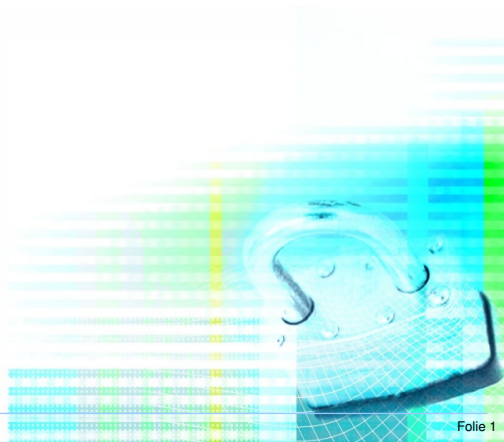


Schulung zu Datenschutz-Koordinatoren

RA Dr. Jan K. Köcher, Dipl.-Inf. Michel Gerdes

DFN-CERT Services GmbH

19. Dezember 2017



Agenda

Block I – Einführung in den Datenschutz
Übungsaufgabe

Block II – Dokumentation von Verfahren

Block I – Einführung in den Datenschutz

Europäisches Grundrecht

- Europäische Menschenrechtskonvention
 - Achtung Privat- und Familienleben, Wohnung und Korrespondenz
 - Recht am eigenen Bild
 - Auftritt in der Öffentlichkeit
- EU-Grundrechte-Charta
 - Achtung Privat- und Familienleben, Wohnung und Korrespondenz
 - Schutz personenbezogener Daten
 - Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
 - **Diese Daten dürfen** nur nach Treu und Glauben **für festgelegte Zwecke** und **mit Einwilligung** der betroffenen Person **oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage** **verarbeitet werden.** ...

Datenschutz-Grundverordnung

- Europaweite Vereinheitlichung der Vorgaben zum Datenschutz
- Grundverordnung
- Anwendungsvorrang
- 25.05.2016: In Kraft getreten
25.05.2018: Anzuwenden
- Eckpunkte:
 - Verbot mit Erlaubnisvorbehalt
 - Sachlicher Anwendungsbereich
 - Räumlicher Anwendungsbereich (Marktortprinzip)
 - Öffnungsklauseln

Gesamtverantwortung: Hochschulleitung

Verantwortlicher für Verarbeitung

- Verantwortung für Rechtmäßigkeit der Verarbeitung
- Beratung durch Datenschutz-Koordinator, Rechtsabteilung und/oder DSB

Datenschutz-Koordinatoren

- Beratung Verantwortliche für Verarbeitungen
- Verarbeitungen in ihrem Bereich
- Unterstützung bei Umsetzung der Anforderungen.

Datenschutzbeauftragte

- Kontrolle Einhaltung des Datenschutzes
- Beratung Verantwortliche für Verarbeitungen und Datenschutz-Koordinatoren bei der Umsetzung der Anforderungen
- Ansprechpartner für DS-Aufsichtsbehörden.

Informationssicherheitsbeauftragte

- Beratung Hochschulleitung und Verantwortliche für Verarbeitungen
- im Hinblick auf die sichere Verarbeitung personenbezogener und insbesondere organisationskritischer Daten.

Personenbezug

- NEU: Nach der DSGVO reicht die indirekte Identifizierbarkeit für Personenbezug aus
- Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.
- Nähere Beschreibung anonyme Daten in Erwägungsgrund 26.
- Faktische Anonymität: Personenbezug ist nur mit unverhältnismäßig viel Aufwand an Ressourcen herstellbar.
 - Empfehlung: Bei faktischer Anonymität im Zweifel von Personenbezug ausgehen oder DSB einbeziehen.

Anonymisierung:

- Name, Vorname, Geburtsdatum, ...
- Matrikelnummer, Personalnummer
- Kombination von Merkmalen
- Gruppengröße

Pseudonymisierung:

- Matrikelnummer
- Personalnummer
- Pseudonymtabelle

Gefährdung und Schutzbedarf personenbezogener Daten

normal

Mindestschutzbedarf, da jede Verarbeitung von personenbezogenen Daten einen Grundrechtseingriff darstellt

sehr hoch

Existenzielle Abhängigkeit von Eingriffsintensität

hoch

- Nicht veränderbare Daten
- Eindeutig identifizierende Daten
- Gesetzlich verankerte Intransparenz
- mögliche gravierende, finanzielle Folgen
- Auswirkungen auf Reputation/Ansehen der Betroffenen
- Auswirkungen auf körperliche Unversehrtheit
- Auswirkungen auf Grundrechtsausübung
- Gefahr der Diskriminierung oder Stigmatisierung
- Eingriffe in besonders geschützten inneren Lebensbereich

Kumulation:

- Erkenntnisgewinn durch sehr viele Daten → Überwachung
- Umfangreiche Rechte durch Bearbeiter → Zusammenführung möglich

Besondere Kategorien

- Ethnische oder rassische Herkunft
- politische Meinung
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetische oder biometrische Daten
- Gesundheitsdaten
- Daten zum Sexualleben oder sexuellen Orientierung

Daten zu Straftaten

Datenverarbeitung mit personenbezogenen Daten zu Straftaten oder strafrechtlichen Verurteilungen benötigt explizite Erlaubnisnorm in nationalem Gesetz

Schutzbedarf

- Verarbeitung verboten
- Explizite Erlaubnisnormen

Spezielle Daten

- Recht am eigenen Bild
- Fernmeldegeheimnis

Verarbeitung

- 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

Betroffene Vorgänge

- Automatisiert Verarbeitungen unter vollständiger oder teilweise Zuhilfenahme von Informationstechnologie (EDV)
- Nichtautomatisiert Manuelle, händische Verarbeitungsvorgänge, die ohne EDV erfolgen: Akten; Anforderung: Organisiert in Dateisystem

Datei(system)

jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob [...] [wie] geordnet geführt wird;

Verfahren & Zweck

Verarbeitung (Verfahren)

- eine formalisierte, wiederholbare Folge der Schritte der Datenverarbeitung zur Umsetzung einer Fachaufgabe bzw. eines Geschäftsprozesses.
- Das/Die Mittel, wie das Ziel erreicht wird
- Gekennzeichnet durch Zweckbestimmung und Abgrenzung zu anderen Verfahren hierüber.

Wichtig

Nicht jede Excel-/Word-Datei dokumentieren

Zweck

- Das Ziel des Verfahrens/der Verarbeitung
- Warum wird die Datenverarbeitung durchgeführt?
- Was soll mit der Datenverarbeitung erreicht werden?

Abrenzung zu IT-Verfahren

- Ein IT-Verfahren kann einer Verarbeitung entsprechen,
- üblicherweise können mit einem IT-Verfahren mehrere Verarbeitungen erfolgen;
- Und für eine Verarbeitung können mehrere IT-Verfahren angewendet werden.

Festlegung Zweck

Abstrakter

- Mehr Verarbeitungen je Zweck
- Problem: Feinheiten der Verarbeitungen auflösen/dokumentieren

Zweckbestimmung

- Bündelung zusammengehörige Zweckverfolgungen zu höherem Zweck
- Wesentliche Zweckverfolgung muss erkennbar bleiben

Konkreter

- Mehr Verfahren zu dokumentieren und zu pflegen
- Übersichtlichkeit geht u.U. verloren
- Mehrfacherfassung von Daten

Zweckänderung

- Zweck vereinbar mit Ursprungszweck:
 - Erlaubnistatbestand
 - Einziger wirklicher Anwendungsfall: wissenschaftliche Forschung und Statistik
- Zweck nicht vereinbar mit Ursprungszweck:
 - Explizite Rechtsgrundlage oder Einwilligung der betroffenen Person erforderlich
 - Verarbeitung muss als eigenes Verfahren dokumentiert werden.

Rechtmäßigkeit der Verarbeitung

Grundsätze

- Gesetzeskonforme Verarbeitung
- Faire Verarbeitung
- Verarbeitung soll transparent gegenüber der betroffenen Person sein
- Verbot mit Erlaubnisvorbehalt
- Orientiert sich am Zweck der Verarbeitung
- Personenbezogene Daten dürfen grundsätzlich nur für den Zweck verarbeitet werden, für den sie ursprünglich erhoben wurden.

Rechtmäßigkeit

- a) Einwilligung der betroffenen Person
- b) Vertrag oder Vorbereitung eines Vertrags mit der betroffenen Person
- c) Erfüllung rechtlicher Verpflichtung des Verantwortlichen
- e) Wahrnehmung öffentlicher Aufgabe oder Ausübung öffentlicher Gewalt
- f) berechnigte Interessen des Verantwortlichen oder Dritten, sofern Interessen der betroffenen Person überwiegen

Besondere Verarbeitungskontexte

Personal-/Mitarbeiterdatenschutz

Beachtung mögliche Einbeziehung Personalrat

Wissenschaftliche und historische Forschung

Datenverarbeitung privilegiert

Administration

Besondere Zugriffsmöglichkeiten mit strenger Zweckbindung

Block I – Einführung in den Datenschutz

→ Übungsaufgabe

Aufgabe 1 – Zweckbestimmung

Aufgabenstellung (15 Minuten)

Definieren Sie bis zu drei Zwecke aus Ihrem alltäglichen Arbeitsumfeld anhand der nachfolgenden Tabelle

Nr.	Name der Verarbeitung	Zweckbestimmung	Begründung für Zweck	Ab-/Begrenzung	Begründung für Ab-/Begrenzung

Aufgabe 1 – Zweckbestimmung

Aufgabenstellung (15 Minuten)

Definieren Sie bis zu drei Zwecke aus Ihrem alltäglichen Arbeitsumfeld anhand der nachfolgenden Tabelle

Nr.	Name der Verarbeitung	Zweckbestimmung	Begründung für Zweck	Ab-/Begrenzung	Begründung für Ab-/Begrenzung
1	Studierendenverwaltung	Verwaltung von Studierenden	Eigenes Verfahren	Kein Bewerbermanagement, keine Prüfungsverwaltung	Andere Zwecke
2	Zeiterfassung	Erfassung der geleisteten Dienstzeiten	Eigenes Verfahren, da als Ergebnis nur relevant, ob Dienstzeit erfüllt	Keine Personalverwaltung	Andere Zwecke
3	Urlaubsantrag	Verwaltung von Anträgen auf Urlaub	Antrag, Genehmigung und Verbuchung	Keine Personalverwaltung	Anderer enger Zweck

Block II – Dokumentation von Verfahren

Vortragende, Kontaktpersonen

DFN-CERT Services GmbH

<https://www.dfn-cert.de/>

RA Dr. Jan K. Köcher

Syndikus, Prokurist

Datenschutzauditor

koecher@dfn-cert.de

Dipl.-Inf. Michel Gerdes

Senior Consultant, GDDcert.

Datenschutzbeauftragter

gerdes@dfn-cert.de