Dokumentation der

Sicherheit der Datenverarbeitung

nach DS-GVO

für nicht-öffentliche Stellen

Stand Januar 2021

Inhalt

1. Allgemeines

(1) Einleitung

Dieses Dokument dient als Hilfestellung für nicht-öffentliche Stellen (wie Unternehmen und staatliche Institutionen, welche am Wettbewerb teilnehmen), um Maßnahmen zur Sicherheit in der Datenverarbeitung ausreichend zu dokumentieren.

Im Ergebnis muss es:

- für den Verantwortlichen zu einer Dokumentation und Übersicht über seine getroffenen Maßnahmen zu führen, was die Sicherheitsanalyse vereinfacht, und
- für die Aufsichtsbehörde nachvollziehbar zu sein.

Dabei ist die Spanne des Umfangs notwendiger Dokumentation groß: vom Einzelselbstständigen mit minimaler IT-Ausstattung zu Großunternehmen mit einer komplexen IT-Infrastruktur (wie z.B. Krankenhäuser). Die Datenschutz-Grundverordnung (DS-GVO) gibt dabei wenig Hinweise, *wie* die Dokumentation der Sicherheit der Datenverarbeitung erfolgen muss. Dieses Dokument zeigt daher einige Formen der Dokumentation auf.

(2) Warum muss eine Dokumentation der Sicherheit der Datenverarbeitung erfolgen?

Die Notwendigkeit, die getroffenen Maßnahmen zur Sicherheit der Datenverarbeitung zu dokumentieren, ergibt sich unmittelbar aus Art. 5 Abs. 2 DS-GVO:
„***Der Verantwortliche*** *ist für die Einhaltung des Absatzes 1 verantwortlich und* ***muss dessen Einhaltung nachweisen können*** *("Rechenschaftspflicht").*“

Sowie aus Art. 24 Abs. 1 DS-GVO:
„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.“*

Die sich daraus ergebende Rechenschafts- und Nachweisfähigkeit des Verantwortlichen ist nur mit Hilfe einer geeigneten Dokumentation möglich. Auf welche Art und Weise der Nachweis erfolgen soll, ist in der DS-GVO jedoch nicht festgelegt. Was die DS-GVO in Artikel 30 ebenfalls fordert, ist das Führen eines „Verzeichnis von Verarbeitungstätigkeiten“. Auch an

© DKL 12/2019

dieser Stelle können die getroffenen Maßnahmen bereits dokumentiert (und somit nachgewiesen) werden.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat entsprechende Hinweise und ein Muster auf ihrer Website veröffentlicht [1,2].
Je nach Umfang oder Komplexität der Verarbeitungstätigkeit ist die Dokumentation der getroffenen technischen und organisatorischen Maßnahmen (TOM) um ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu erreichen im Verzeichnis von Verarbeitungstätigkeiten häufig nicht ausreichend.

(3) Risiko orientierter Ansatz zur Auswahl geeigneter technischer und organisatorischer Maßnahmen

Eine Grundannahme der DS-GVO ist, dass die Verarbeitung personenbezogener Daten immer mit einem Risiko für die Rechte und Freiheiten natürlicher Personen einhergeht. Ein grundlegendes Prinzip der Datenschutz-Grundverordnung ist daher, dass technische und organisatorische Maßnahmen anhand des von der Verarbeitungstätigkeit ausgehendes Risikos ausgewählt und ggfs. angepasst werden müssen. Dies ist z.B. in Art. 32 Abs. 1 DS-GVO zu erkennen: „*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…*“.

Neben dem Begriff der „technischen und organisatorischen Maßnahmen“ steht also auch das „Risiko“. Wie das Risiko eines Verarbeitungsvorgangs ermittelt werden kann, erläutert das Kurzpapier Nr. 18: „Risiko für die Rechte und Freiheiten natürlicher Personen“[3] der DSK. Hierbei sind die Schwere des eintretenden Schadens und dessen Eintrittswahrscheinlichkeit zu berücksichtigen. Daher stellt sich die Frage, ob auch immer die Risikobewertung zu dokumentieren ist. Explizit fordert dies die DS-GVO nur für die Dokumentation der Datenschutz-Folgenabschätzung (Art. 35 Abs. 7 lit. c) DS-GVO). Entsprechende Hinweise sind auf der Homepage[4] des TLfDI zu finden. Jedoch hat der Verantwortliche im Rahmen seiner Rechenschafts- und Nachweispflichten darzustellen, dass die gewählten TOM auch in

1 https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_verantwortliche.pdf
2 https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf
3 Abrufbar unter https://www.tlfdi.de/mam/tlfdi/datenschutz/dsk_kpnr_18_risiko.pdf
4 vgl. https://www.tlfdi.de/mam/tlfdi/datenschutz/dsfa_muss-liste_04_07_18.pdf

Bezug auf das vorliegende Risiko geeignet und angemessen sind. Je nach Umfang und Komplexität der Verarbeitung kann die Risikobetrachtung unterschiedlich umfangreich ausfallen.

2. Mögliche Szenarien

Wie im vorherigen Text beschrieben, ist die Art und Weise, wie technisch organisatorische Maßnahmen sowie deren Geeignet- und Angemessenheit dokumentiert und nachgewiesen werden müssen, nicht vorgeschrieben. Daher werden im weiteren Verlauf drei typische Szenarien beschrieben und welche Dokumentation für die Szenarien nach Ansicht des TLfDI angemessen ist:

- **Szenario A**: Kleinst- und Einzelunternehmen ohne nennenswerte Datenverarbeitungsvorgänge mit personenbezogenen Daten (z.B. Einzelselbstständige, Handwerksbetriebe mit wenigen Beschäftigten).

- **Szenario B**: kleinere Unternehmen und Freiberufler mit Buchhaltung, Personalwesen, Kundendatenbank usw. und Ausgliederung einzelner Verarbeitungsvorgänge (z.B. größere Handwerksbetriebe, Handwerksbetriebe mit Filialen, Arztpraxen, Apotheken, Einzelhandel)

- **Szenario C**: mittlere und große Unternehmen, mit komplexer Datenverarbeitung (d.h. verteilte Systeme, zahlreiche Schnittstellen, komplexe Datenflüsse). Hierunter fallen z.B. Krankenhäuser, Logistikzentren, Großhandel, produzierendes Gewerbe mit einer größeren Anzahl von Beschäftigten.

Für alle Szenarien ist Kap. 3.4 zu beachten.

(1) Dokumentationsvorschlag für Szenario A

In diesem Szenario wird davon ausgegangen, dass nur sehr wenige Verarbeitungsvorgänge mit personenbezogenen Daten und somit oft auch wenige IT-Systeme und –Verfahren genutzt werden (z.B. 1-2 Rechner mit Drucker und wenig Spezialsoftware oder ein kleiner Internetauftritt).

Es wird davon ausgegangen, dass von den Verarbeitungstätigkeiten ein geringes bis normales Risiko für die Rechte und Freiheiten natürlicher Personen ausgeht und der Verantwortliche grundlegende technische und organisatorische Maßnahmen (z.B. Passwortschutz, regelmäßige Backups, Virenscanner, evtl. Firewall, Passwortmanager) getroffen und umgesetzt hat. Hilfestellung bietet hier z.B. der Routenplaner "Cyber-Sicherheit für

© DKL 12/2019

Handwerksbetriebe"[5]. Die getroffenen Maßnahmen können damit bspw. als kurze Stichpunkte ins Verzeichnis der Verarbeitungstätigkeiten aufgenommen werden. Ergänzend sollten die Maßnahmen allerdings ausführlich dokumentiert sein. Um den Nachweis plausibel zu machen, können evtl. Screenshots des Virenschutzes, der lokalen Passwortrichtlinie o. Ä. hinzugefügt werden. Weitere Dokumentationen sind nicht notwendig, da eine übersichtliche IT-Struktur unterstellt wird. Durch die wenigen Verarbeitungsvorgänge, das Vorliegen eines geringen bzw. normalen Risikos und die Umsetzung der gängigen Sicherheitsmaßnahmen (siehe Fußnote 5), kann davon ausgegangen werden, dass damit das vorliegende Risiko ausreichend beachtet wurde. Trifft eine der Annahmen nicht zu (d.h. komplexere Verarbeitungsvorgänge oder hohes Risiko), ist nach Szenario B oder C zu verfahren.

Weiterhin sollte Kap. 3.1 Beachtung finden, wenn Spezialgesetzgebungen das Geschäftsfeld von Kleinstunternehmen branchenbezogen betreffen (z.B. bei Berufsausbildung, Heilberufen oder kleinen Nebenstellen sozialer Träger).

(2) Dokumentationsvorschlag für Szenario B

Dieses Szenario ist dadurch charakterisiert, dass bereits einzelne Strukturen beim Verantwortlichen vorhanden sind, die verschiedene unabhängige Verarbeitungsvorgänge unterstützen (also z.B. Fileserver mit verschiedenen Ablagen und Zugriffsrechten für verschiedenen Mitarbeiter, eine zentrale Nutzerverwaltung, Datenbankserver für Kundenverwaltung, Lagerhaltung usw.). Hier ist es bereits wichtig, die Verarbeitungsvorgänge und somit die Datenhaltung und die Datenflüsse genauer zu analysieren, sich über mögliche Bedrohungen und den damit verbundenen Risiken Gedanken zu machen um daraus angemessene Schutzmaßnahmen abzuleiten.

Um dies systematisch durchzuführen und zu dokumentieren, empfiehlt der TLfDI die Anwendung des Standard-Datenschutzmodells (SDM)[6] für die jeweiligen Verarbeitungstätigkeiten.. Die hierbei entstehende Dokumentation hat auch eine Risikobewertung nach dem SDM zu enthalten sein (siehe dazu Kap. 3.2 dieses Dokumentes).

Der Umfang der Dokumentation ergibt sich somit für gewöhnlich aus der Anzahl der Verarbeitungstätigkeiten, identifizierten Risiken und getroffenen Maßnahmen. Es kann für die Dokumentation eine Tabelle genügen oder es ist ein weiter strukturiertes Dokument

[5] Abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/ACS/routenplaner_print.pdf;jsessionid=E14E6C49BA814678D012D2EF158111F6.1_cid503?__blob=publicationFile&v=8

[6] Abrufbar unter https://www.tlfdi.de/mam/tlfdi/datenschutz/entschliessungen/sdm-methode_v2.0a.pdf

erforderlich. Weiterhin sollte Kap. 3.1 Beachtung finden, wenn Spezialgesetzgebungen das Geschäftsfeld von kleinen Unternehmen branchenbezogen betreffen (z.B. bei Berufsausbildung, Heilberufen oder kleine Nebenstellen sozialer Träger).

(3) Dokumentationsvorschlag für Szenario C

Dieses Szenario trifft zu auf nicht-öffentliche Stellen mit komplexen Strukturen oder Verarbeitungsvorgängen. Diese Verarbeitungsvorgänge sind für die einzelnen Akteure innerhalb der Organisation nicht mehr einfach überschaubar. Dadurch wird es notwendig, detailliert die Verarbeitungsvorgänge zu charakterisieren, zu analysieren und schlussendlich entsprechend zu dokumentieren.

Zusätzlich zu Szenario B müssen Änderungen in den Verarbeitungsvorgängen formalisiert durchgeführt werden, da die Konsequenzen der durchgeführten Änderungen für Einzelne nicht mehr überschaubar sind. Üblicherweise ist dies immer dann der Fall, wenn ein Team von Fachleuten an der Umsetzung und dem Betrieb der IT-Struktur beteiligt ist. In diesem Fall empfiehlt der TLfDI dringend den Aufbau eines Informations-Sicherheitsmanagement-Systems.

Hierfür werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) umfangreiche Methoden und Werkzeuge zur systematischen Erfassung, Dokumentation und Analyse der IT-Struktur und daraus resultierende Maßnahmen abgeleitet. Dazu zählen die - IT-Grundschutz-Standards des BSI[7] und das IT-Grundschutz-Kompendium des BSI[8], welches direkt Bezug auf das Standard-Datenschutzmodell (SDM) nimmt. Diese sollten für dieses Szenario die Analysen aus den Kap. 3.1, 3.2 und 3.4 ergänzen. In der Analyse zu 3.1 muss vor allen Dingen geprüft werden, ob die BSI- Kritisverordnung (für das Unternehmen) Anwendung findet. Das SDM und die BSI-Standards geben dabei bereits Empfehlungen für die Strukturierung der umfassenden System- und Maßnahme-Dokumentation zur IT-Sicherheit und Datenschutz.

7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

8 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

© DKL 12/2019

3. Mögliche Werkzeuge und Ansätze

(1) Ergänzende Anforderungen aus der Bundesgesetzgebung

Bei nicht-öffentlichen Stellen sind verschiedene fachliche Vorgaben zu berücksichtigen, die sich meist unmittelbar aus den ergänzenden Bundesgesetzgebungen ableiten lassen. Als Beispiel sei hier das IT-Sicherheitsgesetz genannt.

Das seit 2015 geltende IT-Sicherheitsgesetz ist ein sogenanntes Artikel-Gesetz und regelt in einzelnen Artikeln die Änderungen von verschiedenen Gesetzen. So wurden bspw. das BSI-Gesetz (BSIG), das Telekommunikationsgesetz (TKG), das Telemediengesetz (TMG), das Energiewirtschaftsgesetz (EnWG), das Atomgesetz (AtG) und auch das Fünfte Buch des Sozialgesetzbuches in Teilen angepasst.
Ziel des IT-Sicherheitsgesetzes ist, IT-Systeme und die digitale Infrastrukturen Deutschlands sicherer zu gestalten, insbesondere im Bereich der „Kritischen Infrastrukturen“. Ziel ist aber auch z.B. die Verbesserung der IT-Sicherheit bei Unternehmen, sowie ein besserer Schutz der Bürgerinnen und Bürger im Internet.
So wurden die Pflichten der Diensteanbieter von Telemediendienste, z.B. von Betreibern von kommerziellen Webangeboten, erweitert. Durch die Änderungen des § 13 Abs. 7 TMG sind höhere Anforderungen an ihre IT-Systeme verankert worden, einschließlich die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

Durch die Änderungen in § 109a Abs. 4 TKG wurden z.B. Telekommunikationsdiensteanbieter verpflichtet ihre Nutzer zu warnen, wenn Störungen von deren Datenverarbeitungssystemen ausgehen und die Nutzer bekannt sind. Soweit technisch möglich und zumutbar, hat er dabei die Nutzer auf angemessene, wirksame und zugänglich technische Mittel hinzuweisen, mit denen sie die Störungen erkennen und beseitigen können.
Betreiber „Kritischer Infrastrukturen“ müssen seitdem die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit informationstechnischer Systeme durch angemessene organisatorische und technische Vorkehrungen – dem Stand der Technik entsprechend - sicherstellen (§ 8a Abs. 1 BSIG) und haben dies mindestens alle zwei Jahre in geeigneter Weise nachzuweisen, bspw. durch Sicherheitsaudits, Prüfungen oder Zertifikate (§ 8a Abs. 3 BSIG). Dabei ist in der Verordnung zur Bestimmung „Kritischer Infrastrukturen“ nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) geregelt, welche Dienstleistungen aus den Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen und Transport und Verkehr als kritisch anzusehen sind.

wichtiger Hinweis:

Aus allen lediglich auszugsweise zitierten vorgenannten Dokumenten ergeben sich verbindliche Pflichten für Verantwortliche, die mit der Verarbeitung personenbezogener Daten verbundenen Risiken zu ermitteln, Maßnahmen zu ihrer Eindämmung zu treffen und dies nachvollziehbar zu dokumentieren[9]. Ziel ist die Aufrechterhaltung der Sicherheit der Verarbeitung sowie die Vorbeugung gegen eine gegen die DS-GVO verstoßende Verarbeitung.[10]

Die Verantwortlichen haben ergänzende Anforderungen aus der Bundes- sowie Landesgesetzgebung daher zwingend zu prüfen und zu berücksichtigen.

(2) Das Standard-Datenschutzmodell

Mit dem **Standard-Datenschutzmodell (SDM)**[11] stellt die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ein Werkzeug bereit, mit dem die risikoadäquate Auswahl und rechtliche Bewertung der von der DS-GVO geforderten technischen und organisatorischen Maßnahmen unterstützt wird.

Das SDM verwendet zur Systematisierung der datenschutzrechtlichen Anforderungen den Begriff „Gewährleistungsziele“. Datenschutzrechtliche Anforderungen zielen auf die rechtskonforme Verarbeitung, die durch technische und organisatorische Maßnahmen (TOM) gewährleistet werden muss. Durch Festlegung und Umsetzung der TOM wird das Risiko des Eintretens von Abweichungen bzgl. der rechtskonformen Verarbeitung gemindert. Gewährleistungsziele bündeln und strukturieren auch im Datenschutz die festgeschriebenen gesetzlichen Anforderungen. Mit ihrer Hilfe können Maßnahmen messbar gestaltet werden. Die beschriebene Methode lehnt sich an den IT-Grundschutz an und hat sich dort bereits bewährt. Im Unterschied zur IT-Sicherheit betrachtet der Datenschutz die Gewährleistungsziele jedoch nicht aus Sicht der Organisation, sondern aus Sicht der betroffenen Person.

Gewährleistungsziele des Datenschutzes gemäß SDM sind:

- Datenminimierung
- Verfügbarkeit,
- Integrität,

---

9 vgl. hierzu Art. 32 DS-GVO Abs. 3

10 vgl. hierzu Erwägungsgrund 83 zu Art. 32 DS-GVO: Alle Maßnahmen sollen ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.

11 DSK:
vgl. https://www.datenschutzkonferenz-online.de/media/ah/20191209_sdm-methode_v2.0a.pdf

© DKL 12/2019

- Vertraulichkeit,
- Nichtverkettung,
- Transparenz,
- Intervenierbarkeit.

Bei der praktischen Umsetzung des SDM wird ausgehend vom Schutzbedarf der Verarbeitungstätigkeit für jede zu betrachtenden Komponente der gesamten Systemstruktur - Daten, Systeme, Dienste sowie Prozesse – bzgl. der Gewährleistungsziele geprüft, welche Referenzmaßnahmen zu einem angemessenen Schutzniveau führen. Daraus resultierend werden dann einzelne, konkrete TOM angewandt und dokumentiert. Beachtet werden sollte, dass bestimmte Einzelmaßnahmen einen Beitrag zur Erreichung mehrerer Gewährleistungsziele beitragen können. Dies ist im Einzelfall ebenfalls zu dokumentieren mit dem Ziel, Datenschutzanforderungen sinnvoll zu strukturieren und in der Folge systematisch in der Organisation umzusetzen.

Entsprechend DS-GVO sind die TOM nicht nur einmalig zu implementieren, sondern vielmehr sollte ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM vorgesehen sein (Art. 32 Abs. 1 lit. d) DS-GVO). Die aktuelle Angemessenheit der TOM orientiert sich dabei am Stand der Technik[12].
Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden (Art. 32 Abs. 2) DS-GVO). Das SDM betrachtet neben den aus der IT-Sicherheit bekannten Schutzzielen vorrangig die Gewährleistungsziele mit Datenschutzbezug. Auch hieraus werden – wie im Bereich der IT-Sicherheit – in analoger Methodik TOM abgeleitet. Im Bereich des Datenschutzes werden additiv auch die Risiken betrachtet, die von den Aktivitäten der Organisation selbst innerhalb und außerhalb ihrer Geschäftsprozesse für die Rechte und Freiheiten natürlicher Personen bestehen. Insofern erfordert die Anwendung der SDM-Methodik eine erweiterte Betrachtungsperspektive hinsichtlich der Risiken, die zu bewerten sind.

Die Umsetzung von IT-Sicherheitsmaßnahmen ist für den Datenschutz essentiell. Sie stellt im SDM jedoch nur die auf den Bereich Datenschutz bezogene Auswahl geeigneter TOM aus der

[12] vgl. Art. 32 Abs. 1 DS-GVO

Perspektive der betroffenen Person(en) und dessen/deren Grundrechtsausübung dar.[13] Daher ist zu beachten, dass Maßnahmen zur Verbesserung der IT-Sicherheit zu einer Erhöhung des Risikos für die Rechte und Freiheiten natürlicher Personen führen können.

(3) Der BSI-Grundschutz

Der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte **IT-Grundschutz**[14] ermöglicht es, durch ein systematisches Vorgehen notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die BSI-Standards liefern hierzu bewährte Vorgehensweisen, das IT-Grundschutz-Kompendium[15] beleuchtet konkrete Sicherheitsaspekte indem konkrete Gefährdungen erläutert und daraus abgeleitet Anforderungen gestellt werden. Bei der Auswahl von Maßnahmen orientiert sich der Grundschutz vorrangig an den aus der IT-Sicherheit bekannten Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit.[16]

Auch das SDM aus Abschnitt 3.2 ist Bestandteil der BSI-Methodik. Deshalb wurde im Rahmen der Modernisierung der Grundschutzmethodik durch das BSI – veröffentlicht im Oktober 2017 – das Verhältnis von Datenschutz und Informationssicherheit neu justiert. Im neuen BSI-Standard 200-2 wird auf das SDM verwiesen, wenn es darum geht, das Risiko eines Grundrechtseingriffs und den daraus folgenden Schutzbedarf zu bestimmen. So werden im neuen Baustein „CON.2 Datenschutz“ Abgrenzungsmerkmale zwischen Informationssicherheit und Datenschutz beschrieben.[17]

---

13 Erläuterung aus dem SDM: „IT-Grundschutz hat vorrangig die Informationssicherheit im Blickfeld und soll die datenverarbeitende Institution schützen. Für die Auswahl von Maßnahmen nach dem SDM ist hingegen die Beeinträchtigung maßgeblich, die ein Betroffener durch die Datenverarbeitung der Institution hinnehmen muss. Vor diesem Hintergrund ist zwischen der Auswahl von Maßnahmen zur Gewährleistung der Informationssicherheit für Institutionen durch verantwortliche Stellen und der von Maßnahmen zur Gewährleistung der Betroffenenrechte zu unterscheiden.“, ebenda

14 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/itgrundschutzAbout_node.html

15 vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

16 Quelle: https://www.datenschutzkonferenz-online.de/media/ah/20191209_sdm-methode_v2.0a.pdf/ > SDM, Version 2a vom 06.12.2019, S. 57f

17 Erläuterung aus dem SDM: Die Anforderung „CON.2.A1 Umsetzung Standard-Datenschutzmodell“ besagt konkret, dass geprüft werden sollte, ob das SDM angewendet wird. Das etwaige Nichtberücksichtigen aller Gewährleistungsziele verbunden mit der Nichtanwendung der SDM-Methodik sowie der empfohlenen Referenzmaßnahmen sollten stichhaltig und ausführlich sachlich begründet werden.; ebenda

© DKL 12/2019

BSI-Grundschutz und SDM ergänzen sich. Sie liefern gemeinsam die Informationen, die erforderlich sind, um die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten zu treffen und diese nachweisen zu können (Art. 5 Abs. 2 DS-GVO).

(4) Verarbeitung im Auftrag

Bedient sich der Verantwortliche eines **Auftragsverarbeiters**, so müssen gem. Art. 28 DS-GVO geeignete technische und organisatorische Maßnahmen durchgeführt werden, so dass die Verarbeitung im Einklang mit der DS-GVO erfolgen kann und die Rechte der betroffenen Person gewahrt werden. Alle Anforderungen müssen den aktuellen Stand der Technik abbilden.

Die Verarbeitung durch den Auftragsverarbeiter erfolgt gem. Art. 28 Abs. 3 DS-GVO **auf** der **Grundlage eines Vertrages** oder eines anderen Rechtsinstruments nach dem Unionsrecht mit festgelegten Pflichten und Rechten der Vertragspartner. Weiterhin muss der Auftragsverarbeiter der verantwortlichen Stelle (dem Auftraggeber) geeignete Garantien liefern, dass die Datenverarbeitung hinreichend abgesichert ist. Dazu kann eine ISO-Zertifizierung zählen oder auch eine Liste technisch organisatorischer Maßnahmen beim Auftragnehmer. Der Teil des Auftragsverarbeitungsvertrages mit den entsprechenden Nachweisen ist dann auch für den Verantwortlichen der Nachweis geeigneter Maßnahmen nach Art. 5 Abs. 2 DS-GVO.

Quellen, Hinweise zum Datenschutz sowie zur IT-Sicherheit
- Auszug -

Quellen mit Informationen

- **Verzeichnis von Verarbeitungstätigkeiten**

  -https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf

- **Auftragsverarbeitung**

  https://www.tlfdi.de/mam/tlfdi/themen/muster_verarbeitungsverzeichnis_auftragsverarbeiter.pdf

  Kurzpapier DSK:

  https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSK_KPNr_13_Auftragsverarbeitung.pdf

  Formulierungshilfe, Fragebogen:

  https://tlfdi.de/mam/tlfdi/start/fragebogen.pdf

- **Orientierungshilfen**

  Unternehmen:

  https://tlfdi.de/tlfdi/datenschutz/unternehmen/

  https://tlfdi.de/tlfdi/gesetze/orientierungshilfen/

  Merkblatt zu Art. 13 DS-GVO:

  https://www.tlfdi.de/mam/tlfdi/datenschutz/merkblatt_artikel_13_ds-gvo.docx

  Merkblatt zu Art. 14 DS-GVO:

  https://www.tlfdi.de/mam/tlfdi/datenschutz/merkblatt_artikel_14_ds-gvo.docx

  Handreichung DS-FA:

  https://www.tlfdi.de/mam/tlfdi/datenschutz/handreichung_ds-fa.pdf

  Europa:

  https://www.tlfdi.de/tlfdi/europa/europaeischedsgvo/

- **Standards**

  SDM und Maßnahmenkatalog (Bausteine):

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

BSI IT-Grundschutz-Standards:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

BSI IT-Grundschutz-Kompendium:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html