Standard-Datenschutzmodul 3.0

Vortrag im Rahmen der verinice.XP 2024

Zertifizierungen und Mitgliedschaften

secianus

Sachverständige für Datenschutz und Informationssicherheit

Horst Pittner
Qualifikationen und Erfahrungen

Unternehmensschützer

Schwerpunkte:

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

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
- Seit 2016 als ext. Datenschutzbeauftragter

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

Agenda

1. Was ist das Standard-Datenschutzmodell 3.0 (SDM 3.0)?
2. Standard-Datenschutzmodell 3.0 und die „Verfahrensspezifische Risikobewertung“
3. Gewährleistungsziele im SDM 3.0
4. Anforderungen und Maßnahmen
5. Der SDM Würfel und die Risiko-Typen
6. Umsetzung in verinice
7. Negativaspekte

Resümee

1. Was ist das SDM?

Mit dem Standard-Datenschutzmodell (SDM) wird ein Werkzeug bereitgestellt, mit dem die

- Auswahl und die kontinuierliche Evaluation technischer und organisatorischer Maßnahmen unterstützt wird,
- die sicherstellen und den Nachweis dafür erbringen, dass die Verarbeitung personenbezogener Daten nach den Vorgaben der DS-GVO erfolgt.

Grundrechtsabwägung!

Datenschutzmodell – kein Datenschutz-**recht**-modell

1. Was ist das SDM?

Mit dem Standard-Datenschutzmodell kann **nicht** geprüft werden, ob eine Verarbeitung nach DSGVO zulässig ist oder nicht!

Die Prüfung der Verhältnismäßigkeit des Grundrechtseingriffs einer Verarbeitung ist **nicht** vom SDM umfasst.

1. Was ist das SDM?

Die Anwendungsbereiche des Standard-Datenschutzmodells sind Planung, Einführung und Betrieb von Verarbeitungstätigkeiten mit denen personenbezogene Daten verarbeitet werden (personenbezogene Verarbeitungen) sowie deren Prüfung und Beurteilung.

2. Verfahrensspezifische Risikobewertung

Die DS-GVO knüpft die Anforderungen an technische und organisatorische Maßnahmen an das mit der Verarbeitung der personenbezogenen Daten verbundene **Risiko** für die Rechte und Freiheiten betroffener Personen.
Art. 32 (2) DSGVO

- Aus der Perspektive der Organisation wird das Risiko für die Betroffenen mit „normalen“ oder „hohen“ Schutzbedarf klassifiziert.

- Im SDM wird der Schutzbedarf ersetzt durch verarbeitungsindividuelles Risiko aus Perspektive der Betroffenen
  - Risikoanalyse für jede Verarbeitung einzeln
  - Gefährdungen sind individuell zu eruieren
  - Eintrittswahrscheinlichkeiten sind individuell zu eruieren

2. Verfahrensspezifische Risikobewertung

Die DS-GVO knüpft die Anforderungen an technische und organisatorische Maßnahmen an das mit der Verarbeitung der personenbezogenen Daten verbundene **Risiko** für die Rechte und Freiheiten betroffener Personen.
Art. 32 (2) DSGVO

Selbstbestimmungsrecht	Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.
Selbstbestimmungsrecht	Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.

3. Normatives Gravitätszentrum

1. **Datenminimierung / Datensparsamkeit**:
   Nur die für den Zweck der Datenverarbeitung notwendigen Daten dürfen verarbeitet werden.
2. **Verfügbarkeit:**
   Der Zugriff auf personenbezogene Daten und ihre Verarbeitung muss unverzüglich möglich sein.
3. **Integrität**:
   Personenbezogene Daten müssen vollständig, korrekt und auf dem neuesten Stand sein.
4. **Vertraulichkeit**:
   Personenbezogene Daten müssen vor unbefugtem Zugriff geschützt werden.
5. **Nichtverkettung:**
   Anforderung, dass personenbezogene Daten nicht zusammengeführt, also verkettet, werden.
6. **Transparenz**:
   Personenbezogene Daten müssen in einer klaren und verständlichen Sprache dargestellt werden. Personen müssen wissen, wer für die Verarbeitung der Daten verantwortlich ist, welche Daten verarbeitet werden und zu welchem Zweck.
7. **Intervenierbarkeit**:
   Die den Betroffenen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Einschränkung müssen gewährleistet werden.

3. Normatives Gravitätszentrum

1. **Datenminimierung / Datensparsamkeit**:
   Nur die für den Zweck der Datenverarbeitung notwendigen Daten dürfen verarbeitet werden.
2. **Verfügbarkeit:**
   Der Zugriff auf personenbezogene Daten und ihre Verarbeitung muss unverzüglich möglich sein.
3. **I**
   …auf dem neuesten Stand sein
   …Anforderung, dass personenbezoge…

Informationssicherheit schützt Organisationen und deren Verarbeitungstätigkeiten,
der Datenschutz schützt Personen mit ihren Grundrechten vor genau diesen Verarbeitungstätigkeiten

6. **Transparenz**:
   Personenbezogene Daten müssen in einer klaren und verständlichen Sprache dargestellt werden. Personen müssen wissen, wer für die Verarbeitung der Daten verantwortlich ist, welche Daten verarbeitet werden und zu welchem Zweck.
7. **Intervenierbarkeit**:
   Die den Betroffenen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Einschränkung müssen gewährleistet werden.

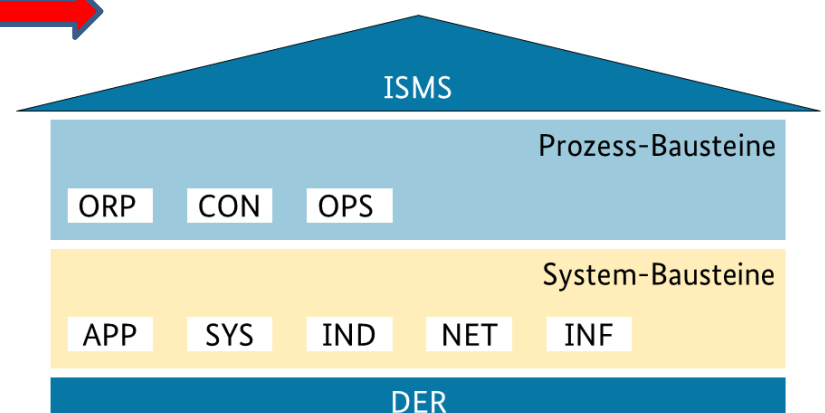
3. Gewährleistungsziele (vs. Grundschutz)

- 5. DSGVO Gewährleistungsziele
  - 5.1 Datenminimierung
    - a) [BASIS] Berechtigungs- und Rollenkonzept
    - b) [BASIS] Löschkonzept, Löschung und Vernichtung
    - c) [BASIS] Reduzierung von erfassten Attributen der betroffenen Personen
  - 5.2 Verfügbarkeit
    - [BASIS] Verfügbarkeit
  - 5.3 Integrität
    - [BASIS] Integrität
  - 5.4 Vertraulichkeit
    - a) [BASIS] Zugelassene Ressourcen und Umgebung
    - b) [BASIS] Umgang mit Datenschutzverletzungen
    - c) [BASIS] Passwortkonzept
  - 5.5 Nichtverkettung
    - a) [BASIS] Zweckbindung der Verarbeitungstätigkeit
    - b) [BASIS] Verfahren bei Zweckänderung
  - 5.6 Transparenz
    - a) [BASIS] Verzeichnis der Verarbeitungstätigkeiten
    - b) [BASIS] Protokollierung
    - c) [BASIS] Dokumentation
    - d) [BASIS] Erfüllung von Informationspflichten
    - e) [BASIS] Erfüllung des Auskunftsanspruchs betroffener Personen
  - 5.7 Intervenierbarkeit
    - a) [BASIS] Verfahren zur Geltendmachung von Rechten durch Betroffene
    - b) [BASIS] Berichtigungsmöglichkeit von Daten
    - c) [BASIS] Einschränkung der Verarbeitung
    - d) [BASIS] Identifizierung und Authentifizierung von Betroffenen
    - e) [BASIS] Datenübertragbarkeit

ULD

Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschutz-Kompendium



4. Anforderungen und Maßnahmen

1. Gewährleistungsziel: Transparenz

   Maßnahme: Erstellung einer Datenschutzerklärung, die transparent über die Verarbeitung personenbezogener Daten informiert

2. Gewährleistungsziel: Integrität und Vertraulichkeit

   Maßnahme: Einsatz von Verschlüsselungstechnologien, um die Integrität und Vertraulichkeit von personenbezogenen Daten zu gewährleisten

3. Gewährleistungsziel: Verfügbarkeit

   Maßnahme: Implementierung von Backup-Systemen, um die Verfügbarkeit personenbezogener Daten im Falle eines Systemausfalls sicherzustellen

4. Gewährleistungsziel: Rechtmäßigkeit

   Maßnahme: Einholung einer Einwilligung zur Verarbeitung personenbezogener Daten gemäß den Anforderungen der DSGVO

5. Gewährleistungsziel: Zweckbindung

   Maßnahme: Festlegung klarer Zwecke für die Verarbeitung personenbezogener Daten und Begrenzung der Verarbeitung auf diese Zwecke

4. Anforderungen und Maßnahmen

1. Gewährleistungsziel: Transparenz

   Maßnahme: Erstellung einer Datenschutzerklärung, die transparent über die Verarbeitung personenbezogener Daten informiert

2. Gewährleistungsziel: Integrität und Vertraulichkeit

   Maßnahme: Einsatz von Verschlüsselungstechnologien, um die Integrität und Vertraulichkeit von personenbezogenen Daten zu gewährleisten

- Anforderungen und Maßnahmen müssen auf 3 Ebenen bedient werden:
  - Ebene 1 – Fachverfahren (Prozesse)
  - Ebene 2 – Fachapplikation (Anwendung)
  - Ebene 3 – Infrastruktur (Systeme, Netze, Räumlichkeiten)

onenbezogener

   Maßnahme: Einholung einer Einwilligung zur Verarbeitung personenbezogener Daten gemäß den Anforderungen der DSGVO

5. Gewährleistungsziel: Zweckbindung

   Maßnahme: Festlegung klarer Zwecke für die Verarbeitung personenbezogener Daten und Begrenzung der Verarbeitung auf diese Zwecke

4. Anforderungen und Maßnahmen

SDM

Maßnahmenkatalog

Hier sind die Bausteine veröffentlicht, die als verbindliche Versionen auf der Basis des SDM V2.0 dienen.

Die einzelnen von der Datenschutzkonferenz bzw. vom Arbeitskreis „Technik“ freigegeben Bausteine des Katalogs werden hier sukzessive veröffentlicht und sind damit zur Anwendung freigegeben.

Wir empfehlen den Anwendern, ihre Erfahrungen bei der Erprobung der verbindlichen Bausteine den Datenschutzaufsichtsbehörden mitzuteilen (z.B. unter sdm@datenschutz-mv.de), und somit zur Weiterentwicklung von Methode und Maßnahmen beizutragen.

Bezeichnung	Format	Größe
Baustein 11 „Aufbewahren“ (Version 1.0 vom 6. Oktober 2020)	PDF	0,75 MB
Baustein 41 „Planen und Spezifizieren“ (Version 1.0 vom 25. März 2021)	PDF	1,08 MB
Baustein 42 „Dokumentieren“ (Version 1.0a vom 2. September 2020)	PDF	0,12 MB
Baustein 43 „Protokollieren“ (Version 1.0a vom 2. September 2020)	PDF	0,14 MB
Baustein 50 „Trennen“ (Version 1.0 vom 6. Oktober 2020)	PDF	0,67 MB
Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“ (Version 1.0 vom 01.11.2021)	PDF	0,82 MB
Baustein 60 „Löschen und Vernichten“ (Version 1.0a vom 2. September 2020)	PDF	0,14 MB
Baustein 61 „Berichtigen“ (Version 1.0 vom 6. Oktober 2020)	PDF	0,52 MB
Baustein 62 „Einschränken der Verarbeitung“ (Version 1.0 vom 6. Oktober 2020)	PDF	0,51 MB

Der Landesbeauftragte für Datenschutz
und Informationsfreiheit Mecklenburg-Vorpommern

https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

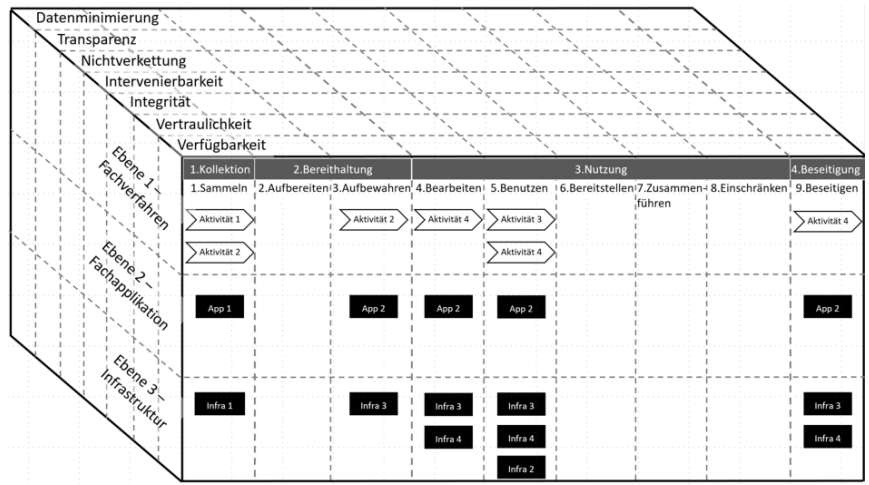
5. Der SDM-Würfel (SDM 3.0)

Der SDM-Würfel

X-Achse: Datenebenen

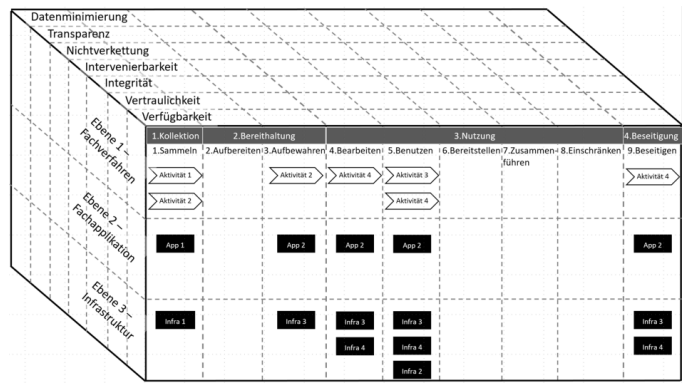
Y-Achse: Phasen eines Datenlebenszyklus

Z-Achse: Gewährleistungsziele



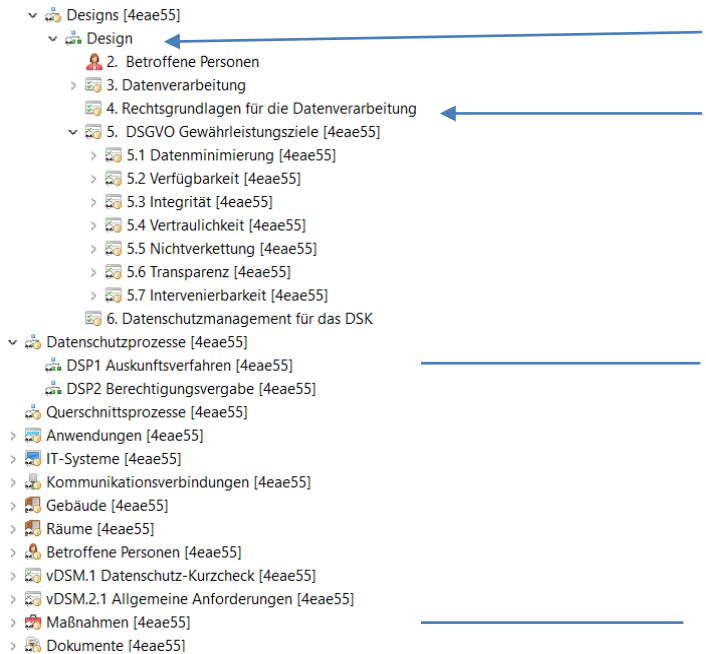
5. Der SDM-Würfel und die Risikotypen (SDM 3.0)

Mit dem SDM 3.0 ergeben sich folgende Neuerungen im Vergleich zur bisherigen Version (SDM 2.0b):



1. Der „SDM-Würfel“ ist eine methodische Hilfe; für die Abbildung eines Datenschutzkonzeptes oder des Datenschutzmanagements nicht relevant.
2. Risiko-Typen „Risiken für Betroffene“ bringt keine neue Anforderung an das DS-Konzept.
3. Aufnahme von Gefährdungen und einfache Risikoanalyse:
   Über die Bewertung der Maßnahmen zu den Gewährleistungszielen hinaus wird eine Risikobewertung für das jeweilige Verfahren gefordert, d.h. der Umsetzungsstatus der Gewährleistungsziele wird als Bewertungsgrundlage in die Risikobewertungen der Verfahren überführt. → Verfahrensspezifische Risikobewertung

6. Abbildung des Datenschutzkonzeptes in verinice



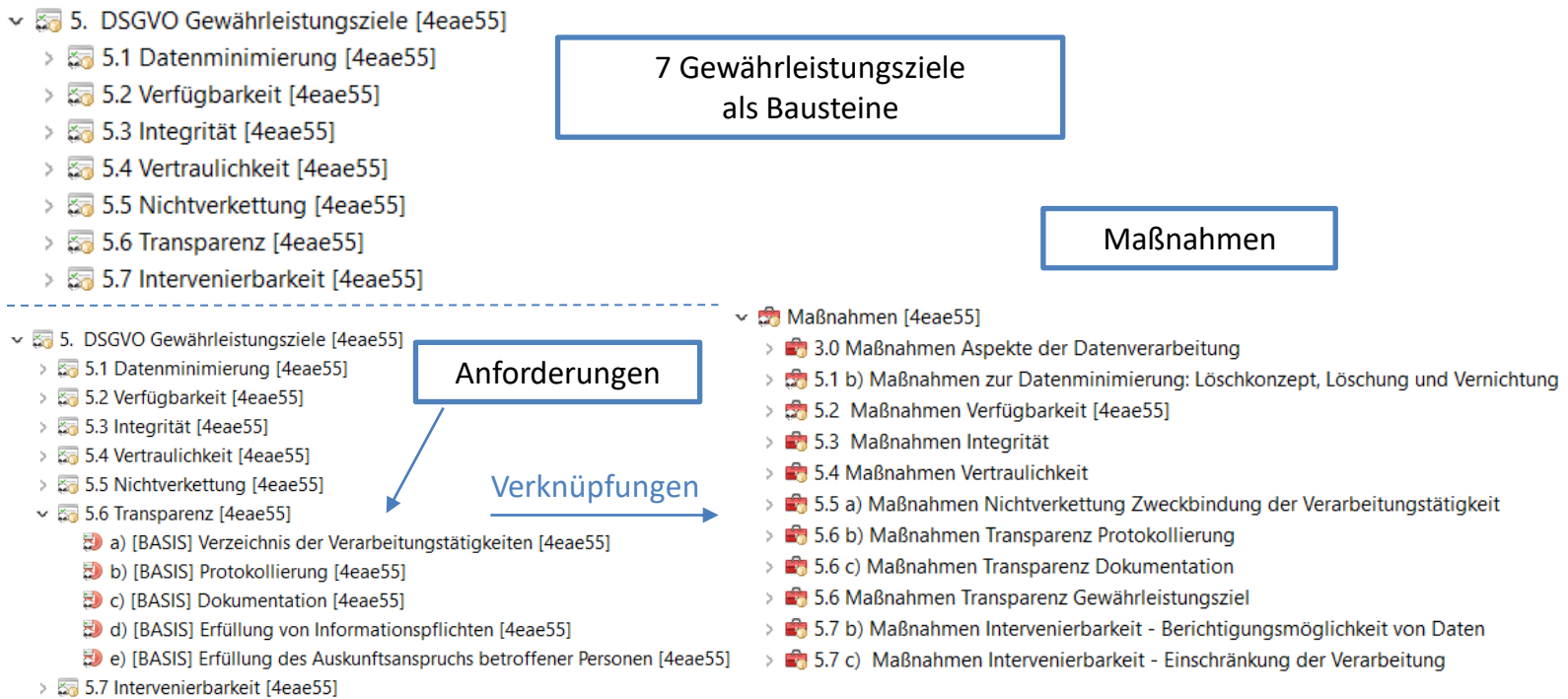
In verinice als Prozess angelegt

Inhalte in verinice als Baustein angelegt

Querschnittsprozesse werden nach Standarddatenschutzmodell („SDM“) mit den Gewährleistungszielen verknüpft

Maßnahmen werden mit Anforderungen aus den Bausteinen verknüpft

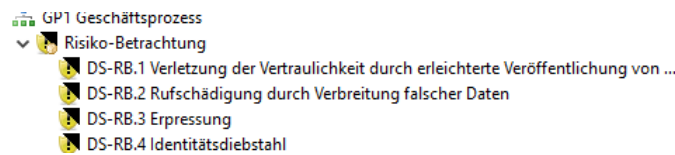
6. Abbildung des Datenschutzkonzeptes in verinice



6. SDM 3.0: Verfahrensspezifische Risikobewertung

Im verinice werden nun die Gefährdungen in der Gefährdungsgruppe „Risiko-Betrachtung“ aufgelistet. Folgende Gefährdungen sind in Anlehnung an Erwägungsgrund 75 DSGVO definiert:

- ✓ Verletzung der Vertraulichkeit durch erleichterte Veröffentlichung von Daten
- ✓ Rufschädigung durch Verbreitung falscher Daten
- ✓ Erpressung
- ✓ Identitätsdiebstahl
- ✓ Erschwerung der Rechtsausübung
- ✓ …

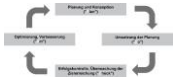


7. Negativaspekte

1. Komplexität:
   Das SDM ist ein sehr umfassendes Datenschutz-Framework und kann für kleinere Unternehmen oder Organisationen zu komplex sein. Die Implementierung des SDM erfordert eine sorgfältige Planung und einiges an Aufwand.
2. Starre Struktur:
   Das SDM bietet zwar eine umfassende Struktur für Datenschutz-Compliance, ist jedoch auch sehr starr und unflexibel. Es kann schwierig sein, das SDM an die individuellen Bedürfnisse eines Unternehmens oder einer Organisation anzupassen.
3. Abhängigkeit von externen Dienstleistern:
   Die Implementierung des SDM erfordert oft die Unterstützung von externen Datenschutz-Experten oder Beratern. Dies kann zu hohen Kosten führen und es kann schwierig sein, geeignete Dienstleister zu finden.

7. Negativaspekte

4. Hohe Anforderungen an das Personal:
   Die Implementierung und Aufrechterhaltung des SDM erfordert eine hohe Expertise im Bereich Datenschutz und ein starkes Engagement des Personals. Dies führt zu zusätzlichen Schulungs- und Fortbildungsmaßnahmen.
5. Mangelnde Flexibilität bei Änderungen:
   Das SDM ist auf Stabilität ausgelegt und Änderungen an der Struktur oder den Prozessen können schwierig sein. Dies kann zu Problemen führen, wenn sich die Anforderungen an den Datenschutz ändern oder neue Datenschutz-Risiken auftreten.



6. Hoher administrativer Aufwand:
   Die Implementierung des SDM erfordert eine umfassende Dokumentation und Verwaltung von Datenschutz-Maßnahmen und -Prozessen. Dies führt zu einem hohen administrativen Aufwand und wird immer zusätzliche Ressourcen erfordern.

Resümee

- Als Datenschutzmanagementsystem geeignet,
  aber im Regelfall erheblich aufwendiger als andere Normen.
  - Aufwand zur Umsetzung auch bei kleinen Institutionen groß.
  - Bei großen Institutionen gleicht sich der Aufwand für das SDM an den Aufwand für die ISO 27701 oder die VdS-100010 an.

- Die Normen ISO 27701 und die VdS-10010 haben das Ziel den Datenschutz in der Institution beherrschbar zu machen.
  Das SDM hat das Ziel die Institution zu beherrschen.

Vielen Dank für Ihre Aufmerksamkeit

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

Grund: Ich bin der Verfasser dieses Dokuments
Ort: Wendelstein
Datum: 2024.03.02 16:26:20+01'00'