Schnittstellen zwischen Datenschutz und Informationssicherheit

Empfehlungen für Hochschulen

Dr. Mattis Neiling

stv. behördlicher Datenschutzbeauftragter

TU Berlin

Präsenztreffen des Netzwerks Hochschuldatenschutz
Frankfurt/Main, 9. Juni 2026

—

Bild: privat

Agenda

- Motivation (2)*
- Rahmenbedingungen und Beispielszenarien (3)
- Wie gelingt die Zusammenarbeit? (3)
- Schnittstellenprozesse (14)**
- Organisatorische Verankerung (Governance-Struktur) (3)
- Fazit (1)

—

*) Anzahl der Folien zu diesem Thema

**) insgesamt werden 12 Prozesse dargestellt - wir fokussieren auf 6 fundamentale

Motivation

—

Bild: privat

Problemstellung

> Datenschutz und Informationssicherheit ähneln sich nicht „zu sehr“, sondern verfolgen verschiedene Schutzziele

Datenschutz

- **schützt** Rechte und Freiheiten natürlicher Personen

Informationssicherheit

- **schützt** Informationen, Systeme und Prozesse **hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit**

—

Rechtliche Einordung: Art. 32 DSGVO - Sicherheit der Verarbeitung verbindet beide Bereiche unmittelbar.

Mögliche Risiken

- fehlende Zuständigkeiten, insb. bei Vorfällen
- Doppelprüfungen oder Lücken bei TOMs
- verspätete Einbindung von DSB und CISO
- parallele, inkonsistente Dokumentationen
- nicht verzahnte Risikoanalysen
- Unklarheit bei Audits und Nachweispflichten
- Mehrfachaufwände der Fachabteilungen durch unabgestimmtes Vorgehen

=> Synergien sollten genutzt werden

Rahmen-bedingungen

.

.

—

Bild: Willem van de Poll: Sachbearbeiter stempelt Dokumente. Lizenz: CC0, via Wikimedia Commons

Rahmenbedingungen für Datenschutz

DSB: unabhängige Beratungs-, Kontroll- und Überwachungsfunktion

- wird **frühzeitig eingebunden**
- ist **nicht operativ verantwortlich**
- vermeidet **Interessenkonflikte**
- wird durch **Datenschutzkoordination** unterstützt

Rahmenbedingungen für Informationssicherheit

CISO/ISB = Berichts- und Steuerungsfunktion

- verantwortet Sicherheitsgovernance & -prozesse
- übernimmt **koordinierende Funktion**
- priorisiert Maßnahmen

—

Hinweis: *Gesetzliche Vorgaben zur Benennung von ISB / CISO und für das Informationssicherheitsmanagement an Hochschulen sind je Bundesland unterschiedlich.*

Benchmark: Was Hochschulen tun

Typische Muster an Universitäten

- getrennte, aber **institutionalisiert zusammenarbeitende Rollen**
- eng verzahnte **Governance-Strukturen**
- keine vollständige organisatorische und personelle Verschmelzung
- gleichzeitige Einbindung von **DSB** und **CISO** in Projekte und IT-Verfahren

Gemeinsame Stabsstelle "Informationssicherheit und Datenschutz" schöpft Synergien (z.B. in Dresden, Jena, Koblenz und Siegen)

Wie gelingt die Zusammenarbeit?

—

Bild: privat

Ansatz: Kooperative Trennung

- **Datenschutz** und **Informationssicherheit** bleiben organisatorisch unterscheidbar
- Zusammenarbeit erfolgt über:
  - definierte Prozesse
  - feste Abstimmungsformate
  - verbindliche Governance
- keine „Mischzuständigkeiten“
- gemeinsame Zuständigkeit nur an klar definierten Schnittstellen (z.B. bei TOMs)

Leitidee: **Getrennte Verantwortung, verbindliche Zusammenarbeit**

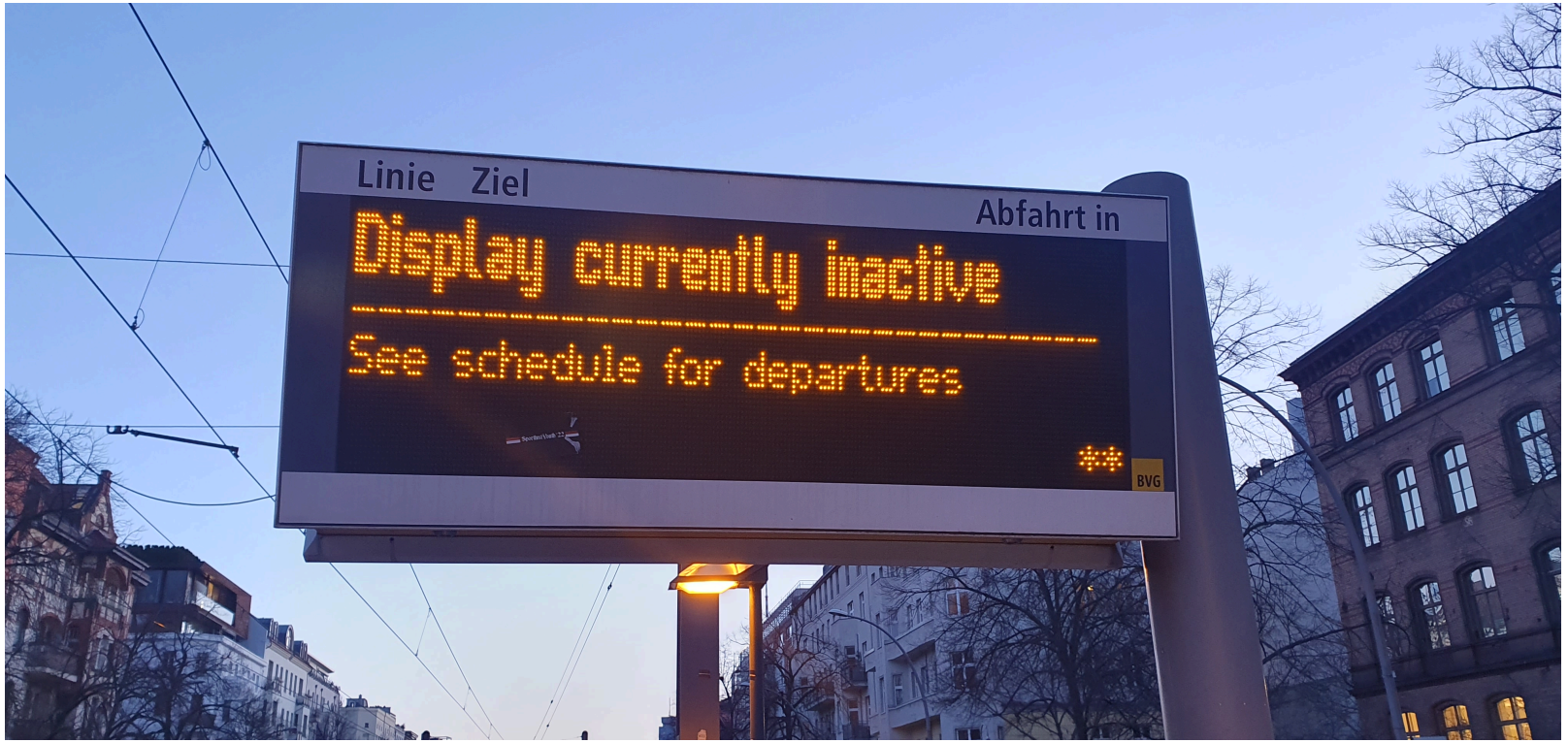
Überblick der Rollen und ihrer Kernaufgaben

Funktion	Kernaufgabe
Behördlicher DSB	unabhängige Beratung und Überwachung
Datenschutzkoordination	operativer Datenschutz und Verankerung
CISO / ISB	Aufbau und Steuerung der Informationssicherheit
CIO, DO, IT, SOC/CERT …	operative Umsetzung und Steuerung
Rechtsabt., Fakultäten u.a.	fallbezogene Beteiligung

Abgrenzung von Aufgabenbereichen

Themenfeld	Datenschutz	Informationssicherheit
Rechtsgrundlagen / Zulässigkeit	**federführend**	unterstützend
Betroffenenrechte	**federführend**	-
ISMS / Sicherheitsstrategie	beratend	**federführend**
TOMs	**federführend**	unterstützend
DSFA	**federführend**	unterstützend
IS-Risikoanalyse	einzubeziehen	**federführend**
Sicherheitsvorfälle	zu informieren	**federführend**
Datenschutzvorfälle	**federführend**	zu informieren

Zentrale Schnittstellenprozesse



—

Bild: privat

Zentrale Schnittstellenprozesse (erste Halbzeit)

1. Datenschutz- und Sicherheitsvorfälle
2. Technische und organisatorische Maßnahmen (TOMs)
3. Audits
4. Risikoanalysen
5. Notfallmanagement und Krisenkommunikation
6. Tools für ISMS- und DSMS-Nachweispflichten

=> Fokus des Vortrags liegt auf den "Top 6"

Zentrale Schnittstellenprozesse (zweite Halbzeit)

7. Projekte und Beschaffungen
8. Logfiles und Forensik
9. Privacy & Security by Design
10. Business Continuity Management (BCM)
11. Betroffenenanfragen
12. ?

=> Fokus des Vortrags liegt auf den "Top 6"

1. Datenschutz- und Sicherheitsvorfälle (1)

> **Nicht jeder Sicherheitsvorfall ist ein Datenschutzvorfall!**

Aber:

- viele Datenschutzverletzungen gehen aus Sicherheitsvorfällen hervor
  (aber nicht alle; d.h. einige Vorfälle ohne Beteiligung des ISB)

—

Bild: privat

1. Datenschutz- und Sicherheitsvorfälle (2)

Zweistufiger Prozess

> **1.** Erkennung und Analyse durch Informationssicherheit sowie Zuarbeit und Schadensminimierung durch die IT

> **2.** Bewertung, ob eine Verletzung des Schutzes personenbezogener Daten vorliegt und ob eine Meldung nach Art. 33 DSGVO erforderlich ist

Empfehlung:

- gemeinsamer Incident-Workflow mit Pflichtbeteiligung des DSB bei Sicherheitsvorfällen bei möglichem Personenbezug
- Aufbau eines Computer Emergency Response Teams (CERT)

2. Technische und organisatorische Maßnahmen

Die TOMs sind der klassische Überschneidungsbereich

- Art. 32 DSGVO verlangt angemessene Maßnahmen
- Datenschutz durch Technikgestaltung sollte früh in Prozesse und Systeme integriert werden (vgl. Art.-25-Leitlinien / EDPB)
- ISO 27001 & BSI-Standards können zur methodischen und technischen Ausgestaltung herangezogen werden

Empfehlung:

- Datenschutz formuliert Anforderungen und Prüfkriterien
- Informationssicherheit steuert Sicherheitsvorgaben bei

3. Audits

- regelmäßige Überprüfung (max. innerhalb von drei Jahren):
  - Datenschutzkonformität aller Verarbeitungstätigkeiten
  - Gewährleistung der Sicherheitsanforderungen aller Geschäftsprozesse und Systeme
  - Vollständigkeit und Korrektheit der Dokumentation

> **Die Arbeitsbelastung der Fachabteilungen und Bereiche sollte leistbar sein!**

Empfehlung:

- Audits methodisch auf Grundlage der ISO-Standards abstimmen
- Datenschutz- und Informationssicherheitsaudits gemeinsam durchführen
- Termine langfristig abstimmen

4. Risikoanalysen

Datenschutz-Folgenabschätzung (DSFA) vs. Informationssicherheits-Risikoanalyse (ISRA)

- **DSFA bewertet Risiken für Rechte und Freiheiten natürlicher Personen**
- **ISRA bewertet Bedrohungen für Informationen, Systeme und Prozesse**
- BSI 200-3 und die DSK-Kurzpapiere zur DSFA stützen die Trennung

Empfehlung:

- ähnlich strukturierte Templates nutzen, enge methodische Verzahnung
  - Berücksichtigung der unterschiedlichen Perspektiven
  - abgestimmte, aber getrennte Durchführung der Analysen
- analoges Vorgehen für Grundrechte-Folgenabschätzung entspr. KI-VO u.a.

5. Notfallmanagement und Krisenkommunikation

- **TU Berlin Hackerangriff in 2021:** die TU blieb handlungsfähig!
  - Krisenmanagement war gut aufgestellt:
    Krisenteam auf Leitungsebene und operativ handelnde Teams
  - externer Dienstleister wurde zur Unterstützung engagiert

Empfehlung:

- Schaffung geeigneter Strukturen, die im Krisenfall abgerufen werden können
- Etablierung einer Task Force „Notfallmanagement und Krisenkommunikation“
- Rahmenvertrag mit Dienstleister für Abruf von Services bei Bedarf

6. Tools für ISMS- und DSMS-Nachweispflichten (1)

> **Ziel:** Implementierung einer weitgehend integrierten und damit ressourcensparenden übergreifenden technischen Lösung

- ISMS & DSMS organisatorisch aufeinander abstimmen
- keine Mehrfacherfassung von Informationen zu Geschäftsprozessen und Verarbeitungstätigkeiten
- Sicherstellung von Integrität, Konsistenz und Aktualität

6. Tools für ISMS- und DSMS-Nachweispflichten (2)

Empfehlung:

- ISMS und DSMS aufeinander abstimmen, idealerweise ein „integrierendes Tool“ auswählen
- weitere Datenbestände einbeziehen, z.B. Betriebskonzepte und Systemdokus
- Zusammenführung von Daten mittels Programmierschnittstellen (APIs)
- „One-Stop-Shop-Systematik“ prüfen/umsetzen

Zentrale Schnittstellenprozesse (zweite Halbzeit)

7. Projekte und Beschaffungen
8. Logfiles und Forensik
9. Privacy & Security by Design
10. Business Continuity Management (BCM)
11. Betroffenenanfragen
12. ?

7. Projekte und Beschaffungen

> Datenschutz und Informationssicherheit werden von Anfang an mitgedacht

Empfehlung:

- Prozesse und IT-Systeme werden schrittweise eingeführt und laufend bewertet
- Verpflichtende frühzeitige Einbindung von CISO und DSB in alle IT-Projekte und Beschaffungsprozesse
- Ermöglicht Beschleunigung der Beteiligungsverfahren mit den Personalräten („**Stellungnahmen werden bereitgestellt**“).

8. Logfiles und Forensik

> Um Angriffe auf die IT abwehren und nachträglich untersuchen zu können, sind Logfiles und ihre Auswertung fundamental.

Empfehlung:

- klare Vorgaben für Löschfristen von und Zugriffsrechte auf Logfiles implementieren
- Zugriffe protokollieren
- DSB und CISO bei forensischen Untersuchungen immer einbeziehen

9. Privacy & Security by Design

- Beschränkung auf notwendige Daten (sowohl Umfang als auch Speicherdauer)
- durchgängige Umsetzung von
  - Löschkonzepten
  - Zugriffs- und Berechtigungsmanagement
  - angemessenen (IT-)Sicherheitsmaßnahmen
- Schutzklassen für Informationskategorien festlegen und praxistauglich anwenden

Empfehlung:

- gemeinsames Herzstück der Sicherheitsarchitektur
- Leitfaden / Checklisten entwickeln

10. Business Continuity Management (BCM)

> dauerhafte Verfügbarkeit von Daten und Systemen sichern

Empfehlung:

- Bildung einer Task Force „Business Continuity Management“
- Zusammenarbeit mit anderen HS, z.B. auf Landesebene
- Strukturen etablieren und geeignete Maßnahmen umsetzen, z.B.
  - Security Operations Center (SOC) mit 24/7 Support
  - Verankerung von Sicherheitsmanagement in den (IT-)Bereichen

11. Betroffenenanfragen (last but not least)

- Betroffenenanfragen sind primär ein Datenschutzprozess
- Unterstützung durch Fachabteilungen und IT für Auszüge aus den Systemen
- Kurzpapiere der Datenschutzkonferenz (DSK) bieten Auslegungshilfe für die Umsetzung

Empfehlung:

- Federführung beim Datenschutz (DS-Koordination)
- Zuständigkeiten und Vorgehensweisen festlegen, z.B.
  - Wer macht wann was?
  - Standard Operating Procedures (SOP)
  - Dokumentation

12.

?

12.

> **HIER könnte ihr Schnittstellenprozess stehen!**

z.B.

- Beratung und Schulung
- Kommunikation & Öffentlichkeitsarbeit
- QM/Zertifizierung (über Audits hinaus)
- Operationalisierung
- …

Organisatorische Verankerung (=Governance-Struktur)

.

.

.

—

Bild: privat

Empfohlenes Rollenmodell

- **DSB** mit unabhängiger Kontroll- und Beratungsfunktion
- **Datenschutzkoordination** ist im operativen Tagesgeschäft aktiv
- **CISO** übernimmt Aufbau und Weiterentwicklung des ISMS
- **SOC/CERT** unterstützt operative Incident-Steuerung
- **CIO, IT, Recht, Fakultäten** werden strukturiert eingebunden

Dreistufiges Governance-Modell

1. Operative Ebene

- regelmäßiges **Jour Fixe CISO + DSB** (ggf. auch CIO, DS-Koordination, IT, ...)
- Fallsteuerung für Projekte, Vorfälle und Prüfungen

2. Fachlich-strategische Ebene

- **Governance-Runde** mit: DSB, CISO, CIO, IT (ggf. Rechtsabteilung)

3. Eskalation und Risikoabwägungen

- über jeweilige **Leitungsebene**
  (Hochschulleitung, CIO oder zuständige Führungskraft)

Eskalationslogik

Empfehlung

1. Abstimmung in regelmäßigem **Jour Fixe** und bei Arbeitstreffen
2. Fachliche Konflikte in der **Governance-Runde** lösen
3. Risiko- oder Zielkonflikte über **CIO / Leitungsebene** klären

Prinzip

- operativ so viel wie möglich klären
- Konflikte strukturiert eskalieren
- Verantwortung der Leitung bei Risikoabwägungen sichern

Fazit

.

.

.

—

Bild: privat

Fazit: Modell der kooperativen Trennung

- klare Verantwortlichkeiten und Rollen
- definierte Schnittstellen
- verbindliche Governance

—

> Entscheidender Erfolgsfaktor ist nicht nur die personelle Ausstattung, sondern vor allem die Fähigkeit, die Zusammenarbeit auf Ebene von Prozessen und Governance verbindlich zu regeln.

Habe fertig.

Diskussion (= „Reden hilft“)