Information zum (Weblink)
Datenschutz - Service
oder Fragen per Mail an:
Mail2@volkerschroer.de

Das Standard – Datenschutz - Modell

der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) [1]

Quelle: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Datenschutzkonferenz (Link: Fußzeile)

Das Standard-Datenschutzmodell (SDM) ist eine Vorgehensweise, mit der die rechtlichen Anforderungen aus der Datenschutzgrundverordnung (DSGVO) in konkrete technische und organisatorische Maßnahmen übersetzt werden können. Es unterstützt damit die Transformation abstrakter rechtlicher Anforderungen in konkrete technische und organisatorische Maßnahmen. Damit unterstützt das SDM Verantwortliche in Wirtschaft und Verwaltung und ist eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele" (Zitate: BfDI und aus dem SDM)

Sie wollen es kurz und direkt? Sprechen wir!

Das Inhaltsverzeichnis ist mit Text – Links unterlegt. Mit einem Klick können Sie das entsprechende Thema direkt aufrufen. Lesen Sie nur, die für Sie interessanten Themenkomplexe. Vielen Dank für Ihr Interesse.

Inhaltsverzeichnis

(Einfach Thema nach Wahl anklicken)

1. Einleitung:....2
(a) Zusammenfasung in 4 Sätzen....2
(b) Die Beteiligten....2
(c) Die Ausnahmen....2
2. Status & Ziele des SDM....3
i) Ziel....3
ii) Zweck....3
iii) Die 7 Gewährleistungsziele....3
3. Anforderungen der DS-GVO....3
(a) Systematisierung durch Gewährleistungsziele und deren praktische Umsetzung (generische Maßnahmen)....4
i) Datenminimierung....4
ii) Verfügbarkeit....4
iii) Integrität....4
iv) Vertraulichkeit....5
v) Nichtverkettung....5
vi) Transparenz....5
vii) Intervenierbarkeit....6
(b) Gewährleistungsziele als Design - Strategie 6
(c) Verarbeitungstätigkeiten....6
i) Ebenen....6
ii) Zweck....6
iii) Komponenten....7
4. Risiken und Schutzbedarf....7
(a) Risiko für Betroffene....7
(b) Risikobetrachtung....7
i) Schwellenwert – Analysefunktionen....7
ii) Risikoidentifikation....8
iii) Risikobewertung....8
(c) Risikobewertung aus Schutzbedarf & Schutzniveau....8
(d) „TOM", insbesondere bei hohem Risiko....8
5. Datenschutzmanagement mit dem SDM....9
(a) Rechtliche Grundlagen....9
(b) Vorbereitungen....9
(c) Spezifizieren und prüfen....10
(d) Prozess....10
6. Organisatorische Rahmenbedingungen....10

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtig- und Vollständigkeit übernehmen kann. Aus Gründen der besseren Lesbarkeit Verwendung der männliche Form, die alle Geschlechter mit einbezieht.

1 Quelle: BSI Das Standard-Datenschutzmodell https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/SDM.html

1. Einleitung:

(a) Zusammenfasung in 4 Sätzen

1.) **Ist der Kunde vollumfänglich und leicht verständlich über Art, Zweck, Dauer und Verarbeitung seiner erhobenen Daten informiert und hat genau dazu sein Einverständnis gegeben?**

2.) **Kann einer Aufforderung zum Nachweis, zur Auskunft, Berichtigung, Löschung, Vergessen, Übertragung sowie Widerspruch jederzeit und fristgerecht nachgekommen werden?**

3.) **Kann Vertraulichkeit je nach Sensibilität, Integrität und Verfügbarkeit der erhobenen Daten jederzeit gewährleistet werden?**

4.) **Zur Erfüllung der Nachweispflicht ist alles einmal festzuhalten, ob Digital oder auf Papier (Nachweispflicht).** *(Link zu: „Einfachem Muster mit Erläuterungen)*

(b) Die Beteiligten

Verantwortliche sind/ist die natürlichen oder juristischen Person, die allein oder gemeinsam über Zweck und Mittel der Verarbeitung entscheidet (Art.4 Nr.7 DS-GVO). Ein Vertreter ist schriftlich zu bestellen (Art.4 Nr. 17 DS-GVO). Risiken und Haftung tragen ausschließlich die Verantwortlichen mit der Entscheidung.

Gemeinsam Verantwortliche legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche (Art.26 DS-GVO). Ein Beispiel ist die Facebook (Meta) Fanpage (EuGH Nr. 81/18 v. 05.06.2018)[2].

Auftragsverarbeiter sind/ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten nur im Auftrag des Verantwortlichen verarbeitet, ohne Verbindung zu Betroffenen (Art.4 Nr. 8 DS-GVO) und ist nur für diese Verarbeitung der Verantwortlicher (Art 28 Abs.10 DS-GVO).

Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt (Art.37 Abs.5 DS-GVO). Seine Aufgaben umfassen (nur) Unterrichtung und Beratung, Überwachung und Einhaltung, Beratung zu Folgenabschätzungen, Zusammenarbeit und Ansprechpartner für die Aufsichtsbehörden und Anlaufstelle für Betroffene. (Art. 39 Abs.1 DS-GVO) .

Weitere Beteiligte Art.4 DS-GVO (Nr.) Vertreter (17), Betroffene, Empfänger (9), Dritte (10), Drittland (ex EU), internationale Organisation (26)

(c) Die Ausnahmen

„***Haushaltsausnahme“:*** Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogenen Daten (c) durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (Art.2 Abs.2 lit.c DS-GVO).

„Datenschutzbeauftragter“: Keine Bestellpflicht, wenn weniger als 20 Personen mit der Verarbeitung beschäftigt **UND** keine geschäftsmäßige Datenübermittlung oder zu Markt- und Meinungsforschung **UND** kein hohes Risiko (§38 Abs.1 BDSG)

„Verzeichnis der Verarbeitungstätigkeiten“: Verzicht auf ein VVT für Kleinstunternehmen und Unternehmer **WENN** weniger als 250 MA **UND** … keine besondere Daten (-kategorien) **UND** keine hohes Risiko (keine DS-FA) **UND** nur gelegentlich. (Art.30 Abs.5 DS-GVO) Dazu die *Aufsichtsbehörden:“ Wird selten vorkommen!*“.[3]

2 Quelle: *EuGH Nr. 81/18 vom 05.06.2018 Facebook-Fanpage* & Art. 26 DS-GVO
3 Quelle: *DSK Hinweise zum Verzeichnis von Verarbeitungstätigkeiten na Art.30 DS-GVO*

2. Status & Ziele des SDM

Ausgang ist das SDM in der Version 2.0b vom 17.04.2022 / Letzte Ergänzung: 27.10.2021.

i) Ziel

„Ziel ist die Überführung der rechtlichen Anforderungen (Gewährleistungsziele der DS-GVO) zu den technischen und organisatorischen Maßnahmen in einen detaillierten Referenzmaßnahmenkatalog für den praktischen, täglichen Gebrauch des Verantwortlichen mit der Möglichkeit eines systematischen, nachvollziehbaren SOLL | IST Vergleichs“ (Prüfungskriterien!).“

ii) Zweck

Das SDM dient ausschließlich einer datenschutzrechtlich konformen Gestaltung von Verarbeitungstätigkeiten nach dem Datenschutzrecht (Transformationshilfe: Recht zu Praxis) und einer Anwendungsstruktur mit systematisierender, rollierender (Vor-) Planung, Einführung, Betrieb.

iii) Die 7 Gewährleistungsziele

von „elementarer Bedeutung“, für die Betroffenenrechte

1.) Verfügbarkeit 3.) Datenminimierung 5.) Nichtverkettung 7.) Intervenierbarkeit
2.) Integrität 4.) Vertraulichkeit 6.) Transparenz

Erfolg basiert auf Vertrauen und Vertrauen basiert auf Ihrem Datenschutz

(45% der Kunden kündigen bei Misstrauen nach dem Okta Digital Trust Index: Einzelhandel/Firmen)[4]

Datenschutz einfach praktisch hilfreich,

(w*enn die Grundlagen einmal gelegt, sind die Abläufe meist verschlankt und der Aufwand gering)*

Mit einem kontinuierlichen Datenschutzmanagement, einem rollierenden, systematischen Plan, vermeiden Sie Risiken, schonen Kosten, Liquidität, vermeiden Ärgernisse und i. d. R. verschlanken sich Abläufe bzw. Prozesse. Die richtige Dokumentation dazu ist weniger Aufwand, als es auf den ersten Blick erscheint – wenn man es macht.

3. Anforderungen der DS-GVO

Eine Aufzählung der gesetzlichen Anforderungen, nebst rechtlicher Ableitungen in einer Übersicht :

Transparenz[1]	Zweckbindung[2]	Datenminimierung[3]
Speicherbegrenzung[3]	Integriät[4]	Richtigkeit
Vertraulichkeit	Berichtigungsmöglichkeit	Löschbarkeit
Rechenschaftspflicht / Nachweisfähigkeit	Identifizierung / Authentifizierung [5]	Unterstützung der Betroffenen bei der Ausübung der Rechte
Eingeschränkte Verarbeitung	Übertragbarkeit	Datenschutz-Voreinstellungen[6]
Eingriffsmöglichkeit bei automatisierter Entscheidung	Profiling: Fehler- und Diskriminierungsfreiheit	Behebung und Abmilderung von Schutzverletzungen
System - Verfügbarkeit	Belastbarkeit (Ausfallsicherheit)	Wiederherstellbarkeit
Evaluierbarkeit (Überprüfungen)	Angemessene Überwachung der Verarbeitung	
Einwilligungsmanagement[7]	Umsetzung aufsichtsbehördlicher Anordnungen	

[1])Spätestens nach einem Monat muss der Betroffene „so oder so“ über eine Verarbeitung informiert sein
[2])Angemessen = Zweck; Erheblich = notwendig zur Zweckerreichung; Beschränkt = kein „nice-to-have“ oder für „später“
[3])Speicherung nur das und solange es für den Zweck unbedingt erforderlich ist (Löschungspflicht! Auch Teile vorab)
[4]) Schutz vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung („TOM“)
[5])der Verantwortliche eine Vorgehensweise zur Authentifizierung von Personen, die die Betroffenenrechte geltend machen, festlegen und umsetzen muss.
[6])Minimale Voreinstellung von Einwilligungen, möglichst „optionale“ Erweiterungen (data protection by default)
[7])Konkrete, klare, eindeutige und umfassende Vorabinformation, gleiches zur Einwilligung / Zustimmung

Im SDM erfolgt nun eine konkrete, praktische Sicht der Aufsicht (wo möglich) nach

Systematisierung | Rechtsgrundlagen | Praktischer Ansatz

4 *Quelle: Oka Digital Trust Index 2020 für Einzelhandel und bei Firmen*

(a) Systematisierung durch Gewährleistungsziele und deren praktische Umsetzung (generische Maßnahmen)

Entgegen der Agenda im SDM habe ich die Systematisierung (rechtlicher Ansatz) und die generischen Maßnahmen (praktische Umsetzung) unter den 7 Gewährleistungszielen jeweils zusammengeführt. Wegen der allgemeinen Gültigkeit ist sicherlich eine sinnvolle Ausprägung der Maßnahmen je nach Verarbeitung, Größe, Umfang und Art der Daten zu berücksichtigen. Zitat:

> *„In der datenschutzrechtlichen Beurteilung müssen Juristen und Informatiker deshalb eine gemeinsame Sprache finden, um sicherzugehen, dass diese rechtlichen Anforderungen auch tatsächlich technisch und organisatorisch umgesetzt werden. Generische Maßnahmen werden sie durch die Gewährleistungsziele unterstützten. Anführung von typischen, technischen und organisatorischen Referenzmaßnahmen die in der Datenschutzpraxis vieler Datenschutzaufsichtsbehörden seit vielen Jahren erprobt sind.“*
> [… angemessen und praktikabel fände ich noch gut]

i) Datenminimierung

Systematisierung: Das Minimierungsgebot erstreckt sich nicht nur auf die Menge der verarbeiteten Daten, sondern auch auf den Umfang der Verarbeitungen, die Speicherfristen und die Zugänglichkeit (je weniger und desto kürzer, um so besser).

Rechtlichen Anforderungen: ergeben sich aus Art.5 Abs.1 lit.c (Minimierung); Art.5 Abs.1 lit.e (Begrenzung); Art.25 Abs.2 (datenschutzfreundliche Voreinstellung) DS-GVO.

Praktisch: Reduzierung um alle nicht mehr notwendigen Daten, wie einzelne Attribute, Verarbeitungsoptionen, Datenisolierung, Pseudonymisierung, Anonymisierung, nicht notwendige Datenmasken, Löschkonzept u.ä.

ii) Verfügbarkeit

Systematisierung: Unverzüglicher Zugriff auf und Auffindbarkeit der (personenbezogenen) Daten und der Verarbeitung im ordnungsgemäß vorgesehenen Prozess, einschließlich einer angemessenen, gut verständlichen Darstellung für die Person (Datenmanagement – Systeme, Datenbanken, Suchfunktionen). Ein Schutz und zügiger Zugriff auch bei physischen oder technischen Zwischenfällen und bei hoher Systemlast. Bei Ausnahme eines Störfalles sind und werden Maßnahmen zur Behebung getroffen.

Rechtliche Anforderungen: Art.5 Abs.1 lit.c (Minimierung); Art.5 Abs.1 lit.e (Begrenzung); Art.25 Abs.2 (datenschutzfreundliche Voreinstellung) DS-GVO

Praktisch: Sicherungskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien gemäß eines getesteten Konzeptes.

iii) Integrität

Systematisierung: Sicherstellung der technischen Prozesse und Systeme in Bezug auf die kontinuierliche Einhaltung der festgelegten Spezifikationen, sowie der Erhalt der Vollständigkeit, Richtigkeit, Unversehrtheit und Aktualität der Daten. Angemessene und regelmäßige Überwachung der Einhaltung, um Abweichungen festzustellen und anzupassen, wo es erforderlich ist. Neben der Fehlerfreiheit ist die Diskriminierungsfreiheit bei automatisierten Bewertungs- und Entscheidungsprozessen IM VORFELD zu prüfen, festzulegen und im Prozess sicher zu stellen.

Rechtliche Anforderungen: Art.5 Abs.1 lit.d, f, Art.32 Abs.1 lit.b (Integrität); Art.22 Abs.3,4 in Verbindung mit ErwGr.71 (Profiling, Fehler-, Diskriminierungsfreiheit); Art.32 Abs.1 lit.b (Belastbarkeit); Art.33 Abs.3 lit.d, Art.34 Abs.2 (Behebung und Abmilderung von Datenschutzverletzungen); Art.32, 33, 34 (Angemessene Überwachung der Verarbeitung) DS-GVO

Praktisch: Enge Eingrenzung von Lese- und Schreibrechten mittels Berechtigungskonzept. Einsatz von Prüfsummen, elektronischen Siegeln und Signaturen in Verarbeitungsprozessen gemäß eines Krypto - Konzeptes. „Härten“ von IT – Systemen zur Vermeidung von Neben-

funktionalitäten. Dokumentiertes und angewendetes (Rollen-) Berechtigungskonzept. Prozesse zur Aufrechterhaltung der Aktualität, zum Löschen und zum Berichtigen von Daten und zur Identifizierung von Betroffenen. Durchführung von Tests zur Dokumentation und Feststellung der Funktionalität, von Sicherheitslücken, Risiken und Nebenwirkungen, einschließlich der Abläufe und Prozesse. Schutz vor äußeren Einflüssen und Zugriffen.

iv) Vertraulichkeit

Systematisierung: Kein Zugriff, Kenntnisnahme oder Nutzung der Daten durch unbefugte Dritte, ob externe, Beschäftigte oder alle Arten von Dienstleistern. Dies gilt auch bei allen Arten von Zwischenfällen.

Rechtliche Anforderungen: Art.5 Abs.1 lit.f, Art.28 Abs.3 lit.b, Art.29, 32 Abs.1 lit.b, Art.32 Abs.4, Art.38 Abs.5 (Vertraulichkeit, Belastbarkeit); Art.33 Abs.3 lit.d, 34 Abs.2 (Behebung, Abmilderung von Schutzverletzungen) DS-GVO

Praktisch: Implementierung eines sicheren Authentifizierungsverfahrens. Festlegung und Kontrolle der Nutzung zugelassener Ressourcen, Kommunikationskanäle, Abläufe, interne Regelungen und vertragliche Verpflichtungen. Prozesse zur Verschlüsselung von Datentransfer und -speicherung, einschließlich der Sicherheit der Systeme und des entsprechenden Krypto – Konzeptes. Enge Eingrenzung des Berechtigungs- und Rollenkonzeptes auf nachprüfbar, identifiziertes und zulässiges Personal, dass örtlich, fachlich zuständig, befähigt, zuverlässig, ist, keinen Interessenkonflikten unterliegt und in angemessen ausgestatteten Räumlichkeiten arbeitet.

v) Nichtverkettung

Systematisierung: Die Vermeidung einer Zusammenführung / Verkettung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, ist durch technische und organisatorische Maßnehmen sicherzustellen (Pseudonymisierung, Anonymisierung, Berechtigungskonzepte). Eine rechtliche zulässige Verkettung ist nur unter eng definierten Umständen möglich.

Rechtliche Anforderungen: Art.5 Abs.1 lit.b (Zweckbindung) DS-GVO

Praktisch: Einschränkung von Verarbeitungs-, Nutzungs-, Transferrechten und Schnittstellen, incl. ausgefeiltem Rollen- und Berechtigungskonzept und nutzerkontrolliertem Identitäts-management. Trennung von Organisation und Abteilungsgrenzen. Qualitätssichernde Revision zur Compliance bei Software – Entwicklung und Verbot von Backdoors. Einsatz von Pseudonymisierung bzw. Anonymisierung und geregeltes Zweckänderungsverfahren.

vi) Transparenz

Systematisierung: In unterschiedlichem Maße müssen Betroffene, Betreiber von Systemen und Kontrollinstanzen erkennen können, welche Daten wann, für welchen Zweck erhoben, verarbeitet werden, welche Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung in den einzelnen Phasen besitzt. Transparenz von der Entstehung bis zur Löschung.

Rechtliche Anforderungen: Art.5 Abs.1 lit.a, Art.12 Abs.1 und 3 bis Art. 15, Art. 34 (Transparenz für Betroffene); Art.5 Abs.2, Art.7 Abs.1, Art.24 Abs.1, Art.28 Abs.3 lit.a, Art.30, Art. 33 Abs. 5, Art. 35, Art. 58 Abs. 1 lit. a und lit. e (Rechenschafts- und Nachweispflicht); Art.32, 33, 34 (Angemessene Überwachung der Verarbeitung); Art.4 Abs.11, Art.7 Abs.4 (Einwilligungsmanagement) DS-GVO.

Praktisch: Dokumentationskonzept im Sinne einer Inventarisierung und dem Zusammenspiel von Verarbeitungs-, Geschäftsprozessen, Datenbeständen, Datenflüssen, Netzplänen, IT – Systemen, Software, Betriebsabläufen, Profiling, Scoring, teilautomatisierten Entscheidungsprozessen, Zugriffen, Änderungen, Versionierungen, Überwachungen, Tests, Auswertungsanalysen, Datenschutz – Folgenabschätzungen bei geänderten oder neuen Prozessen sowie Verträge mit Mitarbeitern, Dritten und Auftragsverarbeitern. Dokumentation der Bearbeitung der Rechte von Betroffenen (Einwilligung, Widerruf, Widerspruch,

Informationspflichten zu Erhebung, Quellen, Umfang, Benachrichtigungen bei Datenpannen, Zweckänderungen).

vii) Intervenierbarkeit

Systematisierung: Erfüllung der den Betroffenen zustehenden Rechten auf Benachrichtigung, Auskunft, Berichtigung, Löschung, Einschränkung, Übertragbarkeit, Widerspruch und Eingriff in automatisierte Bewertungs- und Entscheidungsprozesse, Profiling, sowie Maßnahmen zur Identifizierung bzw. Authentisierung. Zwecks Erfüllung der Betroffenenrechte und möglichen, behördlichen Anordnungen muss der Verantwortliche jederzeit Eingriff in die Prozesse nehmen können.

Rechtliche Anforderungen: Art.12 Abs. 2 (Wahrnehmung Betroffenenrechte), Art.12 Abs.6 (Identifizierung), Art.5 lit.d, Art.16 (Berichtigung), Art.17 Abs.1 (Löschung), Art.18 (Einschränkung), Art.20 Abs.1 (Übertragung), Art.22 Abs.3 (Eingriffsmöglichkeit Profiling), Art.25 Abs.2 (Datenschutz Voreinstellungen), Art.33 Abs.3 lit.d, Art.34 Abs.2 (Behebung, Abmilderungen bei Vorfällen), Art.4 Abs.11, Art.7 Abs.4 (Einwilligungsmanagement), Art.58 Abs.2 lit.f, j (aufsichtsbehördliche Anordnungen) DS-GVO.

Praktisch: Differenzierte Einwilligungs-, Rücknahme -, Widerspruchsmöglichkeit durch notwendige, standardisierte Datenfelder (benachrichtigen, einwilligen, abrufen sperren, löschen, widersprechen, Gegendarstellung, Identifizierung, Authentifizierung), datenschutzfreundliche Voreinstellungen, ein „single point of contact“ für Betroffene. Dokumentation zur Bearbeitung von Anfragen, Störungen, Änderungen bei Verarbeitung und technisch – organisatorischen Maßnahmen.

(b) Gewährleistungsziele als Design - Strategie

In der Planung und Entwicklung, vor der Freischaltung einer Anwendung, sollten die Grundsätze der datenschutzfreundliche Voreinstellung (***Data Protection by Default***) und der datenschutzfreundlichen Technikgestaltung (***Data Protection by Design***) Einzug nehmen.

(c) Verarbeitungstätigkeiten

Art.30 DS-GVO verwendet „Verarbeitungstätigkeiten“ als zentralen Begriff für das Datenschutzmanagement und listet die vom Verantwortlichen im „Verzeichnis der Verarbeitungstätigkeiten“ zu führenden Angaben auf (gem. dem zentralen Begriff „Verarbeitung“ in Art.4 Abs.2 DS-GVO):

- ✔ Name und Kontaktdaten Verantwortliche, Vertreter, Datenschutzbeauftragte.
- ✔ Zwecke der Verarbeitungen und Beschreibung der Kategorien, Betroffenen, Empfänger, Übermittlungen, Drittländer und internationale Organisationen.
- ✔ Vorgesehene Fristen zur Löschung
- ✔ Allgemeine Beschreibung der technisch – organisatorischen Maßnahmen (Art.32 Abs.1 DS-GVO) kurz „TOM“

Allerdings stellen diese Mindestanforderungen noch keine ausreichende Dokumentation im Sinne der Transparenz nach Art.5 Abs.2 DS-GVO dar. Es stellt sich die Frage, ob die richtigen Maßnahmen *zweckgemäß* ausgewählt und mit der *korrekten „Wirkintensität“* betrieben werden.

i) Ebenen

Nach den Erfahrungen der Aufsichtsbehörden hat sich die Darstellung in mind. 3 Ebenen bewährt:
Ebene 1: Darstellung der datenschutzrechtlichen Konformität (Prozessnotwendige Daten)
Ebene 2: Praktische Umsetzung (Sachbearbeitung, Applikation, Verfahren)
Ebene 3: IT – Infrastruktur einschl. Sicherungskonzept (TOM)

ii) Zweck

Zur Darstellung des rechtskonformen Zwecks sollte eine Zweckabgrenzung bzw. Zwecktrennung vorgenommen werden, um strittige Deutungen zu vermeiden. Der Aspekt der Zweckbindung sollte die geeignete Funktionalität im direkten Verarbeitungsprozess (horizontale Zugriffe) und im Umfeld (vertikale Zugriffe, z. B. IT – Services) darlegen.

iii) Komponenten

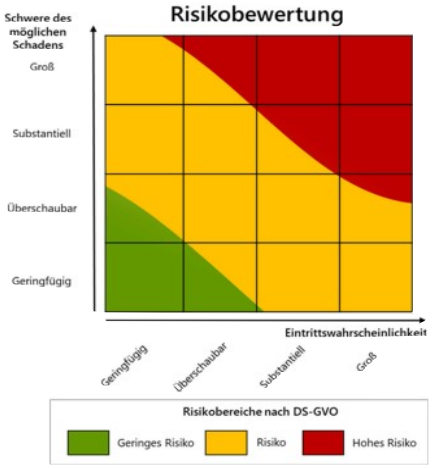
Bei der Modellierung von Verarbeitungstätigkeiten ergeben sich aus der DS-GVO folgende drei Komponenten:

1. Personenbezogenen Daten (Festlegung des Schutzbedarfs der Person)
2. Technische System und Dienste (Ergänzende Daten aus Systemen, z. B. Datums- und Ortsangaben bei Onlineerfassung, Bild & Tonaufnahmen u. ä.)
3. Technische, organisatorische und personelle Prozesse (Schnittstellen, Drittübermittlung, Auftragsverarbeitung)

Besondere Beachtung bei den drei Komponenten finden die Datenformate, die Schnittstellen und die durchgehenden Verantwortlichkeiten.

4. Risiken und Schutzbedarf

Risiko im Sinne der DS-GVO ist die Möglichkeit eines Schadeneintritts für die Rechte und Freiheiten einer oder mehrerer natürlicher Personen, einschließlich der ungerechtfertigten Beeinträchtigung oder zu einem solchen Schaden führen kann. Ausführliche Beschreibung von möglichen Schäden im Erwägungsgrund (75) der DS-GVO (physisch, materiell, immateriell, Diskriminierung, Identitätsdiebstahl & -betrug, Rufschädigung, finanzieller Verlust um nur einige zu nennen). Die Risikoermittlung erfolgt über zwei Dimensionen, (1.) der Schwere des Schadens (Y-Achse) und (2.) der Eintrittswahrscheinlichkeit (X-Achse). Grundsätzlich unterscheiden Verordnung, Gesetz und Aufsicht nur in die Kategorien geringes bis normales Risiko (**grün**, **gelb**) und hohes Risiko (**rot**). Bei „ROT“ ist eine Datenschutz – Folgenabschätzung (DS - FA) zwingend. Bleibt auch nach DS - FA die Stufe „ROT“ ist VOR Verarbeitung die Aufsicht einzuschalten (Art.35, 36 DS-GVO).



Bildquelle: Datenschutzkonferenz (DSK) Kurpapier Nr. 18, Schaubild Seite 5

(a) Risiko für Betroffene

Im Gegensatz zum allgemeinen und IT – Risikomanagement besteht im Datenschutz grundsätzlich die Pflicht, entstehende Risiken mit geeigneten und angemessenen technisch – organisatorischen Maßnahmen auf ein angemessenes Schutzniveau zu reduzieren! Es ist ***NICHT ZULÄSSIG*** auf Behandlung und Anforderung der Grundsätze nach Art. 5 DS-GVO zu verzichten und Risiken daraus in Kauf zu nehmen. ***RISIKO - AKZEPTANZ oder RISIKO - TRANSFER*** (z. B. bekannt aus der Informationssicherheit) stehen den Verantwortlichen im Datenschutz NICHT ZUR VERFÜGUNG. Erst wenn im Interesse des Betroffenen ein angemessenes Schutzniveau (**grün**, **gelb**) erreicht wird, können verbleibende Risiken durch den Verantwortlichen akzeptiert werden.

(b) Risikobetrachtung

i) Schwellenwert – Analysefunktionen

Die Schwellwert – Analyse dient der Identifikation eines voraussichtlich hohen Risikos der Verarbeitungstätigkeit und beinhalte folgende (Prüf-) Schritte:

(1) Alle Verarbeitungen nach Art. 35 Abs.3 lit.a-c DS-GVO wie (a) systematische, umfassende, automatisierte Bewertung persönlicher Aspekte (Profiling), (b) umfangreiche Verarbeitung besondere Kategorien von oder strafrechtliche Daten (Art. 9 Abs.1 und Art. 10 DS-GVO) und (c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(2) Auf der „Muss-Liste“ (auch Positiv- bzw. Negativliste) gem. Art.35 Abs. 4 DS-GVO. Für den nicht-öffentlichen Bereich wird diese Liste von der Datenschutzkonferenz unter diesem LINK veröffentlicht. Darin enthalten sind u. a. biometrische Daten wie Fingerabdruckscanner, medizinische Daten wie DNA-Tests, Finanz- und Bonitätsdaten wie Zahlungsverhalten, Insolvenzliste, Sensordaten wie GPS, Bluetooth, NFC, Funk, Scoring, Profiling u. s. w.

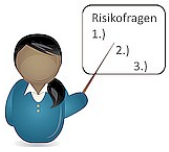
(3) Nach den Leitlinien der Datenschutzgruppe nach Artikel 29 (WP248 Rev.01)[5] reichen zwei zutreffende Kriterien (bzw. auch schon eins) aus. Die Kriterien sind:

() Scoring / Evaluation	() Rechtswirksame, automatische Entscheidungsfindung
() Systematische Überwachung	
() Datenverarbeitung in großem Umfang	() Vertrauliche, höchst persönliche Daten
() Abgleich / Zusammenführen von Daten	() Daten von schutzbedürftigen Personen
() Innovative / neue Technologien	() Hinderung an Rechts- u/o Vertragsausübung

(4) Allgemein nach Erwägungsgrund (76) DS-GVO, objektive Risikobestimmung nach Art, Umfang und Zweck der Verarbeitung.

ii) Risikoidentifikation

Drei + 1 Fragen:



(1)Welche Schäden können für betroffene Personen bei der Datenverarbeitung auftreten?
(2)Wodurch kann es zu einem Schaden kommen?
(3)Welche Handlungen und Umstände können das Schadenereignis auslösen?

✗ Welche technisch – organisatorischen Maßnahmen sind zum Schutz der Daten getroffen und sind diese angemessen und ausreichend? (z. B. an Hand IT – Grundschutz)

iii) Risikobewertung

„Es ist die Aufgabe des Verantwortlichen und ggfs. des Auftragsverarbeiters, die identifizierten Risiken für die betroffenen Personen zu analysieren und einzustufen. Dabei ist die Schwere und die Eintrittswahrscheinlichkeit der identifizierten Risiken nach objektiven Maßstäben zu bestimmen und zu dokumentieren.“ (Zitat DSM Seite 46)

(c) Risikobewertung aus Schutzbedarf & Schutzniveau

Die Eingangsgrafik zu Risikobewertung zeigt, dass ein hoher Schutzbedarf (= Risiko) der Daten durch die Verarbeitung mit entsprechenden technisch – organisatorische Maßnahmen (TOM) im Sinne der DS - GVO gemindert bzw. reduziert werden kann. Das sich aus der Kombination ergebende Schutzniveau muss so hoch sein, dass die verbleibenden Restrisiken durch den Verantwortlichen nachweislich, berechtigt verantwortet werden können; anderenfalls ist eine Verarbeitung mangels Rechtskonformität ausgeschlossen. Was „SO oder SO“ zu dokumentieren ist. Kurz gesagt, wenn bei einer hohen Schadensmöglichkeit (Datenrisiko = **ROT**) aus den Daten, mit technisch-organisatorische Maßnahmen eine geringe Eintrittswahrscheinlichkeit (TOM-Risiko = **GRÜN**) erreicht wird, ist die Risikobewertung „überschaubar“ (Gesamtrisiko = **GELB**). Einordnung gemäß Risikobewertungsgrafik.

Als Grundlage für „TOM“ dient der IT – Grundschutz des BSI[6]. Kommt es zu unterschiedlichen Bewertungen mit dem „operativen Datenschutz“ ist entweder die Maßnahme mit dem höheren Schutzbedarf anzuwenden, oder in einer genaueren Analyse sind die unterschiedlichen Gründe festzustellen und zu bewerten, wie ein angemessenes Schutzniveau erzielt werden kann. Dabei sind die Anforderungen der DS – GVO maßgeblich.

(d) „TOM“, insbesondere bei hohem Risiko

„Grundsätzlich sind Datenverarbeitungsprozesse und damit die Spezifikation der Datenverarbeitung so zu gestalten, dass, wenn möglich, die Verarbeitung ohne Personenbezug erfolgt oder zumindest die Risiken gemindert werden.“ (SDM D3.4 Seite 48)

Genanntes Beispiel ist der Einzelabruf von Daten statt Sammelabruf mit nicht benötigten Daten, wenn diese nicht unterdrückt werden können.

Auf dem aktuellen Stand der Technik sind die hier (SDM) ausgeführten und vorgeschlagenen generischen Maßnahmen eine gute Grundlage, um angemessene Maßnahmen für **normalen**

5 Quelle: Leitlinien der Datenschutzgruppe nach Artikel 29 (WP248 Rev.01)
6 Verweis: BSI IT – Grundschutz

Schutzbedarf zu entwickeln (im SDM D1ff, Seiten 31ff). **Bei hohem Schutzbedarf werden künftig diese Maßnahmen um einen Referenzkatalog* erweitert**, der zur Minderung der Risiken empfohlen wird. Zusätzlich sind individuelle Maßnahmen auszuwählen, bestehende Maßnahmen zu verschärfen und die Protokollierung zu erweitern.

„Transparenz bedeutet, dass eine Verarbeitungstätigkeit anhand von Soll-Ist-Bilanzen prüfbar sein muss. Prüfbarkeit im Nachhinein bedeutet, dass Protokolldaten erzeugt, gespeichert und verarbeitet werden müssen." (SDM D3.4 Nr. 5 Seite 49)

***)Referenzkatalog:** ist Bestandteil des SDM. Die Aufzählung ist nicht abschließend. Die Konferenz trifft keine verbindliche Aussage zur verpflichtenden Umsetzung, gleichwohl wird sie die Dokumentation prüfen, wie mit abweichenden Maßnahmen ein angemessenes Schutzniveau bei hohem bis sehr hohem Risiko für die betroffene Person gewährleistet ist. Auf der entsprechenden Netzseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) ist über einen Link zum LfDI – MV die Sammlung als verbindliche Version hinterlegt[7]: 11. Aufbewahren, 41. Planen und Spezifizieren, 42. Dokumentieren, 43. Protokollieren, 50. Trennen, 51. Zugriffe auf Daten, Systeme und Prozesse regeln, 60. Löschen und Vernichten, 61. Berichtigen, 62. Einschränken der Verarbeitung.

Hinweis zur Verwendung abweichender Maßnahmen zum Referenzmaßnahmenkatalog:

„Auch wenn diese als grundsätzlich geeignet beurteilt werden können, muss separat geprüft werden, ob sie in ihrer konkreten Ausgestaltung tatsächlich dem festgestellten Risiko entsprechen. An dieser Stelle hilft das SDM, die Erörterung auf den Nachweis dessen zu fokussieren, dass (oder inwieweit) die getroffene technische oder organisatorische Maßnahme funktional äquivalent bzw. wirkungsgleich zur Referenzmaßnahme ist." (SDM 4.4.3 Seite 58)

5. Datenschutzmanagement mit dem SDM

„Das Datenschutzmanagement ist eine umfassende Methode, um systematisch alle Anforderungen des Datenschutzrechts in einer Organisation umzusetzen. Im Folgenden wird ein Datenschutzmanagement im Zusammenspiel mit dem SDM näher beschrieben." (SDM D4 Seite 50)

(a) Rechtliche Grundlagen

Die Verantwortlichen sind für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich und müssen den Nachweis erbringen (Führung eines Verarbeitungsverzeichnisses; Dokumentation der technische und organisatorische Maßnahmen; Durchführung der Datenschutz – Folgenabschätzung, wo erforderlich und eine kontinuierliche Evaluierung und ggf. Verbesserung). Für die Einhaltung dieser Aufgabenstellung wird der PDCA-Zyklus (Plan, Do, Check, Act), ein dauerhafter, zyklischer Prozess als Grundlage vorgeschlagen, da auch die Datenschutzprüfungen der Aufsichtsbehörden in der Regel diesem Prozess-Ablauf entsprechen.

(b) Vorbereitungen

(a) ***Klarheit über die sachlichen Verhältnisse*** (Wer ist beteiligt und verantwortlich. Welche Daten werden wozu benötigt und wie verarbeitet. Wer kontrolliert und welche Hilfestellungen gibt es).

(b) ***Zulässigkeit der Verarbeitung*** (durch Einwilligung, Vertrag, Vorvertragsverhandlungen, rechtliche Verpflichtung, den Schutz lebenswichtiger Interessen, in öffentlichem Interesse, im Interesse des Verantwortlichen und überwiegen dabei die Interessen, Grundrechte und -freiheiten der betroffenen Person.)

(c) ***Materiell-rechtliche Beurteilung***, d. h. die grundsätzliche Zulässigkeit der Verarbeitungstätigkeit (Anzuwendendes nationales Datenschutzrecht; Legitimität in Bezug auf Zweck und ggf. Übermittlung an Dritte; Erheblichkeit / Notwendigkeit der Datenerhebung;

„Ausführlichkeit und Detaillierungsgrad insbesondere der Feststellungen zu den sachlichen Verhältnissen werden von Verarbeitung zu Verarbeitung variieren, ebenso wie der Grad der Formalisierung des Vorge-

7 Verweis: BfDI ü/LfDI Mecklenburg – Vorpommern SDM und Referenzkatalog

hens von informeller Befragung bis hin zum Einsatz von standardisierten Fragebögen. Eine strukturierte Zusammenfassung der Ergebnisse ist unabhängig davon ebenso üblich wie für die weiteren Schritte unentbehrlich." (SDM 4.2 Seite 52)

(c) Spezifizieren und prüfen

Grundlegende Voraussetzung für die Spezifizierung (und spätere Prüfung) ist die Festlegung, wie die Gewährleistungsziele operationalisiert werden (in Abhängigkeit des Risikos), d.h. nach Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit, Datenminimierung und Belastbarkeit (eben den Gewährleistungszielen). Nach der qualitativen Bestimmung können die technischen und organisatorischen Maßnahme bestimmt werden.

(d) Prozess

„Die Rechenschaft- und Nachweispflichten sind eine dauerhafte Aufgabe für den Verantwortlichen und sollte daher als dauerhafter, zyklischer Prozess etabliert werden. Mit dem aus dem Qualitätsmanagement bekannten und bewährten PDCA-Zyklus (Plan, Do, Check, Act) steht ein kontinuierlicher Verbesserungsprozess in vier Phasen zur Verfügung, der die Grundlage für den hier beschriebenen Datenschutzmanagement-Prozess (DSM-Prozess) bildet." (SDM D4.1 Seite 50)

4. Verbessern von erkannten Defiziten bei Grundrechtseingriffen bei der Verarbeitung, den Maßnahmen und / oder des Controlling nach Entscheidung des Verantwortlichen.	**(Anweisung) →**	1. Planen / Spezifizieren / DSFA Auswahl aller relevanten Daten, IT-Systeme, Prozesse, Schwellenwertanalyse, DSFA usw
↑ (Erkenntnisse)		**↓ (Sollwert)**
3. Kontrollieren, prüfen beurteilen Kontrolle des laufenden Betriebs an Hand von Soll / Ist Bilanzen und Beurteilung der Prüfungsergebnisse in Bezug auf rechtliche Vorgaben und Wirksamkeit der Maßnahmen	**← (Istwert)**	2. Implementieren der Verarbeitungsfunktionen, der technischen und organisatorischen Maßnahmen und Herstellung der Prüfbarkeit

6. Organisatorische Rahmenbedingungen

Das Standard – Daten - Schutzmodell (SDM) basiert auf der gleichen Grundschutzmethodik wie der BSI – Grundschutz (BSI-G), d.h. Modellierung der Verarbeitungstätigkeiten (Geschäftsprozesse) und bietet daher eine gute gemeinsame Basis, z. B. für die technischen und organisatorischen Maßnahmen des Datenschutzes. In der Zielrichtung besteht allerdings ein wesentlicher Unterschied. Während das SDM die Perspektive des Betroffenen einnimmt, ist es beim BSI – Grundschutz der Schutz er datenverarbeitenden Organisation. Im BSI – Standard Kompendium 200-2 ist der Datenschutz aufgenommen und ergänzt sich idealer Weise mit dem Datenschutz in der Praxis. Auftraggeber für die Entwicklung und Pflege des SDM sind die Mitglieder der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz / DSK). Das Konzept verfolgt das Ziel den Anwendern (Verantwortliche, Datenschutzbeauftragte usw.) und den prüfenden Aufsichtsbehörden Handlungssicherheit im Umgang zu geben. Letzte Änderungen bzw. Ergänzungen:

SDM:	17.04.2020: Behandelte Version 2.0b. Veränderung zu 2.0a sind die Ausführungen zum Referenzmaßnahmenkatalog (SDM E6 Seite 70)
Referenzkataloge:	27.10.2021: Baustein Zugriffe auf Daten, Systeme und Prozesse regeln

Bei Bedarf, einfach einmal sprechen!