ATLANTIC
Hotel Kiel
08.09.2025

Wie viel IT-Grundschutz „steckt“ im SDM?

Martin Rost
Tel.: 0431 988-1391
ULD32@datenschutzzentrum.de
https://www.datenschutzzentrum.de/

SDM
Standard
Datenschutz
Modell

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Agenda

1. Das Problem...
2. Ziele, Aufgaben und Standing der beiden Methoden
3. Die Gemeinsamkeiten
4. Die Unterschiede
5. Geläufige Kompromisse
6. Zusammenfassung und Fazit

Das Problem

Die Umsetzung von Datenschutzanforderungen (DSGVO, BDSG, LDSG, EU-Acts, weitere Spezialgesetze) ist gelungen, wenn die folgenden drei Bedingungen erfüllt werden:

1. Rechtsgrundlage (Gesetz, Vertrag, Einwilligung + Policy) liegt vor.

2. Betroffenenrechte (auf Auskunft, Korrektur, Löschen usw. der DSGVO) werden umgesetzt, und

3. IT-Sicherheit wird sichergestellt, bevorzugt mit einer hohe Qualität sichernden Methode und den Maßnahmen des IT-Grundschutzes (ITGS) des BSI.

Das Problem

So denken **viele IT-SiBe** und **alle Praktiker*innen**, die in IT-Sicherheit ausgebildet wurden, über die Umsetzung der über operativen Datenschutzanforderungen. Ebenso denken viele DSB, operativer Datenschutz wird mit IT-Sicherheit weitgehend miterledigt.

Entsprechend blicken wohl die meisten Praktiker*innen wie folgt auf das SDM:

„SDM ist wie ITGS, erweitert nur um zusätzliche Maßnahmen wegen der weiteren Schutzziele.“ Knapp:

SDM = „ITGS plus“

THESE

Und damit interessiert auch nur folgendes am SDM:

1. *„Welche vom **ITGS vorgesehenen Maßnahmen erfüllen bereits** die Anforderungen der DSGVO bzw. des SDM?“*

2. *„Müssen **zusätzliche Maßnahmen** getroffen werden, über die Umsetzung der Betroffenenrechte hinaus?“*

Das Problem

Datenschutz-Scope in einem ITGS-Tool (Bsp. „Hiscout“*)

Hiscout zu „Synergien ITGS – DS/SDM“

„Im Datenschutz geht es um den Schutz personenbezogener Daten (pbD), die eine **Teilmenge** der oben erwähnten „organisationseigenen Informationen“ sind.“

„Der Datenschutz weicht in seinen **Bedürfnissen** von den beiden vorgenannten Regelwerken (gemeint sind ITGS/BCM, MR) ab: Für die Betrachtung der Risiken wird der **Blickwinkel des Betroffenen** eingenommen, es wird nur eine Teilmenge der vorhandenen Daten betrachtet und die Einteilung der Schutzbedarfe erfolgt in nur zwei Kategorien: „**Hoher Schutzbedarf**“ (es sind pbD vorhanden) und „**Sehr hoher Schutzbedarf**“ (es sind besondere Kategorien von pbD vorhanden).“

„Auch die im **Datenschutz relevanten TOMs** können direkt aus dem Pool der im BCM und/oder **Grundschutz gepflegten Maßnahmen ausgewählt werden und müssen nicht „neu erfunden“ werden**.“

SDM-Sicht

nicht pbDaten als Teilmenge aller schutzwürdigen Daten schützen, sondern **Eingriffsintensität der Verarbeitung verringern**

Datenschutz hat keine „Bedürfnisse“, sondern es bestehen **gesetzliche Anforderungen**

Blickwinkel des Betroffenen ist nicht nur gegen „Hacker“, sondern auch **gegen die Verarbeitung** durch die Organisation.

DSGVO/SDM: normales oder hohes **Risiko**

ITGS liefert nicht alle wesentlichen Maßnahmen an -> bspw. nicht zur Anonymisierung, Pseudonymisierung, Trennung, Protokollierung aus Compliancegründen ...

*Textquelle: https://www.hiscout.com/wp-content/uploads/synergien-grundschutz-datenschutz-notfallmanagement.pdf

Das Problem
Beispiel ITGS-Tool „Cyclesec“

Die Abbildung auf das Standard-Datenschutzmodell in Zahlen

Von den 65 generischen Maßnahmen des SDM lassen sich rund ein Drittel (23) vollständig und weitere neun teilweise durch die Anwendung des IT-Grundschutz-Kompendiums erfüllen. Durch die teilweise entstehenden doppelten Verknüpfungen mit Bausteinen des IT-Grundschutz Kompendiums sind für die Abdeckung der 65 generischen Maßnahmen des SDM im benutzerdefinierten Baustein CON.2.bd.1 nur 24 benutzerdefinierte Anforderungen nötig:

65	23	9	1	24
Generische Maßnahmen im SDM	vollständig durch IT-Grundschutz erfüllbar	teilweise durch IT-Grundschutz erfüllbar	Benutzerdefinierter Baustein CON.2.bd.1	Benutzerdefinierte Anforderungen

In unseren CycleSEC ISMS-Frameworks verwenden wir diesen und weitere benutzerdefinierte Bausteine mit entsprechenden IT-Grundschutz-Checks als Schnittstelle zwischen SDM und ISMS.

https://cyclesec.com/2024/09/02/sdm-teil-1-generischen-massnahmen-im-standard-datenschutzmodell/

Wenn man operativen Datenschutz/SDM der Informationssicherheit/ ITGS unterordnet – und man das Problem auf den Schutz personenbezogener Daten verengt und dabei nur auf der Ebene von Schutzmaßnahmen agiert –, **kommt im Ergebnis kein Datenschutz bzw. Grundrechteschutz** heraus. Denn Datenschutz bedeutet nicht „Schutz besonderer Daten, weil personenbezogen“ sondern „Schutz von Personen vor den Verarbeitungen von Organisationen, die die Verarbeitungen in ihrem Sinne gestalten“.

Zweck

Ziele der DSK („SDM-Owner“): Koordination der Tätigkeiten der DSAen in Deutschland, mit Berücksichtigung der DSAen auch der EU, um für eine einheitliche Auslegung und Anwendung der DSGVO unter unabhängigen DSA zu sorgen. Aufgaben (u.a.): Publikation von Entschließungen, Orientierungshilfen, Kurzpapieren, **Anwendungshinweisen -> SDM**

Zweck des SDM
"Mit dem Standard-Datenschutzmodell (SDM) wird ein **Werkzeug** bereitgestellt, mit dem die **Auswahl und Bewertung 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."

"Das SDM bietet mit seinen Gewährleistungszielen eine **Transformationshilfe** zwischen Recht und Technik und unterstützt damit einen ständigen Dialog zwischen Beteiligten aus dem fachlichen, juristischen und technisch-organisatorischen Bereich."

Das SDM bietet eine Methodik der **(wechselseitigen, verlustbehafteten) Transformation grundrechtlich-normativer Anforderungen in operative Anforderungen.**

Quelle: DSK: https://www.datenschutzkonferenz-online.de/SDM-V3.1, S. 8

SDM Meilensteine

2000: Systematik von Schutzzielen (Informatik-Spektrum, Pfitzmann / Wolf - DuD, Pfitzmann / Federrath)
2007: Pfitzmann berät das BVerfG zur Vorbereitung des Integritäts- und Vertraulichkeitsurteils; Betonung des Abwägenmüssens von Schutzzielen
2008: Pfitzmann, Hansen, Rost, Schutzziele-Diskussion im Kontext Identity-Management
2009: **"Datenschutz-Schutzziele - revisited"** (Artikel in DuD, Rost / Pfitzmann)
2010: DSK erklärt **Schutzziele als Teil der Modernisierung** des Datenschutzrechts.
2012: **Verbindung von Schutzzielen und Maßnahmen nach *Methodik-Vorbild ITGS*** (DuD 2012/06)
2012: Gründung der UAGSDM des AK-Technik der DSK
2015: SDM-V1.0 („Schutzziele“ -> „Gewährleistungsziele“, Bezug BDSG, LDSG, Umfang: 40 S.)
2018: Anpassung an DSGVO (insbes: Risikomodellierung und Verfahrensfokussierung)
2019: **Schnittstelle ITGS <-> operativer Datenschutz** seitens BSI: CON.2-Baustein
2020: SDM-V2 (Bezug: DSGVO, Umfang: 56 S.)
2020: **IT-Planungsrat empfiehlt öffentlicher Verwaltung in Deutschland die Anwendung des SDM**
2021: Generische Maßnahmen: 65; spezif. Maßnahmen in Bausteinen: ca. 400
2022: Entwicklung von **SDM-Tools der 2. Generation** (Führung durch „Wizzards“ statt „Excel-Tabellen“)
2023: **"SDM-Würfel" – alle Anforderungen an eine Verarbeitung, integriert in einer Grafik**
2024: Verabschiedung SDM-V3.1, Betriebsmittel, neue Abbildungen, neues Logo
2025: **SDM-V3.1a, Beginn der Modernisierung**

Quellen:
DSK: https://www.datenschutzkonferenz-online.de/
Rost, Martin, 2024: Das Standard-Datenschutzmodell (SDM) - Einführung in die Umsetzung der operativen Anforderungen der DSGVO Springer-Vieweg, 2. Aufl.

Zweck

Gründung des BSI: 1.1.1991 (BSI-Errichtungsgesetz). Vorgänger: "Zentralstelle für das Chiffrierwesen" als Teil des Bundesnachrichtendienstes. Heute im BMI unabhängige und neutrale Bundesoberbehörde.

Ziele des BSI („ITGS-Owner“): Sicherer Einsatz von Informations- und Kommunikationstechnik im Bund, in der Wirtschaft und in der Gesellschaft.
Aufgaben:
- **Entwicklung von IT-Sicherheitsstandards**,
- die Beratung und Zertifizierung,
- die Warnung vor Sicherheitslücken sowie
- der **Schutz der IT-Systeme des Bundes**.

Zweck des ITGS
Der Zweck des IT-Grundschutz besteht darin, Organisationen dabei zu unterstützen, ein angemessenes und **nachvollziehbares Sicherheitsniveau** für ihre Informationstechnik zu erreichen.
Der IT-Grundschutz verfolgt den Zweck, die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Daten sicherzustellen und IT-Systeme **vor typischen Bedrohungen** wie Cyberangriffen und Datenverlusten zu schützen.

Quellen:
https://www.bsi.bund.de/DE/Das-BSI/Zeitstrahl/BSI-Zeitstrahl_node.html
https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Kurzprofil/kurzprofil_node.html
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/ISO-27001-Basis-IT-Grundschutz/iso-27001-basis-it-grundschutz_node.html

ITGS Meilensteine

1992: IT-Sicherheitshandbuch
1994: Einrichtung des ersten CERT im BSI.
"In Kooperation mit führenden Wirtschaftsunternehmen konzipiert und veröffentlicht das BSI das **IT-Grundschutzhandbuch**." (1994: 18 Bausteine, 200 Maßnahmen)
1998: Erste Version des **ITGS-Tools** (für öffentl. Einrichtungen kostenlos, Support bis 2016, danach Tools externer Anbieter)
2006: ITGS mit **ISO/IEC 27001:2005** kompatibel
2017: **Modernisierung** der IT-Grundschutz-Methodik (u.a. Verbesserung der Skalierbarkeit), neue ITGS-Tools
2019: **Schnittstelle ITGS <-> operativer Datenschutz**: CON.2-Baustein
2023: **Grundschutzkompendium** (Umfang: ca. 1100 Seiten)
(2025: 113 Bausteine zu 10 Themenbereichen)

Quellen:
https://www.bsi.bund.de/DE/Das-BSI/Zeitstrahl/BSI-Zeitstrahl_node.html
https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Kurzprofil/kurzprofil_node.html
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/ISO-27001-Basis-IT-Grundschutz/iso-27001-basis-it-grundschutz_node.html

Standing beider Methoden

Anwendung SDM in Deutschland

Schätzung: **wenige 10.000** (bei schätzungsweise 4 Mio. formalen Organisationen)(*1)
In der Privatwirtschaft und bei kleineren Organisationen wird das SDM überwiegend wohl als Orientierungshilfe oder es werden Teilaspekte selektiv angewandt.(*2)

Wenn DSGVO zunehmend weniger beachtet und durchgesetzt wird(*3), wird sich auch die Anwendung des SDM zumindest quantitativ eher verschlechtern. Das SDM ist bislang keine wirklich in der Breite praktizierte Methode, etwa Faktor 20 mal geringer genutzt als der ITGS.

Anwendung ITGS in Deutschland

Schätzung: **250.000-280.000** meist größere Unternehmen, Behörden und kritische Infrastrukturen(*4)
Nur ein kleiner Teil der Organisationen richtet sein *gesamtes* Informationssicherheits-management systematisch nach ITGS aus(*5).

ITGS ist anerkannt, NIS/NIS2 und der CR-Act werden diese Anerkennung bzw. Anwendung absehbar weiter verbessern.

Quellen:
*1. perplexity.ai, Prompt: „Soziologie, Wie viele Organisationen gibt es schätzungsweise in Deutschland?“ (2025-0825)
*2. ULD 2022: Umfragen zur Nutzung des SDM: https://www.datenschutzzentrum.de/uploads/sommerakademie/2022/SAK2022_IB05_SDM.pdf
*3. heute journal vom 12.08.2025, 21:45 Uhr: Interview mit Max Schrems
*4. https://www.eco.de/presse/cybersicherheit-nur-wenige-unternehmen-in-deutschland-sind-auf-nis2-vorbereitet/
*5. https://www.tenfold-security.com/bsi-it-grundschutz/

SDM und ITGS
Gemeinsamkeiten

- definiertes **Schutzobjekt** (nur: welches?)
- Normen- und **Regel-Verankerung** (nur: wie verbindlich?)
- systematisches Vorgehen, dafür zentral:
  Bestimmung von Standard-Maßnahmen aus einem vorgegebenen Set an Schutzzielen
- risikobasiert mit **Risikostufen und Schutzbedarfsabstufungen**, ermöglicht Skalierung von Schutzmaßnahmen (nur: wie genau?)
- **Maßnahmenkataloge** (Bausteine) für Standard-Lösungen
- kontinuierliche Verbesserung durch Management

SDM und ITGS

Unterschiede: Objekt, Regelwerk

	SDM	**ITGS**
Schutzobjekt	Personen auch: Sozialstruktur (mit Gewaltenteilung, Markt, freien Diskursen, Demokratie), die „Personen“ erzeugt.	Organisation
materielles Gestaltungsobjekt	die einzelne ***„Verarbeitung“*** mit den jeweils genutzten Prozessen und Betriebsmitteln	Informationssicherheits-Management-system, steuert den ***„Informationsverbund“*** mit den organisationsweiten Betriebsmitteln: *Geschäftsprozesse*, IT, Netzwerke, Daten, Infrastruktur
Normen- und Regelwerke	DSGVO, BDSG, LDSG, Spezial-Gesetze -> „*Gewährleistungsziele*“	BSI-G, NIS/2, CR-Act, Policies, ISO- und eigene Standards, „*Schutzziele“,* zentral: Selbstverpfichtungen der Leitungen

Unterschiede: Risikomodellierung, Risikobeurteilung

	SDM	**ITGS**
Risiko / Schutzbedarf / Gefährdung	Beziehen sich auf die von einer Verarbeitung durch die Organisation betroffenen **Person**.	Beziehen sich auf die „Prozesse“ (Geschäftsprozess, Verfahren) und den Wert von Informationen für die **Organisation**.
Hauptangreifer	Die **verarbeitende Organisation**, die Personen (Bürger*innen, Kund*innen) qua Verarbeitung beherrschen könnte, weil sie die DSGVO-Anforderungen an Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit und Nichtverkettung nicht auf einem angemessenen Niveau beachtet.	Interne Mitarbeiter* innen, externe Organisationen, Hacking, **Dritte**, durch unbefugte, illegale Zugriffe Welcher Schaden könnte für die Organisation entstehen, wenn die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit für ein konkretes Objekt (z.B. Information, Anwendung, System) innerhalb der Organisation verletzt werden?
Strategie der Risiko-Beurteilung	„Schwellwertanalyse der Verarbeitung“, Art. 35 DSGVO	Gefährdungsanalyse BM, Abschätzen von Time, Budget, Know-how ext. / int. Angreifer

SDM und ITGS

Verbindung von Norm und Maßnahme

	SDM	**ITGS**
Bestimmung Standard-maßnahmen	für jedes Gewährleistungsziel ausgewiesen im generischen **Maßnahmenkatalog** und den **Bausteinen**	für jedes Schutzziel ausgewiesen im **Grundschutzkompendium**
Skalierbarkeit der einzelnen Maßnahmen	**Keine Abstufung pro Schutzziel**, es gelten immer alle „Grundsätze“ (Art 5 DSGVO) bzw. „Gewährleistungsziele“; die Bestimmung der Maßnahme ergibt sich aus der Risikostufe der Verarbeitung, nicht aus der Gefährdungsanalyse bspw. der Betriebsmittel.	Das Maß des Risikos bemisst sich entlang der Gefährdungsanalyse pro Schutzziel, deshalb kann bspw. die Einstufung pro Sicherung der Verfügbarkeit und Integrität „normal“, Sicherung der Vertraulichkeit „hoch“ sein, mit entsprechender **Abstufung der Wirkung** von Schutzmaßnahmen.
relative Vollständig-keit des Katalogs	**nein**, verweist bei Kryptomaßn. auf Maßnahmen des ITGS	**ja**

Unterschied: Risikoskala, Skalierbarkeit von Maßnahmen

	SDM	**ITGS**
Einstufung für Maßnahmen-skalierung	Schwellwertanalyse zur **Beurteilung der Grundrechtseingriffintensität** einer Verarbeitung (DSFA?)	Risikoanalyse anhand Szenarien zur **Bewertung von Schäden** Gesetzesverstöße, Beeinträchtigung der persönlichen Unversehrtheit, Aufgabenerfüllung, Innen- oder Außenwirkung und finanzielle Auswirkungen.
Übergang von „normal“ zu „hoch“ (SDM: „Risiko“ ITGS: „Schutzbedarf“)	Selbstanwendung der gesetzlich gleichbleibend geforderten Maßnahmen, gesteigert wirk-same Maßnahmen durch **Selbst-anwendung der Maßnahmen auf sich selber** (Bsp: permanent kontrolliert zweckgebundene, redundante, verschlüsselte, gehashte, löschbare Protokolldaten) (keine Risikostufe für „sehr hohes Risiko“)	Differenzierung der Anforderungen nach Schutzzielen, dann weitergehende, „**strengere Maßnahmen**“ für die relevanten Schutzziele, zusätzlich: Maximalprinzip, Kumulation Bei Schutzbedarf „sehr hoch“ mit „Gefahr für Leib und Leben“ wird viel „selber Nachdenken“ verlangt

Reifegrade SDM- und ITGS-Nutzung

Reifegrad	SDM-Nutzung	ITGS-Nutzung
0	kein operativer Datenschutz, aber DSB	keine Informationssicherheit, oft sensible Admins
1	**vereinzelte Maßnahmen**, „die ein Admin so kennt“ (typ: GP, Berechtigungskonzept, Löschen, Verschlüsselung), „Papierlage“, VVZ, einzelne Betroffenrechte, konzeptlos	**vereinzelte Maßnahmen**, „die man als Admin so kennt“ (typ: Dokumentation, Verschlüsselung (vpn), Protokollierung, Hashen), alles konzeptlos und ohne Qualitätsmaßstab, IT-GS aber bekannt
2	Regel-Normen-Bezug von Maßnahmen verstanden, Betroffenenrechte, DSFA, **Methodiksuche**: ITGS / ISO / SDM	ITSiBe, Bezug zwischen Regel-Normen-Katalog und Maßnahmen, starten **Methodikbefassung** ITGS / ISO (typische Idee: operatDS wird mit „erledigt“)
3	ITGS befassen, ins SDM reinschnuppern, **SDM ≈ ITGS** (Toolentw./-suche f. DS beginnt)	ITGS-Tool nutzen, systematisch zumindest auf ISO-/**ITGS-Orientierung abstellen**, ITSiBe
4	SDM-Orientierung, SDM-Schulung, SDM-Toolunterstützung, **Schnittstelle zu ITGS**	**Schnittstellen: ITIL, CoBIt, DSGVO, SDM,** neuerdings: NIS2, CRA, DA, KI, ... Aufbau ISMS
5	**Aufbau DS-Abteilung in Organisation, steuerndes Datenschutzmanagement** auf SDM-Basis, Schulungen operativer DS	**Etabliert: ISMS**, ITSiBe, Team, permanente Schulungen (gerade zu neuen Themen)
6	externe Auditierung, **DAKS-Zertifizierung**	**BSI-Zertifizierung**

CON.2.A1 Umsetzung Standard-Datenschutzmodell (2023)

"Die gesetzlichen Bestimmungen zum Datenschutz (DSGVO, BDSG, die Datenschutzgesetze der Bundesländer und gegebenenfalls einschlägige bereichsspezifische Datenschutzregelungen) MÜSSEN eingehalten werden. Wird die SDM-Methodik nicht berücksichtigt, die Maßnahmen also nicht auf der Basis der Gewährleistungsziele systematisiert und mit dem Referenzmaßnahmen-Katalog des SDM abgeglichen, SOLLTE dies begründet und dokumentiert werden." (S. 5)

CON.2.A1 Umsetzung Standard-Datenschutzmodell (2023)

"Eine weitere **Gefahr für Personen bzw. Beschäftigte ist ein falsch angesetzter Schutzbedarf** ihrer personenbezogenen Daten. Dieser Schutzbedarf, der typischerweise durch die Institution, die verantwortlich personenbezogene Daten verarbeitet, selbst festgelegt wird, kann aus verschiedenen Gründen falsch oder zu niedrig angesetzt sein:“

- Die Institution hat den gegenüber der Informationssicherheit *erweiterten Schutzzielkatalog des Datenschutzes* nicht berücksichtigt.

- Die Institution hat bei der Schutzbedarfsermittlung nicht zwischen den *Risiken für die Umsetzung der Grundrechte der Betroffenen* und den Risiken für die Institution unterschieden.

- Die Institution hat zwar die beiden Schutzinteressen unterschieden, aber die Funktionen der Verarbeitung und der Schutzmaßnahmen *zugunsten der Institution bzw. zugunsten betroffener Personen* gestaltet."

Risiko-Typen: ITGS (CON.2) und SDM (wortgleich)

- Typ A: Der *Grundrechtseingriff* bei natürlichen Personen durch die Verarbeitung ist **nicht hinreichend milde** gestaltet.

- Typ B: Die Maßnahmen zur *Verringerung der Eingriffsintensität* einer Verarbeitung sind mit Bezug auf die Gewährleistungszielen **nicht vollständig oder werden nicht hinreichend wirksam betrieben** oder nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.

- Typ C: Die Maßnahmen, die nach der *Informationssicherheit* geboten sind (z.B. IT-Grundschutz nach BSI), sind **nicht vollständig oder werden nicht hinreichend wirksam betrieben** oder werden nicht in einem ausreichenden Maße stetig kontrolliert, geprüft und beurteilt.

- Typ D: Die Maßnahme der **Informationssicherheit werden nicht ausreichend datenschutzgerecht**, im Sinne des Risikotyps A und Risikotyps B, betrieben.

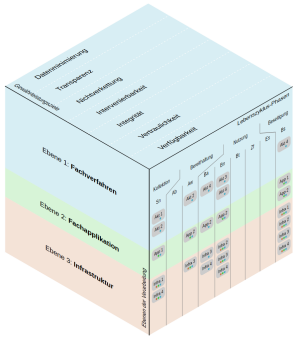
Quellen:
- BSI 2023: IT-Grundschutz-Bausteine, Edition 2023, CON.2 Datenschutz, S. 142
- DSK 2025: SDM V3.1a, S. 51

Reichweite von Planung/Implementation von Maßnahmen

SDM

Geltungs-bereich

0.a Rechtliche Analyse anhand der Verfahrensdokumentation
0.b Schwellwertanalyse, Feststellung der Grundrechtsrisiken für Personen



1. Strukturanalyse einer Verarbeitung am SDM-Würfel
2. Zuordnung von Standard-Maßnahmen/ Bausteinen zu Phasen und Ebenen und Betriebsmitteln
3. Soll-Ist-Vergleich, Analyse der Risiken (ggfs. DSFA Art. 35 als Projekt umgesetzt)
4. *Planung Implementation v. Maß.*
5. *Rechtliche Beurteilung*
6. *Umsetzung der Maßnahmen*
7. *Kontinuierliche Verbesserung im Rahmen des DS-Managements*

Verantwortlichkeit und Controlling (DSB) sind geregelt, aber: Wer macht es, die Abteilungsleitung oder DS-Abteilung?

ITGS (BSI-Standard 200-2)

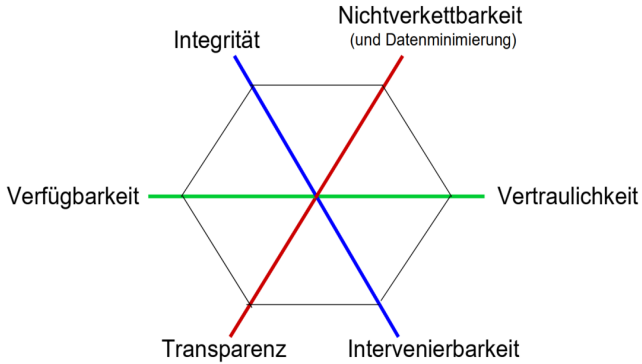
Geltungs-bereich

0. Rechtliche Analyse

1. Strukturanalyse der Organisation
2. Schutzbedarfsfeststellung
3. Modellierung nach ITGS, Gefährdungsanalyse
4. Bausteine des IT-Grundschutz-Kompendiums auf die zu schützenden Objekte matchen
5. Soll-Ist-Vergleich („Grundschutz-Check“)
6. Planung der Maßnahmen (Priorisierung, Budgetierung, Zuständigkeiten, Fristen)
7. Behandlung besonderer Risiken
8. Kontinuierliche Verbesserung

Methodik-Unterschied: Abstimmung der Maßnahmen untereinander

SDM, Risiko der Verarbeitung: Bsp. „hoch“



ITGS, Beispiel für Ergebnis des Schutzbedarfs nach einer Gefährdungs-/ Risikoanalyse:
- Verfügbarkeit: normal
- Integrität: sehr hoch
- Vertraulichkeit: sehr hoch

- Verfügbarkeit
- Integrität
- Vertraulichkeit

- Verfügbarkeit
- Integrität
- Vertraulichkeit

- Verfügbarkeit
- Integrität
- Vertraulichkeit

→ Maßnahmen f. normal
→ Maßnahmen f. hoch
→ Maßnahmen f. hoch

Verwaltung

1. Integrität
2. Nichtverkettung
3. Vertraulichkeit
4. Verfügbarkeit
5. Transparenz
6. Intervenierbarkeit

Unternehmen

1. Verfügbarkeit
2. Nichtverkettung
3. Intervenierbarkeit
4. Integrität
5. Transparenz
6. Vertraulichkeit

Forschungs-Inst.

1. Transparenz
2. Intervenierbarkeit
3. Verfügbarkeit
4. Vertraulichkeit
5. Integrität
6. Nichtverkettung

Alle Maßnahmen entweder „normal“ oder „hoch“
(Aber: Abstimmung der Maßnahmen untereinander in verschiedenen Organisationstypen unterschiedlich)

Quelle: Rost, Martin, 2024: Das Standard-Datenschutzmodell (SDM) - Einführung in die Umsetzung der operativen Anforderungen der DSGVO Springer-Vieweg, 2. Aufl.

Konflikte zwischen IT-GS und SDM, die gut regelbar sind: Bsp. Backup

IT-Sicherheit: Backups für den Notfall auch langfristig behalten, um einen Systemausfall abfangen zu können.

Datenschutz: personenbezogene Daten müssen, auf Anfrage des Betroffenen bzw. nach Ablauf des Erforderlichkeit des Verarbeitens, gelöscht werden.

Gute Praxis: Backup so einrichten – im Zweifel durch Umkopieren -, dass zu löschende personenbezogene Daten auch gelöscht werden können. Das kann hohen Aufwand (mit hohen Kosten) erzeugen, ist aber machbar selbst mit Backup-Medien, die nur einmal beschreibbar sind.

Konflikte zwischen IT-GS und SDM, die gut regelbar sind: Bsp. Protokollierung

IT-Sicherheit: Je mehr Informationen und je länger gespeichert, desto besser für Angriffserkennung, Risikoanalyse und Wiederherstellbarkeit.

Datenschutz 1: Eine zu lange oder zu umfangreiche Speicherung kann gegen die DSGVO verstoßen. Personenbezogene Protokolle dürfen nur so lange und in dem Umfang gespeichert werden, wie es zur Erfüllung des jeweiligen Zwecks notwendig ist, z.B. auch für die Fehlererkennung oder die Abwehr von Bedrohungen.

Datenschutz 2: Operativer Datenschutz ist ebenfalls auf hochauflösende Informationen angewiesen, um der Organisation anhand fehlender oder falscher (z.B. Konfigurationen von) Schutzmaßnahmen nachweisen zu können, wenn sie nicht DSGVO-konform gearbeitet hat: Protokolldaten können Personen auch entlasten.

Gute Praxis: *Protokollierung als eigene Verarbeitung* einrichten (also: mit eigener Rechtsgrundlage, Schwellwertanalyse/DSFA, Umsetzung Betroffenenrechte (Beschäftigten-Datenschutz!)), mit allen Stakeholdern am Tisch.

Konflikte zwischen IT-GS und SDM, die gut regelbar sind: Bsp. Verschlüsselung/ Nichtverkettung

IT-Sicherheit: Nur die Kommunikationspartner sollen Zugriff auf die Inhalte haben. Ein Dienstanbieter oder Dritte können weder mitlesen noch die Daten entschlüsseln.

Datenschutz 1: Ein Dienstanbieter oder Dritte können weder mitlesen noch die Daten entschlüsseln.

Datenschutz 2: Zugriff auf die Inhalte hat aber... die Organisation, der Verantwortliche. Die Maßnahme „Verschlüsselung“ schützt nicht vor einer nicht-rechtmäßigen Verarbeitung durch die Organisation selber, die Vollzugriff hat.

Gute Praxis:
Externe Zugriffe auf Daten, Kommunikationsverbindungen, IT-Systeme bzw. Verarbeitungen durch *Verschlüsseln* verhindern.
Interne Zugriffe durch Einziehen von *Trennungen* (von Datenbeständen, IT-Systemen, Verarbeitungen durch Rollen- & Rechtekonzept) wirksam unter Bedingungen stellen und wirksam (= mit Fehlerkorrektur) kontrollieren.

Praxis
Kompromisse

- Die Berücksichtigung der Informationssicherheit durch den operativen Datenschutz setzt voraus, dass die **unterschiedlichen Grade** der Geltung der rechtlichen Regelungen (SDM: Grundrechte, ITGS: Einfachgesetze, Selbstverpflichtung) sowie der Zwecke (Schutz Personen, Schutz Organisationen) der dafür eingesetzten Methoden bekannt und anerkannt sind, weil diese Unterschiede in nennenswert vielen praxisrelevanten Fällen zu nennenswerten harten Konflikten führen können. **(Operativer) Datenschutz führt in der Regel rechtlich vor Informationssicherheit.** Faktisch führt jedoch methodisch Informationssicherheit, weil reifer und vor allem: im Interesse der Organisationen liegend.
- Beim Design von Infrastruktur und organisationsweit genutzten Betriebsmitteln **tritt Datenschutz/SDM etwas gegenüber Informations-Sicherheit/ITGS zurück**. Datenschutz fokussiert stattdessen bevorzugt die konkrete Verarbeitung, das heißt, ein zweckbestimmtes Verfahren, einen Geschäftsprozess oder ein Forschungsprojekt.
- DSGVO <–> NIS2 / CR-Act / AI-Act / Data-Act ... ist alles noch zu klären.

Zusammenfassung

- SDM greift die **Zuordnung von Standard-Maßnahmen** (gemäß „Stand der Technik“) zu **Schutzzielen** des ITGS auf.

- SDM greift auf die „Krypto-Maßnahmen“ aus dem IT-Grundschutz-Kompendium zurück.
  Aktuell aber nur mangels eigener Ressourcen; mahnend, dass die Schutzobjekte beider Methoden nicht übereinstimmen!

- Die Bestimmung der Konfigurationsanforderungen von Risiken-mindernden Schutzmaßnahmen ist im SDM insofern einfacher als bei ITGS, als dass bereits **aus der Risikoeinstufung der Verarbeitung qua Schwellwertanalyse die Anforderungen** an die Wirksamkeit der Betriebsmittel (BM) und Schutzmaßnahmen folgen.
  - SDM: Wenn BM Anforderungen nicht erfüllt, darf BM nicht genutzt werden.
  - ITGS: Genutzt werden darf, was funktioniert, es muss nur sicher betrieben werden können. Der Einsatz des BM bzw. von Schutzmaßnahmen muss rechtskonform erfolgen, wobei Rechtskonformität in Praxis erfahrungsgemäß zweitrangig ist.

- Eine allseits akzeptable Lösung zu finden, ist erfahrungsgemäß möglich.
  Voraussetzung 1: Die IT-Sicherheit agiert nicht bedingungslos, sondern systematisch/ methodisch, bspw. nach ITGS.
  Voraussetzung 2: Datenschutz weiß, wie normative Bedingungen technisch umsetzbar sind, bspw. systematisch/methodisch nach SDM.

Fazit

- Operativer Datenschutz würde ohne Informationssicherheit nicht funktionieren, setzt eine „informationssichere“ Organisation voraus, die zugleich der stärkste Angreifer auf Personen und deren Selbstbestimmung ist. Logische Folge für die Praxis: **starke Konflikte innerhalb der Organisation**, die typisch zu Lasten des Datenschutzes vermieden werden. *Deshalb ist „SDM = ITGS plus“ attraktiv.*
- Sowohl die Ziele und Zwecke als auch die Methodik unterscheiden sich in einem Maße, **dass SDM und ITGS je für sich bzw. unabhängig voneinander angewendet werden müssen. Daraus folgt, dass sie zueinander Schnittstellen bereitstellen sollten** (das BSI mit ITGS/CON.2 weiß und respektiert das).
- Wenn ITGS den in der Regel geltenden normativen Primat des Datenschutzes anerkennt, findet sich in der Regel eine praxistaugliche Lösung. **Es finden sich nur dann keine DSGVO-konforme Lösungen, wenn Organisationen mit ihren Verarbeitungen zu viele und besonders sensible Daten nur im eigenen Interesse verarbeiten und Datenschutz dabei als Teil- oder Untermenge der Informationssicherheit untergepflügt wird.**

Vielen Dank für Ihre Aufmerksamkeit!

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein
Martin Rost
Telefon: 0431 988 – 1391
uld32@datenschutzzentrum.de
https://www.datenschutzzentrum.de/