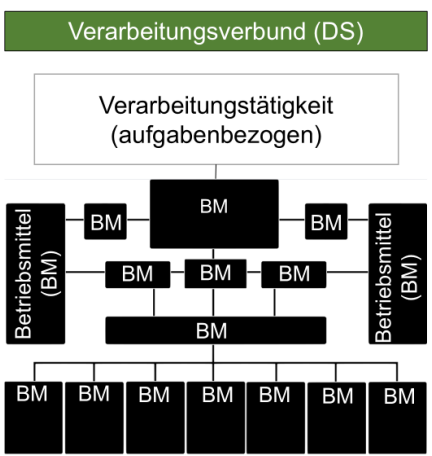
These: Ein **Informationssicherheitsmanagementsystem** berührt den Datenschutz nur am Rande

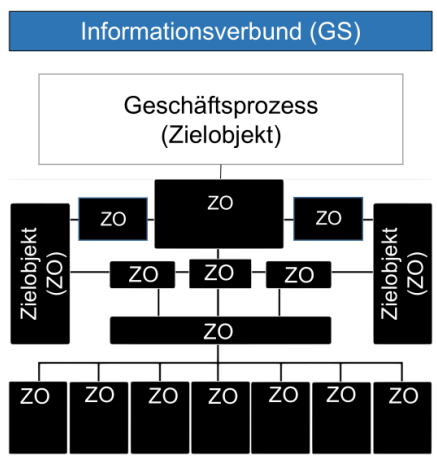
BSI GS-Kompendium - CON.2 Datenschutz
CON.2.A1 Umsetzung Standard-Datenschutzmodell

DIN EN ISO/IEC 27001:2022-01
Die Organisation muss die Anforderungen an die Wahrung der Privatsphäre und den Schutz personenbezogener Daten nach den geltenden Gesetzen und Vorschriften sowie den vertraglichen Anforderungen ermitteln und erfüllen.

Geschäftsprozess vs. Verarbeitungstätigkeit

Verbunde im Datenschutz (DS) und im IT-Grundschutz (GS)





Die **Verarbeitungstätigkeit** einer Stelle wird nach dem Verarbeitungszweck von anderen Verarbeitungstätigkeiten abgegrenzt und unterschieden (Abgrenzung).

Ein Informationsverbund kann alle **Geschäftsprozesse** oder auch nur eine Auswahl der Geschäftsprozessen einer Institution umfassen (Gruppierbarkeit).

07.07.2025 2. IT-Grundschutz-Tag 2025 | IT-Grundschutz und Datenschutz 2

Dr. Christoph Wambsganz
Geschäftsstelle des Bayerischen Landesbeauftragten für den Datenschutz

Gewährleistungsziele vs. Schutzbedarf vs. Risiko

Datenschutz Gewährleistungsziele	BSI-Grundschutz Schutzbedarf	ISO 27001 Risikoeinstufung
Verfügbarkeit	Verfügbarkeit	Verfügbarkeit
Integrität	Integrität	Integrität
Vertraulichkeit	Vertraulichkeit	Vertraulichkeit
Transparenz		Authentizität
Datenminimierung		
Intervenierbarkeit		
Nichtverkettung		

Gewährleistungsziele vs. Schutzbedarf vs. Risiko

Datenschutz Gewährleistungsziele	BSI-Grundschutz Schutzbedarf	ISO 27001 Risikoeinstufung
Verfügbarkeit	Verfügbarkeit	Verfügbarkeit
Das Gewährleistungsziel Verfügbarkeit bezeichnet die Anforderung, dass der Zugriff auf personenbezogene Daten und ihre Verarbeitung unverzüglich möglich ist und sie ordnungsgemäß im vorgesehenen Prozess verwendet werden können.	Verstoß gegen Gesetze/Vorschriften Beeinträchtigung des informationellen Selbstbestimmungsrechts, Beeinträchtigung der persönlichen Unversehrtheit, Beeinträchtigung der Aufgabenerfüllung, negative Innen- oder Außenwirkung und finanzielle Auswirkungen.	Prozess zur Informationssicherheits-Risikobeurteilung, um Risiken im Zusammen hang mit dem Verlust der Verfügbarkeit von Informationen innerhalb des Anwendungsbereichs des ISMS zu ermitteln.

Gewährleistungsziele vs. Schutzbedarf vs. Risiko

Datenschutz Gewährleistungsziele	BSI-Grundschutz Schutzbedarf	ISO 27001 Risikoeinstufung
Integrität	Integrität	Integrität
Das Gewährleistungsziel Integrität … bezeichnet die Eigenschaft, dass die zu verarbeitenden **personenbezogenen** Daten unversehrt, vollständig, richtig und aktuell bleiben.	Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf „Daten“ angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.	Prozess zur Informationssicherheits-risikobeurteilung, um Risiken im Zusammen hang mit dem Verlust der Integrität von Informationen innerhalb des Anwendungsbereichs des ISMS zu ermitteln.

Gewährleistungsziele vs. Schutzbedarf vs. Risiko

Datenschutz Gewährleistungsziele	BSI-Grundschutz Schutzbedarf	ISO 27001 Risikoeinstufung
Vertraulichkeit	Vertraulichkeit	Vertraulichkeit
Das Gewährleistungsziel Vertraulichkeit bezeichnet die Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen oder nutzen kann. Unbefugte sind nicht nur Dritte außerhalb der verantwortlichen Stelle …	Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.	Vertraulichkeits- oder Geheimhaltungs-vereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, sollten identifiziert, dokumentiert, regelmäßig überprüft …

Gewährleistungsziele vs. Schutzbedarf vs. Risiko

secianus

These:

Eine konsistente Zusammenführung von Schutzbedarfsfeststellung und Risikobewertung gemäß Informationssicherheitsstandards mit der Bewertung von Datenschutzrisiken im Sinne der DSGVO ist methodisch nicht möglich, da beide Konzepte auf unterschiedlichen Zielsystemen, Bewertungsmaßstäben und Rechts- / Normgrundlagen beruhen.

Anforderungen und Maßnahmen

Datenschutz	BSI-Grundschutz	ISO 27001
SDM Baustein 43 „Protokollieren“	OPS.1.1.5 Protokollierung	Anhang A, 8.15 Protokollierung
… Es ist erforderlich, um der Rechenschaftspflicht nach Art. 5 Abs. 2 zu genügen.	… betriebs- und sicherheitsrelevante Ereignisse protokollieren, d. h. sie automatisch speichern und für die Auswertung bereitstellen.	Die Protokollierung ist ein zentrales Element der Informationssicherheit, das … unterstützt, ihre Systeme und Daten umfassend zu überwachen und zu schützen.
„Protokollierung“ sollte als ein Verarbeitungen-übergreifender Prozess mit Ausweis des Zwecks, der Verantwortung, der verwendeten Mittel sowie der getroffenen Schutzmaßnahmen …	Ziel … ist es, alle relevanten Daten sicher zu erheben, zu speichern und geeignet für die Auswertung bereitzustellen, damit möglichst alle sicherheitsrelevanten Ereignisse protokolliert werden können.	Protokolle, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen, müssen erstellt, gespeichert, geschützt und analysiert werden.

Anforderungen und Maßnahmen

Datenschutz	BSI-Grundschutz	ISO 27001
Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“	ORP.4 Identitäts- und Berechtigungs-management	Anhang A, 8.3 Informationszugangs-beschränkung
… unrechtmäßigen Datenverarbeitung durch Zugriffe, die … nicht vom **Zweck** der Datenverarbeitung gedeckt sind, unterbunden werden.	… dass Benutzende … ausschließlich auf die IT-Ressourcen und Informationen zugreifen können, die sie für ihre Arbeit benötigen	… Kontrolle des Zugriffs auf vertrauliche Informationen… … um unbefugten Zugriff oder Missbrauch zu verhindern.
Für alle möglichen Datenzugriffe müssen die Gewährleistungsziele mit Blick auf die Rollen bzw. Personengruppen sowie auf die Systeme und Dienste erfüllt werden.	Benutzendenkennungen und Berechtigungen DÜRFEN NUR aufgrund des tatsächlichen Bedarfs und der Notwendigkeit zur Aufgabenerfüllung vergeben werden …	Der Zugang zu Informationen und anderen damit verbundenen Werten muss in Übereinstimmung mit der festgelegten themenspezifischen Richtlinie zur Zugangssteuerung eingeschränkt werden.

Anforderungen und Maßnahmen

- Überwachungssyteme SIEM, Logging, Videoüberwachung
  - ISO/IEC 27001 (A.12.4.1, A.16.1.7) OPS.1.1.7.A22 Einbindung des Systemmanagements in automatisierte Detektionssysteme vs.
  - Prinzip der Datenminimierung und Verhältnismäßigkeit Art. 5 und 6 DSGVO
- Backups vs. Datenlöschung
  - ISO/IEC 27001 (Anhang A.12.3.1) & CON.3 Datensicherungskonzept fordern Backups
  - Art. 17 DSGVO („Recht auf Vergessenwerden“)
- Biometrische Zugangskontrollen (Art. 9)
- Zentrale Benutzerverwaltung vs. Datenminimierung Art. 5 Abs. 1 lit. c DSGVO
- Langzeitaufbewahrung von Logs vs. Speicherfrist Art. 5 Abs. 1 lit. e DSGVO
- Archivierung …
- …

Risikoanalysen

Datenschutz	BSI-Grundschutz	ISO 27001
SDM 3.1 D3.2 Risikobetrachtung	Standard 200-3	ISO 27005
Risikohöhe, Schutzbedarfsstufe, Schutzniveau und Restrisiko	Gefährdung Eintrittshäufigkeit Auswirkung Restrisiko	Schwachstelle / Bedrohung Eintrittshäufigkeit Auswirkung Restrisiko
Der Schutzbedarf einer natürlichen Person bei der Verarbeitung personenbezogener Daten in Bezug auf ihre Rechte und Freiheiten ergibt sich aus dem Risiko, das von der Verarbeitungstätigkeit und deren Eingriffsintensität ausgeht.	… das Risiko ermittelt, das von einer Gefährdung ausgeht. Wie hoch dieses Risiko ist, hängt sowohl Von der Eintrittshäufigkeit der Gefährdung als auch von der Höhe des Schadens ab, der dabei droht.	Das Ziel der ISO 27005 besteht darin, eine präzise Bewertung der Informationssicherheitsrisiken durchzuführen, auf deren Grundlage das Informationssicherheits-Managementsystem (ISMS) optimiert werden kann.

Resümee

- Schutzbedarf im Datenschutz ist nicht gleich Schutzbedarf in der Informationssicherheit.
- Datenschutzziele sind häufig konträr zu Informationssicherheitszielen
- Informationssicherheitsmaßnahmen stehen sehr oft im Widerspruch zu Datenschutzmaßnahmen.

<u>These:</u>

Datenschutz und Informationssicherheit sind **Konkurrenten** um die Hoheit über die Sicherheitsmaßnahmen.
Keine Partner aber auch keine Gegner.

SECIANUS GmbH & Co. KG

Further Straße 14
D-90530 Wendelstein

Tel.: +49 (0) 9129 29 39 808
Fax: +49 (0) 911 39 38 069

eMail: info@secianus.de
Internet: www.secianus.de