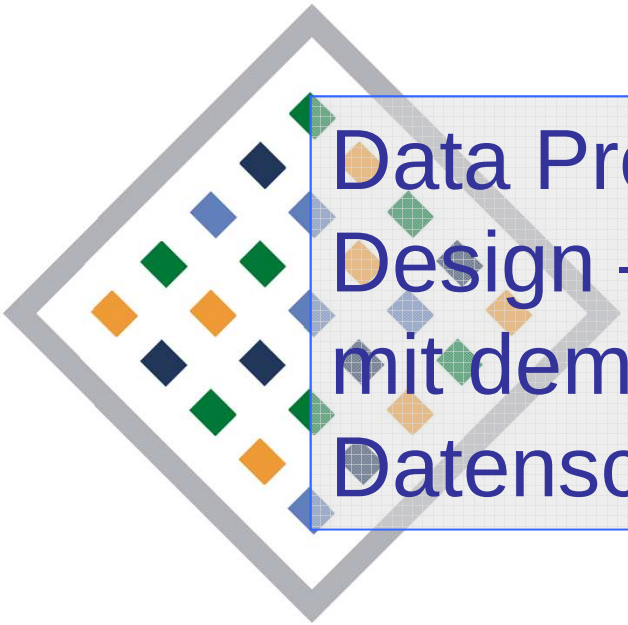
EAID-Workshop „Technologischer Datenschutz - Vorgaben der Datenschutzgrundverordnung“



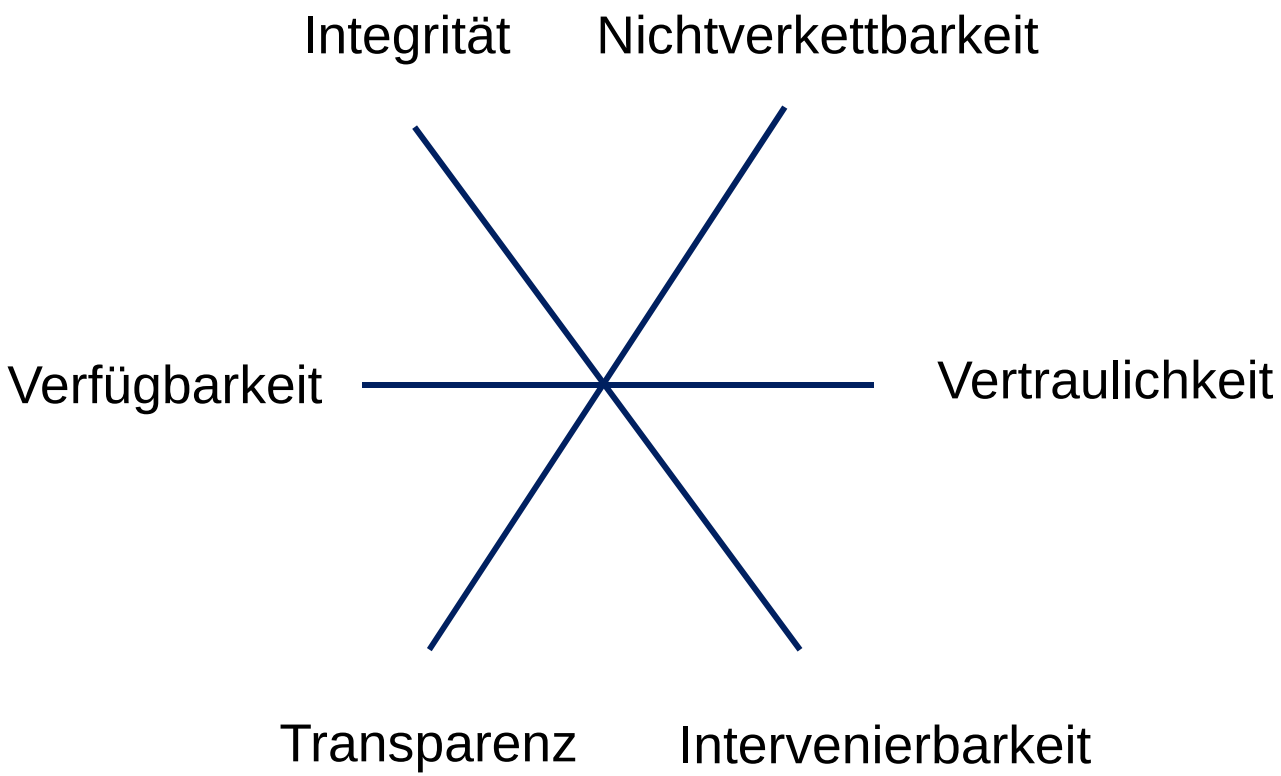
Data Protection by Design – Umsetzung mit dem Standard-Datenschutzmmodell

Gabriel Schulz
Stellvertreter
des Landesbeauftragten für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

68. Sitzung des AK Technik 15./16.02.2017


SDM
Standard-Datenschutzmodell

Systematisierung der Schutzziele (2009)



Standard-Datenschutzmodell

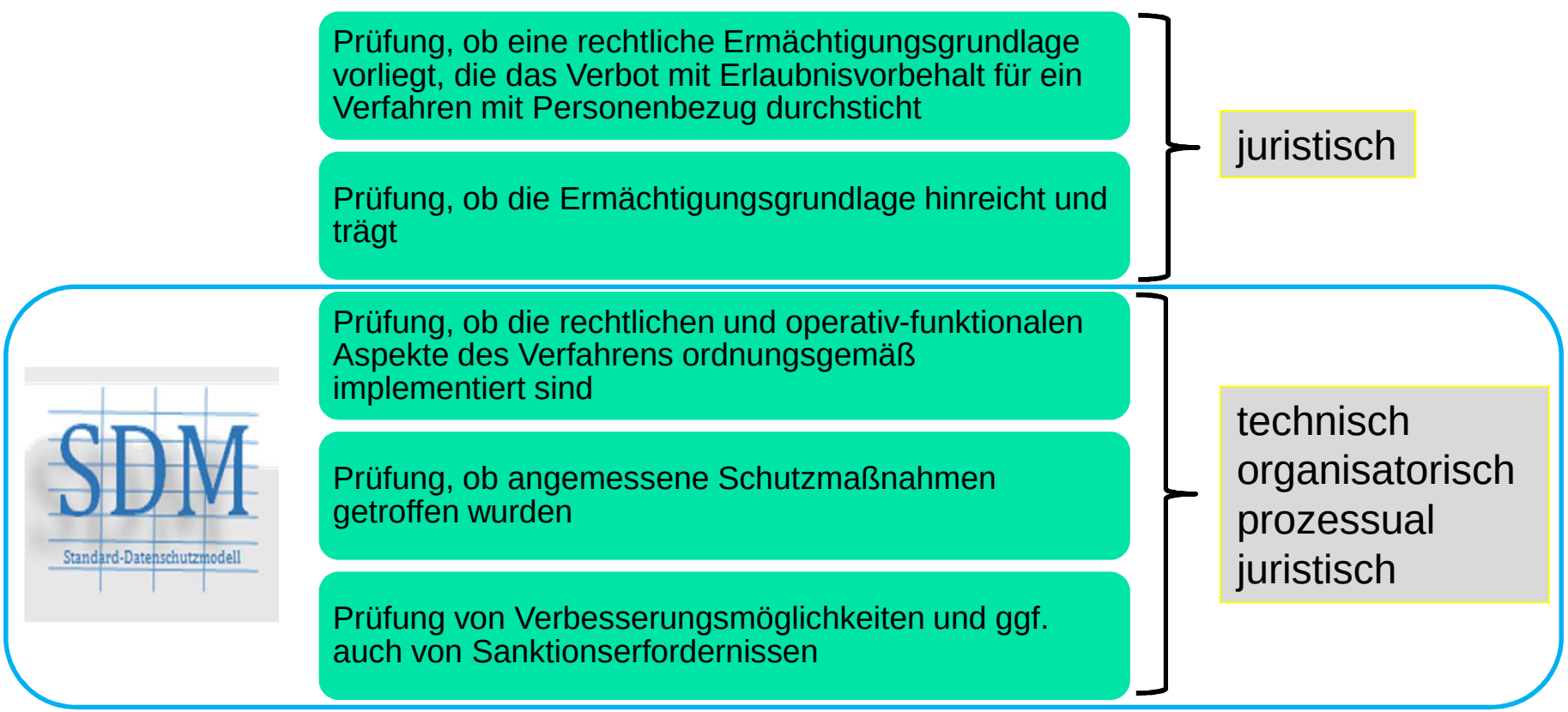
- Methode zur Datenschutzberatung und –prüfung auf der Basis der einheitlichen **Gewährleistungsziele**
  - Verfügbarkeit
  - Integrität
  - Vertraulichkeit
  - Nichtverkettung
  - Transparenz
  - Intervenierbarkeit

  - Datenminimierung

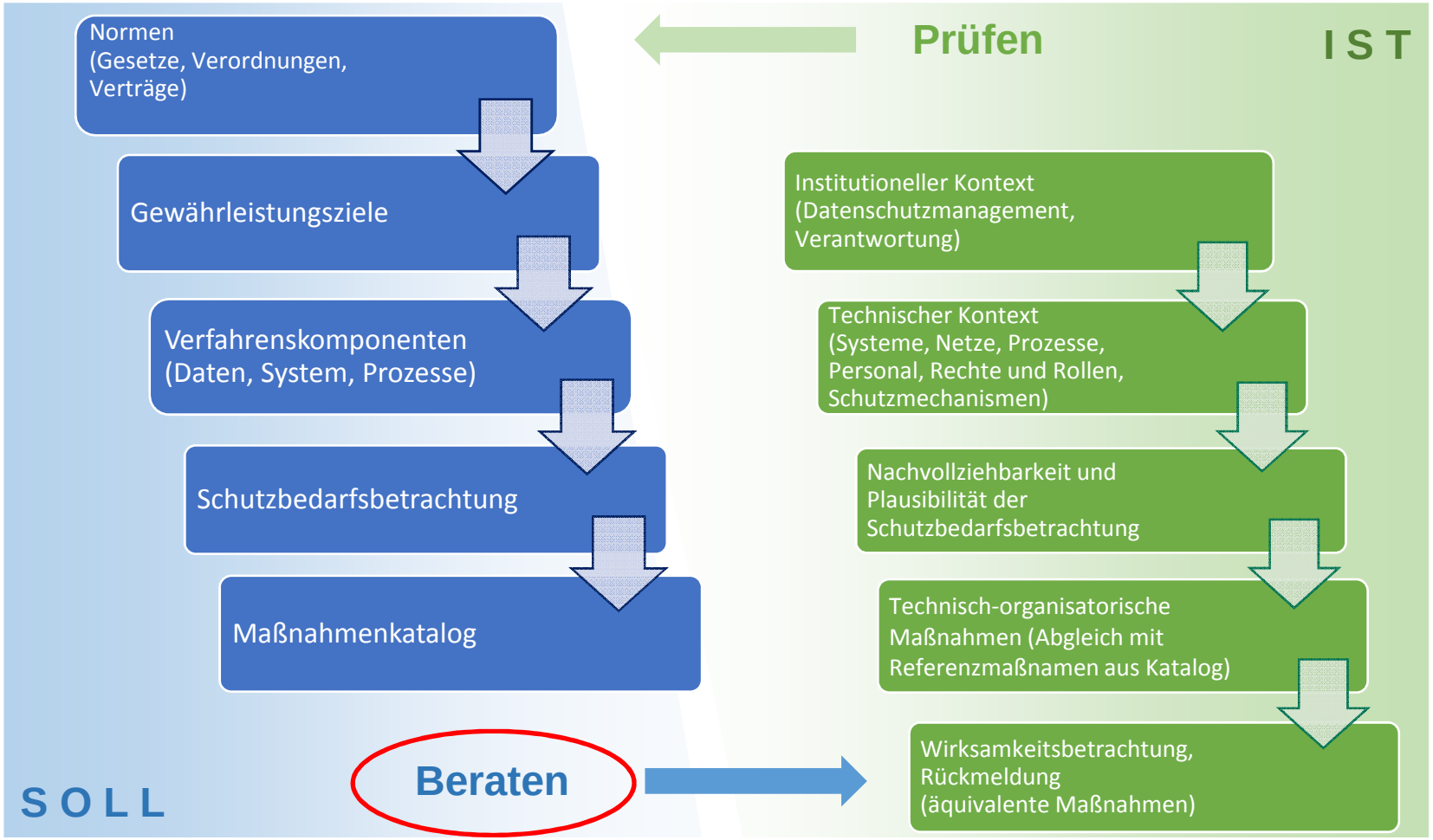
Gewährleistungsziele – wofür?

- Normen lassen sich nicht ohne Weiteres technisch operationalisieren, d. h. in technische Funktionen umsetzen.
- Wie kann der Jurist sichergehen, dass rechtliche Anforderungen tatsächlich technisch umgesetzt werden?
- Juristen und Techniker müssen ihre Anforderungen transformieren können!

SDM-Ablaufmodell



SDM-Ablaufmodell



Data Protection by Design
-
Umsetzung mit Hilfe des SDM

Prinzipien von Privacy by Design

Prävention statt nachgelagerte Abhilfe

Datenschutz per "Default"

Respektieren der Privatsphäre der Benutzer

Anwendung von sieben Grundprinzipien

Einbettung von Datenschutz und -sicherheit im Design

Sichtbarkeit und Transparenz

Schutz über den gesamten Lebenszyklus

Volle Funktionalität - eine Positivsumme, keine Nullsumme

Ann Cavoukian (ehemalige Informationsfreiheits- und Datenschutzbeauftragte der kanadischen Provinz Ottawa)

Vorgaben der DS-GVO (Art. 25)

Data Protection by Design / by Default

geeignete technische und organisatorische Maßnahmen

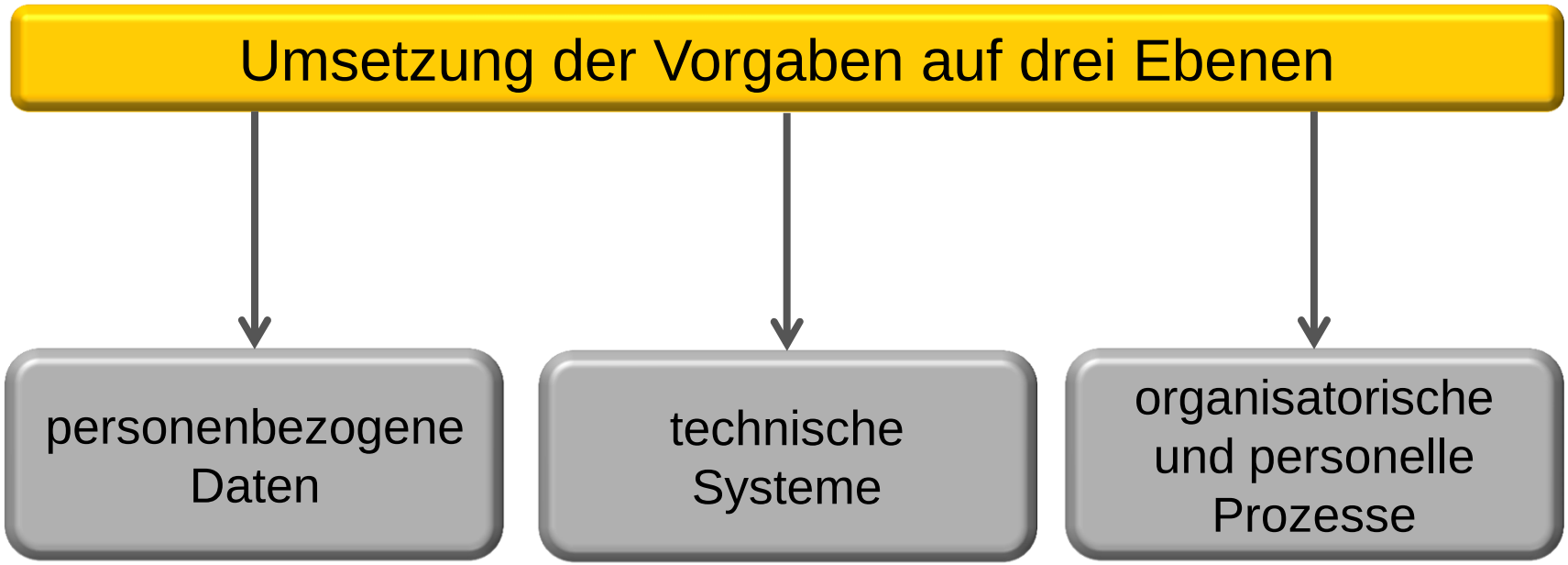
abhängig
- vom Stand der Technik
- von Implementierungskosten
- von Art, Umfang, Umständen und Zweck der Verarbeitung
- von Risiken für die Rechte und Freiheiten der Betroffenen

zum Zeitpunkt der Festlegung der Mittel

Spezifikation

zum Zeitpunkt der eigentlichen Verarbeitung

Umsetzung mit Hilfe des SDM



Orientierung an Gewährleistungszielen

Maßnahmen zur Umsetzung der Gewährleistungsziele müssen prüffähig frühzeitig für folgende Phasen geplant, spezifiziert, dokumentiert und protokolliert werden

- Spezifikation, Auswahl und Dimensionierung der Funktionalitäten
- Auswahl und Dimensionierung der Schutzmaßnahmen
- Implementierung, Installation, Konfiguration und Dokumentation der Funktionalitäten und Schutzmaßnahmen
- Planung von Tests und Freigaben mit anschließender befristeter Pilotierung des Verfahrens
- Planung der Kontrolle und Prüfung des laufenden Betriebs der Funktionen und Schutzmaßnahmen
- Möglichkeiten der Beurteilungen des laufenden Betriebs
- Anpassung der Sicherheit an den Stand der Technik
- Festlegungen für die Beendigung des Verfahrens

Orientierung an Gewährleistungszielen

Datenminimierung

- Reduzierung von erfassten Attributen Betroffener
- Reduzierung der Verarbeitungsoptionen
- Reduzierung der Kenntnisnahme vorhandener Daten
- Automatisierte Verarbeitungsprozesse, die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen
- Automatische Sperr- und Löschroutinen

Orientierung an Gewährleistungszielen

Verfügbarkeit

- Sicherungsverfahren für Daten, Prozesszustände, Konfigurationen, Datenstrukturen, Protokolle
- Dokumentation der Syntax von Daten
- Vertretungsregelung für Personal
- Redundanz von Hardware, Software, Infrastruktur
- Getestete Wiederherstellungsprozesse (Restore)

Orientierung an Gewährleistungszielen

Integrität

- technischer Integritätsschutz
  - elektronische Signaturen und Siegel
  - Prüfsummenverfahren
- Einschränkung von Schreib- und Änderungsrechten
- Soll-Definitionen für Prozesse und Tests auf Einhaltung
- Prozesse zur Aufrechterhaltung der Aktualität von Daten

Orientierung an Gewährleistungszielen

Vertraulichkeit

- Verschlüsselung beim Transport
- Verschlüsselung bei der Speicherung
- Rechte- und Rollenkonzept
- Eingrenzung der zulässigen Personals hinsichtlich Erforderlichkeit, Qualifikation, Zuverlässigkeit
- Authentisierungsverfahren

Orientierung an Gewährleistungszielen

Nichtverkettung

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
- Minimierung der Schnittstellen von Verfahren
- Trennung nach Organisations-/Abteilungsgrenzen
- Rollenkonzepte mit abgestuften Zugriffsrechten
- Zulassung nutzergesteuerten Identitätsmanagements
- Einsatz von Anonymisierungsdiensten, zweckspezifischen u. o. befristeten Pseudonymen, anonymen Credentials

Orientierung an Gewährleistungszielen

Transparenz

- Dokumentation von Verfahren (Prozesse, IT-Systeme, Daten, Datenflüsse, Schnittstellen, Tests, Freigaben…)
- Dokumentation von Einwilligungen und Widersprüchen
- Dokumentation von Unterrichtungen Betroffener
- Protokollierung von Zugriffen und Änderungen
- Nachweis der Quellen von Daten
- Versionierung

Orientierung an Gewährleistungszielen

Intervenierbarkeit

- Konzepte für Prozesse zur Einwilligung, Rücknahme, Widerprüche
- Konzeption für die Umsetzung der Betroffenenrechte
  - Löschen
  - Sperren
  - Auskunft
- Standardisierte Abfrage- und Dialogschnittstellen
- Single Point of Contact

Orientierung an Gewährleistungszielen

Ergebnis: Beurteilbarkeit eines Verfahrens

ein Verfahren muss so geplant und eingerichtet werden, dass

- nicht-regelkonforme Aktivitäten anhand
  - von Spezifikationen (und deren Tests),
  - von Dokumentationen und
  - von Protokolleinträgen

  zumindest im Nachhinein gesichert entdeckt werden können
- im Ergebnis rechtliche, funktionale, technische und organisatorische Mängel kontrolliert angezeigt, eskaliert und behoben werden können

SDM-Baustein Spezifikation

Ziel der Spezifikation:

- zum Zeitpunkt des Produktivsetzens durch den Verantwortlichen sollen relevante Anforderungen erfüllt sein
- für jede spezifizierte Anforderung bzw. Eigenschaft soll eine anzuwendende Prüfmethode ausgewiesen werden
- die datenschutzrechtliche Beurteilbarkeit eines Verfahrens soll sichergestellt werden

Was soll beurteilt werden?

- Funktionen, mit denen personenbezogene Daten erhoben, verarbeitet und übermittelt werden
- Wirksamkeit der Schutzmaßnahmen, die getroffen wurden

SDM-Baustein Spezifikation

Für welche Prüfinstanzen wird mit dem Baustein Spezifikation Transparenz hergestellt?

- für die Organisation selbst
- für die von den Aktivitäten der Organisationen unmittelbar betroffenen Personen
- für mögliche Auftragnehmer
- für die Fachaufsicht
- für die Aufsichtsbehörden

Ein erster Praxistest

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 Schulverwaltungssoftware 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 Datenverarbeitungsanlagen -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 Dienstvereinbarungen) - 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
			Geburtsdatum							
	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									

Der Landesbeauftragte für
Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern

Werderstraße 74a

19055 Schwerin

Telefon: 0385-59494-0

Telefax: 0385-59494-58

E-Mail: info@datenschutz-mv.de

Internet: www.datenschutz-mv.de
www.informationsfreiheit-mv.de
www.medienscout-mv.de