SDM
Standard-Datenschutzmodell

Neues zum Standard-Datenschutzmodell (SDM)

Sommerakademie 2018

Martin Rost

DATENSCHUTZAKADEMIE Schleswig-Holstein

ULD

Agenda

1. Aktueller Status des Standard-Datenschutzmodells (SDM)
2. Kurzdarstellung des SDM
3. Risiko, Schutzbedarf und Schutzniveau
4. Beispiele für SDM-Anwendungen
5. SDM und IT-Grundschutz
6. Kurzvorstellung der fertiggestellten SDM-Bausteine der „UAGSDM Bausteine“

   Datenschutz-Management, Löschen, Aufbewahren, Protokollieren, Planen und Spezifizieren, Trennen, Dokumentieren
7. Wie geht es weiter?

Warum SDM?

Artikel 32 „Sicherheit der Verarbeitung“

„(…) treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

(…)

*d) ein **Verfahren** zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“*

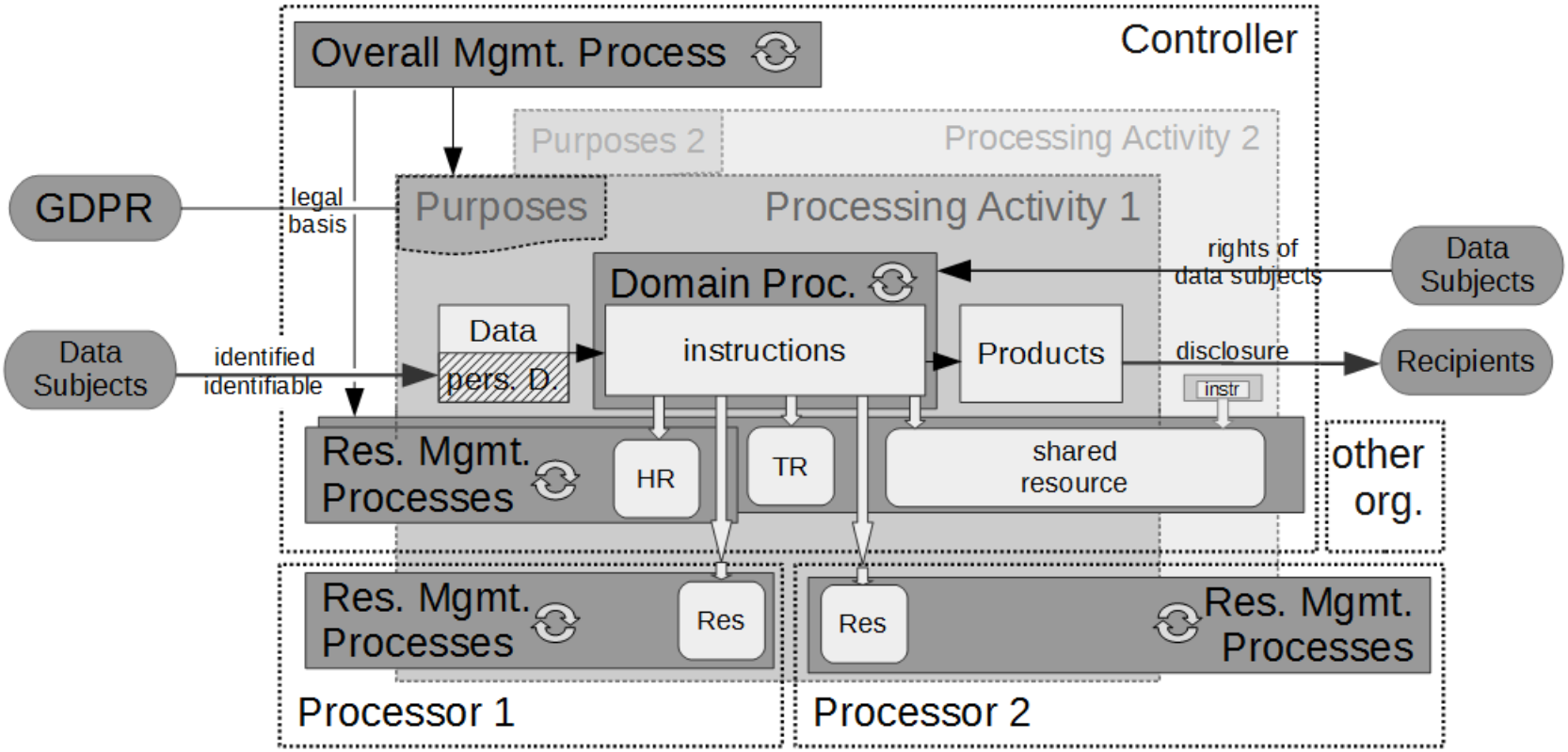
Gegenstand einer Datenschutzprüfung ist eine „Verarbeitung“ (Art. 4 Abs. 2 DSGVO)

“Im Sinne dieser Verordnung bezeichnet der Ausdruck „*Verarbeitung*“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie

- das Erheben,
- das Erfassen,
- die Organisation,
- das Ordnen,
- die Speicherung,
- die Anpassung oder Veränderung,
- das Auslesen,
- das Abfragen,
- die Verwendung,
- die Offenlegung durch Übermittlung,
- Verbreitung oder eine andere Form der Bereitstellung,
- den Abgleich oder die Verknüpfung,
- die Einschränkung,
- das Löschen oder die Vernichtung; (….)”

Auch eine Datenschutzprüfung ist eine Verarbeitung. → Eine Datenschutzprüfung muss in diesen Teilprozessen einer DS-Prüfung ebenfalls den Grundsätzen aus Art. 5 genügen.

„Model of Processing Activity“



Autor:
Dr. Bruegger / ULD
Die Arbeit wurde vom BMBF gefördert in den Projekten EIDI und iKoPA

Aktueller Status SDM

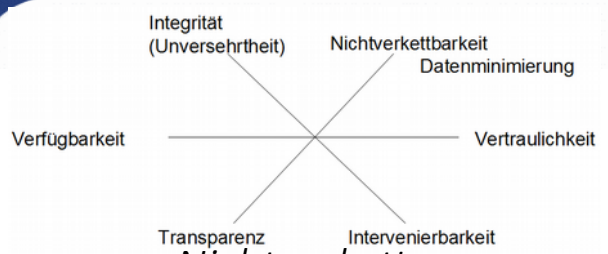
V 0.9 - 2015

V 1.0 - 2016

V 1.1 - 2018

- Das SDM ist eine Methode zur **Prüfung und Beratung von Verarbeitungen.**
- **DSB-Konferenz** bestätigt 2018/04 zum dritten Mal die Verwendung der SDM-Methodik (V1.1, 42 Seiten, Erprobungsfassung).
- **SDM-Handbuch** kann von den **Webseiten** der deutschen Datenschutz-aufsichtsbehörden und der DSB-Konferenz bezogen werden.
- SDM ist **normativ verankert in der DSGVO.**
- SDM lehnt sich methodisch an **IT-Grundschutz** des BSI an.
- Das Erarbeiten von **Texten zu Schutzmaßnahmen** ist Datenschutzaufsichts-behörden vorbehalten.
- Eine **Englischversion** der V1.0 der SDM-Methodik liegt vor.
- Eine **Tool-Unterstützung** bspw. durch Verinice / HiScout wird angestrebt.
- Wesentliche **Änderung V1.1 gegenüber V1.0**: a) Umstellung auf die DSGVO, b) Schutzbedarfsermittlung der Risikobestimmungen der DSGVO angepasst.
- Die Datenschutzbeauftragten der Bundesländer *Hessen, Mecklenburg-Vorpommern, Schleswig-Holstein, Sachsen* sowie *der Evangelischen Kirche Deutschlands* haben **am 10.9.2018 zur Sommerakademie 2018 in Kiel einen ersten Katalog mit Referenz-Datenschutz-Schutzmaßnahmen** veröffentlicht.

Modellierungskomponenten des SDM



1. **Normative Anker des Modells: 6+1 Gewährleistungsziele**
   - Gewährleistungsziele (*Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung (Datenminimierung), Intervenierbarkeit*) strukturieren operative Anforderungen der DSGVO und setzen Grundsätze aus Art. 5 DSGVO und Anforderungen insb. aus Art. 9, 12-23, 24, 25, 32, 35 DSGVO funktional um.
   - Zentrale Funktion: *Normative Soll-Werte werden in funktionale Soll-Werte transformiert.*
   - Für jedes Gewährleistungsziel sind *Schutzmaßnahmen* bestimmt oder bestimmbar.
2. **Bestimmen der Wirksamkeit von Schutzmaßnahmen anhand der Risikohöhe einer Verarbeitung**
   - *Risiken* bestehen für Betroffene allein deshalb, weil eine Organisation personenbeziehbare Daten verarbeitet („Risiko für die Rechte & Freiheiten natürlicher Personen“).
   - *Schutzbedarf* haben natürliche Personen
   - Der Schutzbedarf (begründet die Gestaltung der Verarbeitung und die Wirksamkeit von Schutzmaßnahmen) ist seitens des Verantwortlichen festzusetzen: *normal / hoch / sehr hoch*
3. **Komponenten einer Verarbeitung**
   - Die Gestaltung einer datenschutzgerechten Verarbeitung muss die Komponenten *Daten, IT-Systeme und Prozesse* umfassen.

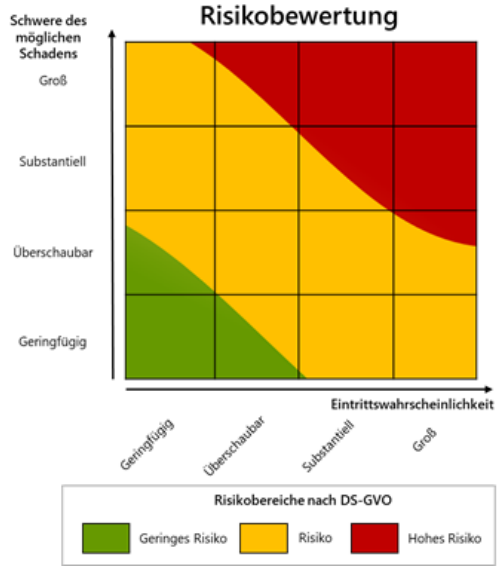
Risikohöhe, Schutzbedarf, Schutzniveau

- „Risiko“ (DSGVO)
  - **Risikotyp 1**: **Datenverarbeitung einer Organisation ist beliebig**. Die Anforderungen der DSGVO werden nicht wirksam umgesetzt, d.h. der Grundrechtseingriff der Organisation geht über das unbedingt Erforderliche hinaus (bzw.: ist nicht minimal-intensiv).
    - **Risikokriterien** für Datenschutz sind durch die *Negation der Grundsätze des Art. 5* DSGVO (bzw. der Gewährleistungsziele des SDM) bestimmbar.
    - **Angreifermodell und Szenarien** bestimmen das real bestehende operative Risiko: Wer hat (auch mit hinreichender Rechtsgrundlage ausgestattet) Interesse an Daten sowie Ressourcen für den Zugriff?
  - **Risikotyp 2: Nutzung unsicherer IT.** Die Organisation tut zu wenig zur Absicherung der Geschäftsprozesse.
    - **IT-Sicherheitsmanagement muss DS-Management** folgen sucht bei Mängeln und mangelnder Datenschutz-Profilierung von IT-Schutzmaßnahmen den Konflikt mit IT-Sicherheitsmanagement / Verantwortlichem.
  - ***Die Höhe des Risikos einer Datenverarbeitung bemisst sich an Risikotyp 1 und Risikotyp 2, wenn eine Organisation ohne operativen Datenschutz und -Expertise und ohne Schutzmaßnahmen personenbezogene Daten verarbeitet.***
- Schutzbedarf (SDM)
  - **Der Schutzbedarf einer Person richtet sich nach dem Risiko, das eine Verarbeitung ohne Schutzmaßnahmen erzeugt.**
    → normales Risiko = normaler Schutzbedarf, hohes Risiko = hoher Schutzbedarf, ...
- „Schutzniveau“ (DSGVO)
  - **Das Schutzniveau einer Verarbeitung entspricht dem real erzielten Schutz für Betroffene durch Gestaltung der Verarbeitung sowie der Implementation von Schutzmaßnahmen, mit denen das Risiko der Verarbeitung für den Betroffenen auf ein verantwortbares Maß gemindert wurde.**

Risikobestimmung gem. Art. 29-Gruppe

1. **Bewerten oder Einstufen** (Scoring)
   ("Evaluation or scoring")
2. **Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung**
   ("Automated-decision making with legal or similar significant effect")
3. **Systematische Überwachung**
   ("Systematic monitoring")
4. **Vertrauliche oder höchst persönliche Daten**
   ("Sensitive data or data of a highly personal nature")
5. **Datenverarbeitung in großem Umfang**
   ("Data processed on a large scale")
6. **Abgleichen oder Zusammenführen von Datensätzen**
   ("Matching or combining datasets")
7. **Daten zu schutzbedürftigen Betroffenen**
   ("Data concerning vulnerable data subjects")
8. **Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen**
   ("Innovative use or applying new technological or organisational solutions")
9. **Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert**
   ("When the processing in itself prevents data subjects from exercising a right or using a service or a contract")

Wenn **mind. 2 Kriterien** aus dieser Liste zutreffen, besteht ein *hohes Risiko*, das die Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 erfordert.



aus: WP 248 der Art. 29 Gruppe ab Seite 10 ff. / DSK: „Gemeinsame Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist (2018-0525) / ebenso: DSK: „Kurzpapier Nr. 18"

IT-Grundschutz „CON.2: Datenschutz"

BSI-Standards zur Informationssicherheit

Informationssicherheit und Grundschutz

BSI-Standard 200-1
Managementsysteme für Informationssicherheit (ISMS)

BSI-Standard 200-2
IT-Grundschutzmethodik

BSI-Standard 200-3
Risikoanalyse auf der Basis von IT-Grundschutz

BSI-Standard 100-4
Notfallmanagement

IT-Grundschutz-Kompendium

Kapitel 1: Vorspann
Kapitel 2: Schichtenmodell und Modellierung

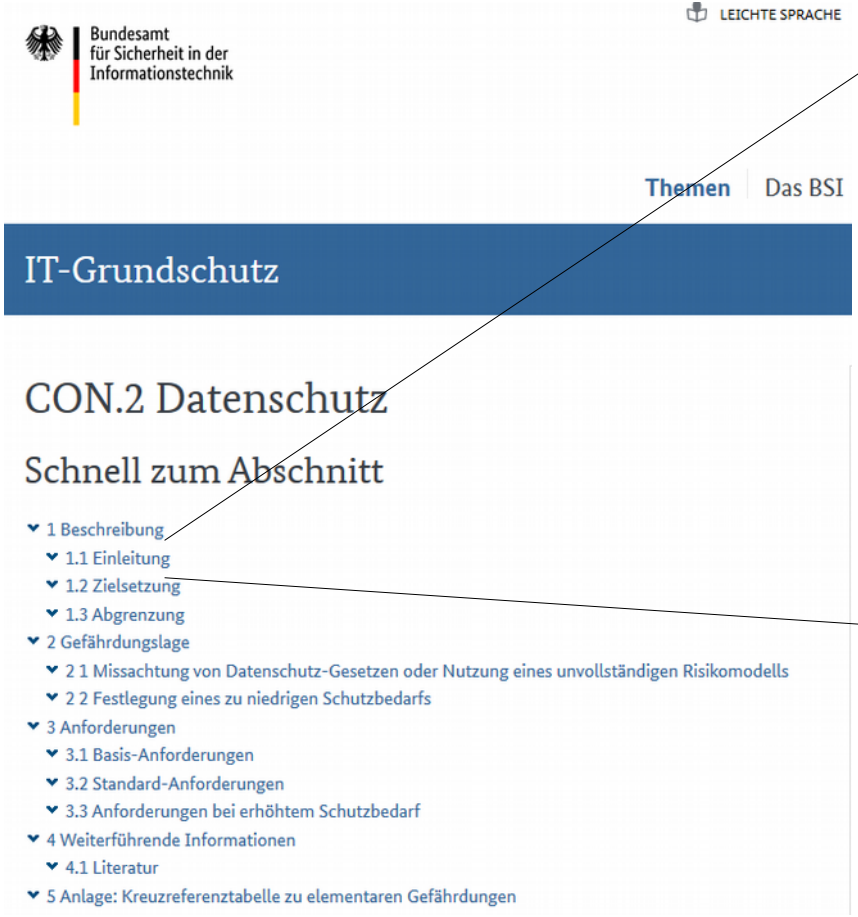
Elementare Gefährdungen

Schichten

Prozessbausteine:
- ISMS (Sicherheitsmanagement)
- ORP (Organisation und Personal)
- CON (Konzepte und Vorgehensweise)
- DER (Detection und Reaktion)

Systembausteine
- IND (Industrielle IT)
- APP (Anwendungen)
- SYS (IT-Systeme)
- NET (Netze und Kommunikation)
- INF (Infrastruktur)

IT-Grundschutz und SDM



Bundesamt für Sicherheit in der Informationstechnik

LEICHTE SPRACHE

Themen | Das BSI

IT-Grundschutz

CON.2 Datenschutz

Schnell zum Abschnitt

- 1 Beschreibung
  - 1.1 Einleitung
  - 1.2 Zielsetzung
  - 1.3 Abgrenzung
- 2 Gefährdungslage
  - 2 1 Missachtung von Datenschutz-Gesetzen oder Nutzung eines unvollständigen Risikomodells
  - 2 2 Festlegung eines zu niedrigen Schutzbedarfs
- 3 Anforderungen
  - 3.1 Basis-Anforderungen
  - 3.2 Standard-Anforderungen
  - 3.3 Anforderungen bei erhöhtem Schutzbedarf
- 4 Weiterführende Informationen
  - 4.1 Literatur
- 5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

1.1 Einleitung

Aufgabe des Datenschutzes ist es, Personen davor zu schützen, dass diese durch den Umgang mit personenbezogenen Daten auf der Seite von Institutionen an der Ausübung von Grundrechten beeinträchtigt werden. Die Verfassung der Bundesrepublik Deutschland gewährleistet das Recht der Bürgerinnen und Bürger, grundsätzlich selbst über die Verwendung ihrer personenbezogenen Daten zu bestimmen. Die Datenschutzgesetze des Bundes und der Bundesländer nehmen darauf Bezug, wenn sie den Schutz des Rechts auf informationelle Selbstbestimmung hervorheben. Die EU-Grundrechte-Charta formuliert in Artikel 8 unmittelbar das Recht auf den Schutz personenbezogener Daten (Absatz 1), hebt die Notwendigkeit einer Rechtsgrundlage zur Datenverarbeitung hervor (Absatz 2) und schreibt die Überwachung der Einhaltung von Datenschutzvorschriften durch eine unabhängige Stelle vor (Absatz 3). Die Datenschutz-Grundverordnung [DSGVO] führt diese Anforderungen der Grundrechte-Charta näher aus. Von herausragender Bedeutung ist dabei der Artikel 5 DSGVO, der die Grundsätze versammelt, die teilweise als *Schutzziele* ausgewiesen sind. Das Standard-Datenschutzmodell (SDM) bietet eine Methode, um diese geforderte Umsetzung von Datenschutzvorschriften auf der Grundlage von sieben Schutzzielen bzw. Gewährleistungszielen systematisch überwachen zu können.

*„**Das Standard-Datenschutzmodell (SDM)** bietet eine Methode, um diese geforderte Umsetzung von Datenschutzvorschriften auf der Grundlage von sieben Schutzzielen bzw. Gewährleistungzielen systematisch überwachen zu können.“*

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_2_Datenschutz.html

IT-Grundschutz "CON.2: Datenschutz"

- Es überführt datenschutzrechtliche Anforderungen in einen Katalog von Gewährleistungszielen.
- Es gliedert die betrachteten Verfahren in die Komponenten Daten, IT-Systeme und Prozesse.
- Es berücksichtigt die Einordnung von Daten in die drei Schutzbedarfsabstufungen normal, hoch und sehr hoch und ergänzt diese um entsprechende Betrachtungen auf der Ebene auch von Prozessen und IT-Systemen.
- Es bietet einen hieraus systematisch abgeleiteten Katalog mit standardisierten Schutzmaßnahmen.

- Die Institution hat den gegenüber der Informationssicherheit erweiterten Schutzzielekatalog 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 des Verfahrens und der Schutzmaßnahmen zugunsten der Institution bzw. zu Ungunsten betroffener Personen gestaltet.

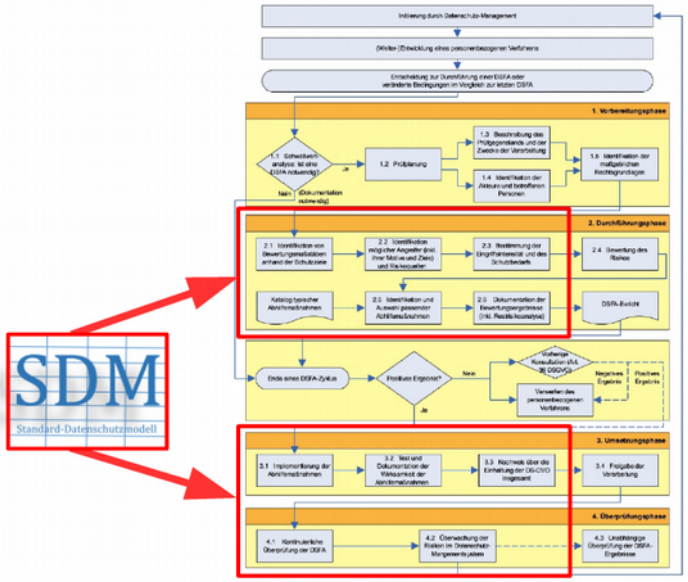
Beispiel für Maßnahmenkatalog für Schulverwaltungs-SW

(LfD Mecklenburg-Vorpommern)

1. Entwurf eines Maßnahmenkatalogs für die Einführung einer Schulverwaltungssoftware nach dem Standard-Datenschutzmodell

	Daten			Gewährleistungsziele						
Schutz-bedarf	Schüler	Erziehungs-berechtigte	Lehrer (Beschäft-igten Daten)	Datensparsamkeit	Verfügbarkeit	Integrität	Vertraulichkeit	Nichtverkettbarkeit	Transparenz	Intervenierbarkeit
Normal	Schülernummer	Name	Name	- Rechte- und Rollenkonzept - rollen- und aufgabenabhängige Gestaltung der Eingabemasken - automatisierte Sperr- und Löschroutinen - Möglichkeit der Anbringung von Sperrkennzeichen - Möglichkeit der Pseudonymisierung nach Bedarf - Möglichkeit der Anonymisierung nach Bedarf - vorkonfigurierbare Exportmöglichkeiten für verschiedene Zwecke (z.B. Informationen für Vereine, etc.) - landesweit abgestimmtes Softwareänderungs-management	- Rechte- und Rollenkonzept - Backup von Daten und Konfiguration nach Backupkonzept - Redundanz der zentralen Systeme - geeignete dezentrale Backupmaßnahmen (z.B. Papierunterlagen oder Backupleitung...) - baulicher Datenschutz (z.B. Brandschutz, Zugangsschutz,...) - Schutz vor Schadsoftware - Firewall - regelmäßige Wartung von Hard- und Software - Vertretungs-regelungen für Personal - Festlegung von Datenformaten - Festlegung der Aufbewahrungsstrategie	- Rechte- und Rollenkonzept - Festlegung der jeweils erforderlichen Erfassungsfrequenz der Datenbestände - Prüfsummen, Hashverfahren - Integritäts-bedingungen für Datenbanken (z.B. Vorgaben für Formate und Wertebereiche) - Integritätsschutz für Software (z.B. Signaturen) - Protokollierungs-verfahren hinsichtlich der Eingabe und Änderung von Daten	- Rechte- und Rollenkonzept - logische Trennung von Schulverwaltungsnetz und Netz für die Lehre - zentrale Administration der verwendeten IT-Systeme durch von der verantwortlichen Stelle Beauftragte - Zugriff auf die Schulverwaltungssoft ware nur mit Verfahren nach dem Stand der Technik (u.a. Kryptokonzept, Ende-zu-Ende Verschlüsselung, individualisierte Clientzertifikate, sichere Passwortgestaltung) - baulicher Datenschutz (z.B. Zugangsschutz) - Verpflichtung auf das Datengeheimnis - klare vertragliche Regelungen (z.B. Auftragsdatenverarbeitung, Wartungsverträge) - Mandanten-trennung bei	- Rechte- und Rollenkonzept - Mandanten-trennung bei gemeinsamer Verarbeitung der Daten mehrerer Schulen auf zentralen Datenverarbeitungs anlagen -frühestmögliche Anonymisierung und Pseudonymisierung, - zweckbezogene Pseudonymisierung - Beschränkung der Datenschnittstellen auf das erforderliche Maß - Beschränkung der Funktionalität der Software auf das erforderliche Maß - bei regelmäßiger Übermittlung von Daten an Dritte ~~durch~~ Bereitstellung eines separaten Abrufdaten-bestandes durch die verantwortliche Stelle	- Rechte- und Rollenkonzept - Möglichkeit der Kenntnisnahme von gespeicherten Daten durch den Betroffenen - Verfahrens-dokumentationen (u.a. Freigabe, Vorabkontrolle, Verfahrensbeschreibung, Sicherheits-konzept, Verträge, Rechtevergabe, relevante Dienst-anweisungen und Dienstverein-barungen) - Dokumentation von Einwilligungen und Widersprüchen (soweit relevant) - Dokumentation der Softwareversions-verwaltung und anderer Administrations-handlungen - Protokollierungs-verfahren hinsichtlich der Eingabe und Änderung von Daten -Auswertungskonzept für Protokolle - Protokollierung von	- Rechte- und Rollenkonzept - Möglichkeit der Einsicht von Schülern (ggf. Erziehungsberechtigte) in über sie gespeicherte Daten - Möglichkeit des Ausdrucks des über den Betroffenen gespeicherten Daten auf Anforderung (z. B. Schülerstammblatt) - Einrichtung von Prozessen zur Berichtigung, Sperrung oder Löschung von Daten - Rücknahmemöglichkeit von Einwilligungen - Einsichtnahmemöglichkeit in Protokolldateien bspw. zu Übermittlungsvorgängen (ggf. gemeinsam mit dem bDSB) - Verfahren zur Beauskunftung von Datenübermittlungen (ggf. unter Einbeziehung der Empfänger) - Einrichtung von Prozessen zur Information des Betroffenen bei Änderungen von Grunddaten
	Name, ggf. Geburtsname	Vorname	Vorname							
	Vorname	Anschrift	Anschrift							
	Anschrift	Telefon-nummer	Telefon-nummer?							
	Telefonnummer	Klassen-elternrat	Geburtsdatum							
	Geburtsdatum		Titel							
	Geschlecht		Funktion							
	Geburtsort		Vertretungs-/Ausfallstunden							
	Geburtsland									
	weitere Schülerdaten									
	Staatsangehörigkeit									
	Ausbildungsbetrieb									
	Einschulungsdatum									
	bisher besuchte Schulen									
	zurzeit besuchte Jahrgangsstufe und Klasse gebenenfalls erfolgter Wechsel, Wiederholung, Begrenzung der Verweildauer									
	Entlassungsdatum									
	erreichter Abschluss oder Abschlussprüfung									
	Überweisungsdatum, Name, Anschrift der aufnehmenden Schule									
	Schwerpunkte bei Ausbildungsgängen (z.B. Fremdsprachenbelegung)									
	Praktika									
	Fahrschülerin oder Fahrschüler									
	Mandat in Mitwirkungsorganen									
	sonstige schulbezogene Funktionen									
	Beurlaubung vom Schulbesuch									
	An-/Abmeldung vom Schulbesuch nach Auslandaufenthalt									
	Teilnahme an erforderlichen Untersuchungen									
	Leistungsdaten der Schüler mit normalen Schutzbedarf									
	Feststellungsprüfung in einer Fremdsprache (Sprache des Herkunftslandes)???									
	Kurseinstufungen									
	Fächer des Wahlpflichtunterrichts									

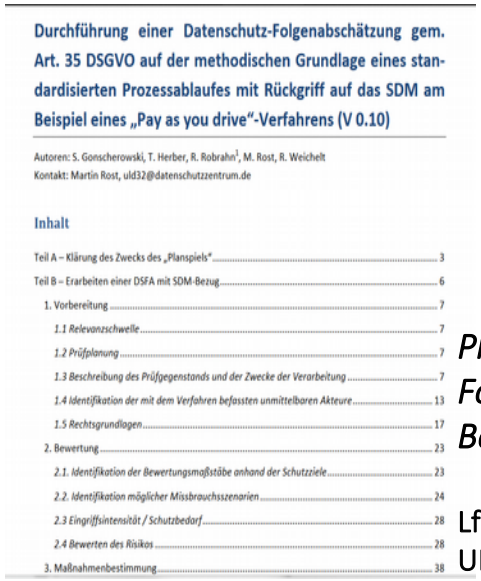
SDM als Grundlage für eine DS-Folgenabschätzung gem. Art. 35 DSGVO



Whitepaper „Datenschutz-Folgenabschätzung“

Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
ULD (Unabhängiges Landeszentrum für Datenschutz), Kiel
Universität Kassel, Institut für Wirtschaftsrecht

https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf



Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO auf der methodischen Grundlage eines standardisierten Prozessablaufes mit Rückgriff auf das SDM am Beispiel eines „Pay as you drive“-Verfahrens (V 0.10)

Autoren: S. Gonscherowski, T. Herber, R. Robrahn[1], M. Rost, R. Weichelt
Kontakt: Martin Rost, uld32@datenschutzzentrum.de

Inhalt

Planspiel „Datenschutz-Folgenabschätzung“ am Beispiel „pay-as-you-drive“

LfD-Mecklenburg-Vorpommern
ULD Kiel

https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf

SDM-Bausteine
Aufbau der Texte

- Baustein 60 „Löschen und Vernichten“
  - 1. Bezug zu Gewährleistungszielen
  - 2. Beschreibung
    - Daten
    - Systeme
    - Prozesse
  - 3. Differenzierung bei hohem Schutzbedarf
  - 4. Referenzen
  - 5. Zusammenfassung der Maßnahmen

SDM, V1.1
Aktuelle Bausteine

SDM

Maßnahmenkatalog

Der Maßnahmenkatalog zum SDM befindet sich noch in der Erarbeitungsphase. Die einzelnen Bausteine des Katalogs werden sukzessive veröffentlicht und zur Anwendung freigegeben.

Wir weisen ausdrücklich darauf hin, dass die hier veröffentlichten Bausteine noch nicht in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder abgestimmt worden sind. Wir empfehlen den Anwendern, ihre Erfahrungen bei der Erprobung der Bausteine den an der Entwicklung der Bausteine beteiligten Datenschutzbehörden mitzuteilen, und somit zur Weiterentwicklung von Methode und Maßnahmen beizutragen.

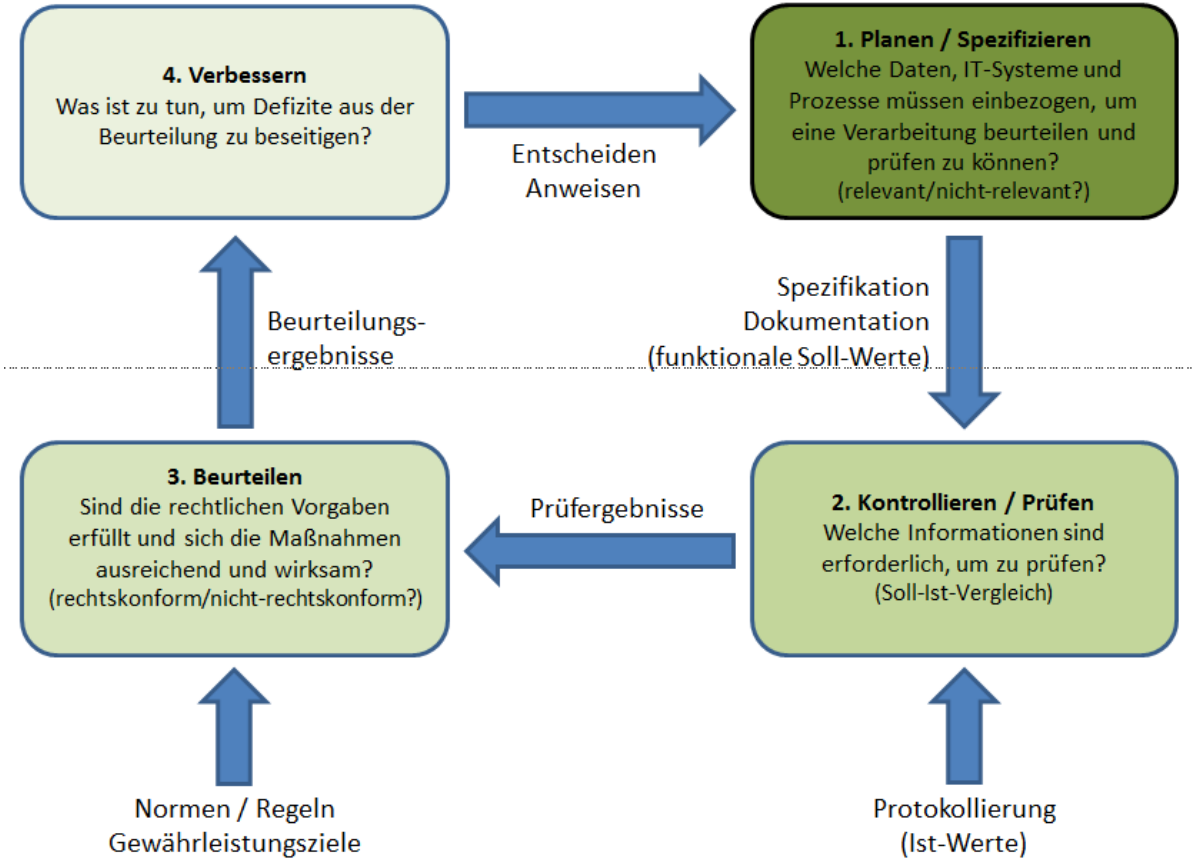
Bezeichnung	Format	Größe
Baustein 11 „Aufbewahrung“	PDF	0.52 MB
Baustein 41 „Planung und Spezifikation“	PDF	0.63 MB
Baustein 42 „Dokumentation“	PDF	0.61 MB
Baustein 43 „Protokollierung“	PDF	0.53 MB
Baustein 50 „Trennung“	PDF	0.63 MB
Baustein 60 „Löschen und Vernichten“	PDF	0.61 MB
Baustein 80 „Datenschutzmanagement“	PDF	0.84 MB

Newsletter

- Löschen
- Aufbewahrung
- Protokollierung
- Dokumentation
- Planung / Spezifikation
- Trennung
- Datenschutzmanagement

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

SDM als Framework für Datenschutz-Management gem. Art. 32 Abs. 1 lit. d DSGVO



1. Schutzmaßnahmen für relevante Verarbeitungskomponenten bestimmen und deren Prüffähigkeit spezifizieren. (*Plan*)

2. Prüfergebnisse anhand funktionaler Soll-Ist-Differenzen herstellen, die rechtlich beurteilt werden können. (*Do*)

3. Rechtliche Beurteilung von Prüfergebnissen erzeugen. (*Check*)

4. Aus rechtlichen Beurteilungen der Verarbeitung Veränderungsbedarfe formulieren und deren Umsetzung initiieren. (*Act*)

Der PDCA-Zyklus eines DSMS unterliegt seinerseits der Anforderung nach kontinuierlicher Verbesserung.

Quelle:
SDM-Baustein „Datenschutz-Management“

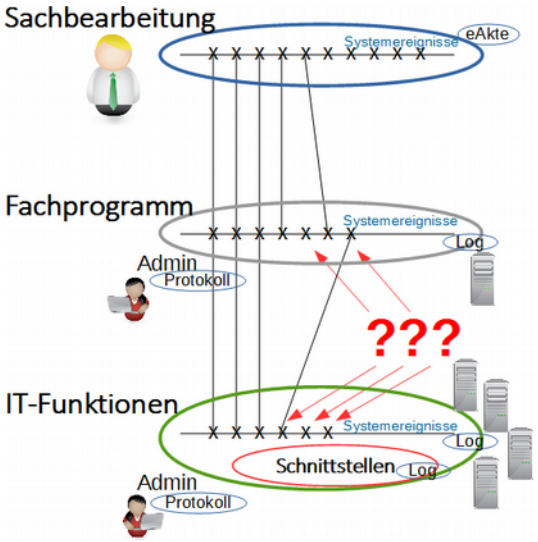
Referenz-Baustein „Löschen“

„Der Vorgang des Löschens muss auf irreversible Weise bewirken, dass aus den gelöschten Daten selbst mit verhältnismäßig hohem Aufwand keine Informationen über bestimmte oder bestimmbare Personen mehr gewonnen werden können. (…) Datenschutzrechtlich ist eine Löschung eines Datums erst dann vollzogen, wenn auch keine Kopie dieses Datums mehr bei dem Verantwortlichen oder einem möglichen Auftragsverarbeiter gespeichert ist.“

- Festlegen der Löschmethoden entsprechend Schutzbedarf
  - Überschreiben der Informationen einzelner Datenfelder, die auf elektronischen Datenträgern gespeichert wurden, mit Hilfe von Löschprogrammen (bspw. **Wipe-Tools**),
  - komplettes Überschreiben ganzer Datenträger mit speziellen Lösch- oder Anwendungsprogrammen (z.B. mit **Wear-Levelling-Algorithmen von Flashspeichern**)
  - Austragen aus elektronischen Verzeichnissen bzw. Tabellen bspw. durch Datenbank-Löschbefehle mit anschließender **Reorganisation der Datenbank**,
  - **physikalische Zerstörung** (Vernichtung) des Datenträgers (bspw. Papier, Festplatten, SSD-Speicher) durch mechanisches Zerkleinern (Schreddern), Einschmelzen oder Verbrennen.
- Hoher Schutzbedarf
  - Nutzung gesichert integrer Löschtools; standardisierte, transparente (spezifizierte., dokumentierte, protokollierte) Löschvorgänge auch für temporäre Dateien, Backups, Protokolleinträge.

Zweck und Ebenen der Protokollierung

- Setzt Transparenz-Anforderung der DSGVO zur Herstellung der Prüfbarkeit in der **Vergangenheit** um
- Zweck der Protokollierung: Feststellen, zu welchem Zeitpunkt welches Ereignis durch welche Entität ausgelöst wurde (→ **Wann, was, wer**?)



1. Die Aktivitäten der **Sachbearbeitung**;
2. die **Funktionen des Fachprogramms** für die Sachbearbeitung;
3. die **Administration des Fachprogramms**;
4. die **IT-Funktionen der Infrastruktur** (Hardware, Software)
   einer Organisation, auf denen die Fachprogramme aufsetzen (PCs, Server, virtuelle Systeme, Betriebssysteme, Middleware/DB, CPU-Cluster, SAN/NAS) - **Sonderfunktionalität**: Schutzmaßnahmen (Hashen, Verschlüsseln, Anonymisieren...);
5. die **Systemübertritte**, Übermittlung von Daten zu anderen Organisation(seinheit)en;
6. die **Administration der IT-Infrastruktur.**

7. Und ebenso ist zu **protokollieren**, ob ein ***Controlling*** all dieser Protokolle stattgefunden hat. (Erst dadurch kann der Nachweis der Wirksamkeit der Protokollierung und Maßnahmen erbracht werden.)

Protokollierung auf Ebene der Verarbeitung

- **Das Lesen von Daten** - Soweit gesetzlich keine vollständige Protokollierung kann eine selektive ausreichen;
- **Die Eingabe von Daten** - Eine Eingabeprüfung erfolgt grundsätzlich verarbeitungsorientiert (z. B. Protokollierung in Akten, soweit vorhanden, Protokollierung direkt im Datenbestand, sofern keine Akten geführt werden). Das Faktum, dass Daten eingegeben wurden, ist im Regelfall vollständig zu protokollieren.
- **Die Änderung von Daten** - ist im Regelfall vollständig zu protokollieren.
- **Das Sperren von Daten** - ist im Regelfall vollständig zu protokollieren.
- **Die manuelle Löschung von Daten** - ist im Regelfall vollständig zu protokollieren.
- **Die Übermittlung von Daten** - ist im Regelfall vollständig, unter Angabe der Rechtsgrundlage und einem Verweis auf den Vorgang oder das Aktenzeichen, im Protokoll zu protokollieren..
- **Die Benutzung eines automatisierten Abrufverfahrens** - ist im Regelfall vollständig zu protokollieren, unter Angabe der Gründe der Abrufe (Vorgang, Aktenzeichen etc.) .
- **Der Aufruf von Programmen** - Den Aufruf von Programm zu protokollieren kann erforderlich sein bei besonderen Programmen, die z. B. nur zu bestimmten Zeiten oder Anlässen und besonders ausgewiesenen Zwecken benutzt werden dürfen. In diesen Fällen ist grundsätzlich eine vollständige Protokollierung angezeigt.

Protokollierung bei hohem Schutzbedarf

- Abrufbarkeit aller Protokolldaten von **zentraler Stelle** aus und von **Backup & Restore** erfasst (*Verfügbarkeit*)
- Nachweis der Vollständigkeit der Protokolldaten mit hoch auflösendem, zertifiziertem **Zeitstempel und Signieren** der Daten, regelmäßige Übungen zur **Analyse von Protokolldaten** (*Integrität*)
- **Verschlüsseln** von Protokolldaten und Protokolldatentransport (*Vertraulichkeit*)
- Vollständige **Spezifikation, Dokumentation der** Daten (inlusive Auswertungsszenarien) und des Zugriffs (*Transparenz*)
- **Rollen- und Rechtekonzept** regelt bedingten Zugriff auf die Protokolldaten, Regelwerk für Zugriff durch externe Organisationen (*Nichtverkettung*)
- Protokolldaten neuer Verfahren(skomponenten) müssen sich leicht einbinden lassen (Testen!), fehlerhafte oder unverständliche Einträge müssen **annotiert** werden können, Protokoll-Datenbestände sind vollständig zu **löschen** (= wipen) (*Intervenierbarkeit*)

Empfehlungen

1. Aus der Schutzmaßnahme *Protokollierung* eine „Verarbeitung“ machen.
2. Komponenten: Protokollserver, Ticketsystem und Adminplattform

Referenz-Baustein „Planung / Spezifikation“

- Setzt Transparenz-Anforderung der DSGVO fzur Sicherung der Prüfbarkeit in der Zukunft um
- Zweck einer Planung: Alles relevanten Komponenten zusammenstellen und die Voraussetzung zur Prüfbarkeit der Funktionen und Schutzmaßnahmen der Verarbeitung schaffen
  - Erarbeitung einer umfassenden **Beschreibung der Verarbeitung**
  - Identifizieren des Verantwortlichen, der **Akteure und Betroffenen**
  - Sichten und ggfs. Erstellen der **Rechtsgrundlagen**
  - Erstellung eines datenschutzspezifischen **Angreifermodells**
  - Feststellung der **Risiken für die Betroffenen**
  - Formulieren der **funktionalen Anforderungen** an Verarbeitungsprozess und **Schutzmaßnahmen**
  - Erstellung eines **Berichts an den Verantwortlichen** planen
  - Erstellung eines **Konzepts (Projektplanung) zur Umsetzung der funktionalen Anforderungen (Lasten-/ Pflichtenheft)**
  - Begleitung der **Implementation der Schutzmaßnahmen**
  - Erstellung eines **Testkonzepts / Pilotkonzepts**
  - Erstellung des **Freigabeverfahrens**

Beschreibung einer Verarbeitung umfasst:

- Prozess der „**Fachlichkeit**“ mit den fachrechtlichen und datenschutz-rechtlichen Anforderungen
- die Nutzung einer **Fachapplikation** durch die Sachbearbeitung,
- die **Technik der Datenverarbeitung**, der Prozesse, IT-Systeme und IT-Infrastrukturen,
- die **Schnittstellen** von Prozessen und IT-Systemen sowie die jeweilige **Administration** der vorgenannten Ebenen.

Referenz-Baustein „Dokumentation“

- Setzt Transparenz-Anforderung der DSGVO in Bezug auf **Prüfbarkeit des aktuellen Betriebs** um
- Zweck einer Dokumenation: **Herstellung der Prüfbarkeit** einer Verarbeitung
  - Dokumentation ist Voraussetzung für Prüfbarkeit. Nicht gegebene Prüfbarkeit aufgrund einer mangelhaften Dokumentation verstößt gegen Transparenzgebot und kann bereits das Prüfergebnis (mit anschließender Sanktionierung) sein.
- Dokumentation muss alle relevanten Komponenten (Datenbestände, IT-Systeme und Prozesse) der Verarbeitung auflisten einschließlich des Ausweises der aus den normativen Soll-Anforderungen der DSGVO gewonnenen **funktionalen Soll-Anforderungen** und der Methode, mit der die funktionalen Soll-Werte erzeugt wurden und Ist-Werte gemessen werden, um **Prüfergebnisse für die rechtliche Beurteilung** zu erzeugen.
- **Formale Anforderungen** an eine Dokumentation:
  - Strukturierter Aufbau;
  - Orientierung am Datenschutzrecht, gerade bei technischen und organisatorischen Aspekten;
  - Sichern der Vollständigkeit (alles Relevante, wobei gezeigt werden muss, wie Klärung der Relevanz herbeigeführt wurde);
    - Sichern der Aktualität, Revisionsfestigkeit, gesicherte Fortschreibung, Inkraftsetzen

Referenz-Baustein „Aufbewahrung“

„Aufbewahrung“ beschreibt Maßnahmen zur Speicherung von personenbezogenen Daten, die zur Aufbewahrung in physikalischen Speichermedien (Datenträgern) über längere Zeiträume (Langzeitspeichersystem) erforderlich sind, um auf sie während des gesamten Aufbewahrungszeitraums zugreifen zu können. Es geht nicht um Datensicherungen, mit dem Ziel, Datenbestände bei Verlust wiederherstellen zu können (Backups).

Ebene Daten

M11.01 Inventur aller vorhandenen Daten-Formate vor der Aufbewahrung
M11.02 Festlegung geeigneter Datenformate für die aufzubewahrenden Daten
M11.03 Definition der signifikanten Eigenschaften der im Langzeitspeicher abzulegenden Dokument-Typen, ihrer zukünftige Ziel- oder Nutzergruppe sowie der Art der zukünftigen Verwendung
M11.04 Festlegung von Art, Umfang und Format der mit aufzubewahrenden Metadaten
M11.05 Festlegung aller Verifikationsdaten, die zum Erhalt des Beweiswertes von Daten mit aufbewahrt werden müssen

Ebene Systeme

M11.06 Ausdruck von aufzubewahrenden Daten auf Papier
M11.07 Aufbewahrung von Hard- und Softwarekomponenten für den Zeitraum der Aufbewahrung der damit ursprünglich verarbeiteten Daten
M11.08 Spezielle Zugriffsschutzmechanismen für Hard- und Softwarekomponenten, die nicht mehr dem Stand der Technik entsprechen
M11.09 Überführung aufzubewahrender Daten in neue digitale Repräsentationen
M11.10 Redundante Vorhaltung von Datenbeständen
M11.11 Räumlich verteilte Speicherung von Daten
M11.12 Parallele Nutzung unterschiedlicher Speichersysteme
M11.13 Regelmäßiges Ersetzen von Datenträgern (Refreshment)
M11.14 Regelmäßige Migration auf andere Speichersysteme
M11.15 Virtualisierungs- oder Emulationstechniken zum Erhalt der Lauffähigkeit veralteter Software

Ebene Prozesse

M11.21 Festlegung von Zuständigkeiten für alle Details der Aufbewahrung
M11.22 Definition der Kriterien für die Auswahl der technischen Systeme zur Erhaltung der Daten
M11.23 rechtzeitige Festlegung des Zeitpunktes der Konvertierung in das Aufbewah-rungsformat bzw. der Migration auf andere Speichersysteme
M11.24 Regeln zum Umgang mit versionierten Daten
M11.25 Prozesse für die Protokollierung jeder Formatkonvertierung und für die Prüfung der Protokolle
M11.26 Prozesse für die Protokollierung jeder Migration auf andere Speichersysteme und für die Prüfung der Protokolle

Referenz-Baustein „Trennung“

„Unterschiedliche Zwecke der Tätigkeiten erzeugen unterschiedliche Befugnisse zur Verarbeitung, die unterschiedliche Trennungsmaßnahmen erfordern. Diese zweckdefinierten Trennungsanforderungen, die typischerweise auf der organisatorischen Ebene formuliert werden, dürfen dann nicht von der Technik, die als Infrastruktur für die Datenverarbeitung genutzt wird, unterlaufen werden. Die Technik muss vielmehr diese Trennungsgebote unterstützen.“

6 Prüfschritte sind für eine Verarbeitung zu durchlaufen:

1) Prüfen ob ein **verfassungsrechtlich begründetes Trennungsgebot** besteht
2) Prüfen ob ein **zweckorientiert organisationsbezogenes Trennungsgebot** besteht
3) Prüfen der Anforderungen an eine **Übermittlung zwischen Mandanten**
4) Prüfen der Anforderungen an die **Abgeschlossenheit von Transaktionen** innerhalb eines Mandaten
5) Prüfe der Anforderungen an die **Unabhängigkeit von Konfigurationen** zwischen Mandanten
6) Prüfen der Anforderungen an eine **mandantenübergreifende Verwaltung** einer Datenverarbeitung

logische Trennungen:

- durch *Organisationsanweisung*;
- durch *parallel betriebene Instanzen innerhalb einer Applikation*;
- von Fachapplikationen, *parallel innerhalb eines Betriebssystems*;
- von Fachapplikationen, jeweils *eine Instanz in einem virtuellen Betriebssystem* auf einem gemeinsamen „Host“;

physikalische Trennung:

- von Fachapplikationen, in einem Betriebssystem auf einer *eigenen IT-Hardware* in einem gemeinsamen Rack eines Server-Raums über unterschiedliche Netze erreichbar;
- von Fachapplikationen, bei der jede Fachapplikation in einem Betriebssystem auf einer *eigenen IT-Hardware in unterschiedlichen Räumen eines Gebäude(komplexes) über unterschiedliche Netze* erreichbar betrieben werden;
- physikalische Trennung von Fachapplikationen, bei der jede Fachapplikation in anderen Rechenzentren (in unterschiedlichen Ländern), die bspw. spezialisiert für bestimme Verwaltungen („*kommunales Rechenzentrum*“) oder für spezielle Berufsgeheimnisträger („*Apotheken-Rechenzentrum*“).

Wie weiter? Referenzbausteine und Modellierungen

- Die **nächsten Referenz-Bausteine** in der Warteschlange sind:
  - Rollen und Berechtigungen
  - Datensicherung und Wiederherstellung
  - Auskunft
  - Berichtigung
  - Pseudonymisierung und Anonymisierung
- Erste **SDM-Modellierungen mit Verinice** liegen vor, für die Verwaltung in SH ist eine Modellierung mit **HiScout** (Werben mit SDM-Kompatibilität) vorgesehen.
- Wir führen eine Liste mit Toolherstellern und planen noch in diesem Jahr einen **Herstellerworkshop** (bisher Kontakt zu 10 Firmen und 2 Hochschulen).

SDM, V1.1

Wie weiter? Internationalisierung des Modells

- **Internationalisierung** des SDM
  - **englische Übersetzung** des SDM V1.0 ist seit einem halben Jahr verfügbar.
  - **spanische Übersetzung** des SDM V1.1 ist kurz vor Abschluss (auch wg. Export nach Südamerika)
- **Art. 29-Gruppe** kennt das DSFA-Framework (referenziert), zumindest das Konzept der Gewährleistungsziele ist bekannt, es ist aber weiterhin unklar, wie es mit dem SDM auf europäischer Ebene weitergeht.
- Viele Kollegen der Datenschutzaufsichtsbehörden (national / international) nutzen **ISO-Frameworks und -Maßnahmensammlungen**. Dabei ist es vollkommen ungeklärt, wie mit diesen die Anforderungen der *DSGVO berücksichtigt* werden können.
- Vielfach scheint es so, dass im Technikbereich das **Verständnis für Grundrechtseingriffe** („Risiko für Rechte und Freiheiten“) fehlt.

Zentraler Server für alle Informationen rund um das SDM:
https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Vielen Dank für Ihre Aufmerksamkeit!

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