Die Datenschutzreform an Hochschulen Strategische Entscheidungen

Johannes Nehlsen

Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen
c/o Rechenzentrum Universität Würzburg

Die Reform im Vergleich

BayDSG (alt)	DSGVO und BayDSG (neu)
Meldepflichten nur im TMG (und TKG)	Meldepflichten bei allen Vorfällen
Informationspflichten auf Webseiten (Datenschutzerklärung, Cookies …)	Informationspflichten zu jeder Verarbeitungstätigkeit Erste Ebene Name und Kontaktdaten des Verantwortlichen Kontaktdaten des Datenschutzbeauftragten Zwecke und Rechtsgrundlagen der Verarbeitung Empfänger oder Kategorien von Empfängern Übermittlung von personenbezogenen Daten „an ein Drittland“ Zweite Ebene Dauer der Speicherung der personenbezogenen Daten Betroffenenrechte Widerrufsrecht bei Einwilligung Pflicht zur Bereitstellung der Daten Sonderfall
Informationspflichten bei elektronischen Einwilligungen	
Knappe Informationspflichten bei schriftlichen Einwilligungen	
Verschuldensunabhängiger (nur) materieller Schadensersatzanspruch	Auch immaterieller Schadensersatz Beweispflicht im wesentlichen beim Verantwortlichen
Maßnahmenorientiere Datensicherheit	Risikoorientierte Datensicherheit
Freigaben und Verfahrensverzeichnisse mit Ausnahmen • Vorübergehend erstellte Daten • Interner Verwaltungsablauf • Ausschließlich zu Zwecken der Datensicherung und Datenschutzkontrolle • Wenn eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen unwahrscheinlich ist	Verzeichnis von allen Verarbeitungstätigkeiten Datenschutzfolgeabschätzung bei Bedarf

Persönlichkeitsrecht

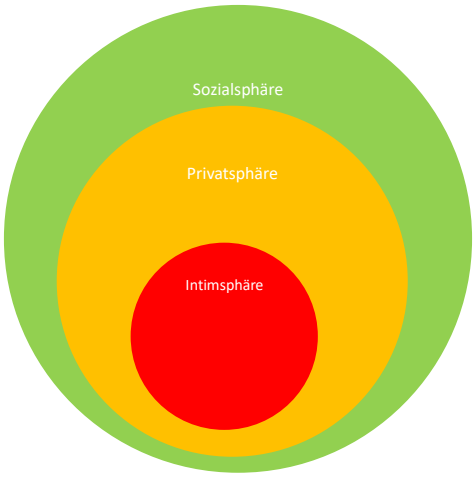
Beispiel für einen Sonderfall

„Momenten der Entspannung oder des Sich-Gehen-Lassens außerhalb der Einbindung in die Pflichten des Berufs und Alltags“ BVerfGE 120, 180, 207

Wem gebe ich meine Telefonnummer?

Farblegende

Farben geben den Umfang „Freiraum“ für mögliche Eingriffe wieder



Informationelle Selbstbestimmung

- Unterfall des Persönlichkeitsrecht
- Entscheidungsfreiheit
- Mehr Information und Transparenz, wenn Wahlfreiheit nicht besteht oder höhere Risiken bestehen

Personenbezogene Daten

- Informationen von Identifizierte Personen
- Informationen über identifizierbare Personen
- Pseudonyme Daten sind nicht Anonyme Daten
- Anonyme Daten
  ➔ Datenschutzrecht nicht anwendbar,
  außer die Anonymisierung ist ein Verarbeitungsschritt

EuGH Urteil vom 19.10.2016 C-582/14

Wann endet der Personenbezug von Daten?

- sehr hoher personeller Aufwand …
- sehr hoher wirtschaftlicher Aufwand …
- praktisch nicht durchführbar …
- **gesetzliche Verbote (z.B. TKG, TMG, Videoüberwachung) …**

… einen Personenbezug herzustellen

Maßgeblicher Zeitpunkt ist der jeweilige Verarbeitungsvorgang

➔ Regelmäßig prüfen, ob inzwischen personenbezogene Daten vorliegen

Was ist „eine“ Verarbeitungstätigkeit?

Art. 4 Nr. 2 DSGVO (umformuliert und gekürzt)

Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten

oder

„Summe von sachlich zusammengehörenden Verarbeitungen“

Knoblauch Kommentar Datenschutz in Bayern Art. 30 DSGVO Nr. 9

Die Hochschule macht doch alles selber!

- Softwareanbieter
- Support und Wartungsleistungen
- Telefonie
- Cloudservices
- Hardwarebeschaffung
  - Gewährleistung
  - Garantieabwicklung
  - Hardwareentsorgung
- Reinigungsleistungen
- Kooperationen

Lösung:

- Geheimhaltung (EVB-IT, wenn nicht dann extra)
- Vertrag zur Auftragsverarbeitung
- Sitz des Dienstleister und Dienstleistungserbringung und Unterauftragnehmer prüfen
- Vereinbarungen zu gemeinsam verantwortliche Stellen treffen

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten" gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für Datenschutzaufsicht

Muster 9: Online-Shop – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
Online-Shop Keramik
Hinterer Weg 15
91522 Fallstadt

Tel. 0981/123456-0
E-Mail: keramik@ shop-keramik-fallstadt.de
Web: www.shop-keramik-fallstadt.de

Vorstand: Gerlinde Meier, geb. 21.02.1986

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Hans Klausen 0981/123456-1 hans@ shop-keramik-fallstadt.de	01.01.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name und Adressen der Beschäftigten • ggf. Religions-zugehörigkeit • Eindeutige Kennzahlen zur Steuer...	Externes Buchhaltungsbüro	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Betrieb der Webseite des Startups (über Hosting-Dienstleister)	Peter Diercksen 0981/123456-2 peter@ shop-keramik-fallstadt.de	19.03.2018	Vertrieb von eigenen Produkten	• Kunden • Webseitenbesucher	• IP-Adressen • Stammdaten der Kunden • E-Mail-Adressen + Passwörter	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept + HTTPS-Verschlüsselung + OWASP-Top10-Schutz + Patch Management
Kundenverwaltung	Marie Greiner 0981/123456-3 marie@ shop-keramik-fallstadt.de	19.03.2018	Verwaltung der Kundendaten	Kunden	• Stammdaten der Kunden • Kaufhistorien	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Zahlungsabwicklung bei Kunden (über externen Dienstleister)	Peter Diercksen 0981/123456-2 peter@ shop-keramik-fallstadt.de	19.03.2018	Durchführung der Zahlungsverarbeitung	Kunden	• Stammdaten der Kunden • Zahlungsdaten (Bankverbindung)	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Werbemaßnahmen zur Kundengewinnung und -bindung	Marie Greiner 0981/123456-3 marie@ shop-keramik-fallstadt.de	20.03.2018	Marketing zur Kundenakquirierung	• Bestandskunden • potenzielle Neukunden	• E-Mail-Adressen der Kunden • IP-Adressen	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...	...	...	...	...	...	...	...	...	...

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Webplattform bzgl. OWASP-Top10 absichern
- ✓ Automatische Updates aktivieren
- ✓ Standard-Gruppenverwaltung
- ✓ Patch-Management bei CMS berücksichtigen
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virenscanner/Sicherheitssoftware
- ✓ Kundendatenbank absichern
- ✓ Backups regelmäßig (insb. von Kundendaten)
- ✓ Papieraktenvernichtung mit Standard-Shredder

Beispiele unter https://www.lda.bayern.de/de/kleine-unternehmen.html

Folgen für die Hochschule im Alltag

- Dokumentieren!
- Warum möchte ich die Daten?
- Wem gebe ich die Daten weiter (ggf. auch intern)
- Wo ist meine rechtliche Erlaubnis?
  z.B.: Hochschulgesetz, Haushaltsrecht, Verträge, TMG, TKG, BayEGovG, BayDSG-Videoüberwachung, Archivgesetz
- Erstellen der Dokumentation
- Erstellen der Information
- Arbeitshilfen:
  https://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen/index.php

Strategische Entscheidungen

- Zuständigkeiten klären und schaffen
  - Dezentrale Datenschutzbevollmächtigte?
  - Wer meldet Datenschutzvorfälle?
  - Wer unterschreibt Verträge zu Auftragsvereinbarungen?
  - Wer ist bei Vereinbarungen zu gemeinsamen Verantwortlichen einzubinden?
- Aufgabenbereich der Datenschutzbeauftragten anpassen
  - Wer soll das Verzeichnis der Verarbeitungstätigkeit verwalten?
  - Soll der Datenschutzbeauftragte die Datenschutzvorfälle melden?
- Datenschutzbeauftragten der Aufsicht melden
- Umsetzungsgremium einsetzen
- Geschäftsordnung / verbindliches Konzept zum Datenschutz

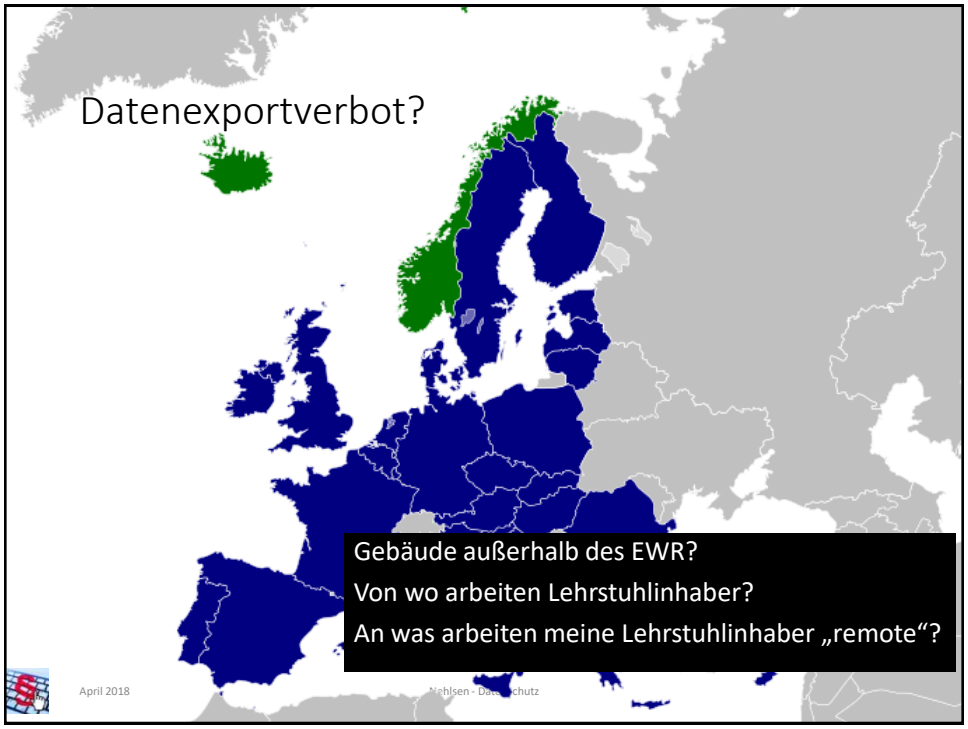
Arbeitspakte

- Anpassung der Datenschutzhinweise auf Webseiten und Formularen
- Dokumentation auffüllen
- Verträge kontrollieren
- Normen zur Datenverarbeitung finden
- Satzungen ggf. Anpassen
  - Z.B. Verarbeiten der E-Mail-Adresse von Bewerbenden bei Immatrikulation
- Datenschutzmaßnahmen überprüfen

Ziele ausgeben, wie z.B.:

- Dokumentation und Information über ein Managementtool
- Vertragsmanagement einführen
- Asset-Management stärken und ausbauen
- (Mobile-)Devicemanagement
- Datenschutz-Selbstverpflichtungen

Datenexportverbot?



Gebäude außerhalb des EWR?
Von wo arbeiten Lehrstuhlinhaber?
An was arbeiten meine Lehrstuhlinhaber „remote“?

Und was ist mit der Datenschutzfolgenabschätzung?

- Betrachtung des Verfahrens
- Bestehen hohe Risiken?

- Wenn ja, dann
  - Systematische Beschreibung
  - Notwendigkeit und Verhältnismäßigkeit
  - Bewertung der Risiken
  - Bewältigung der Risiken
- Bewältigung der Risiken nicht möglich?
  - Konsultation der Aufsichtsbehörde

Bußgelder gegen Hochschulen?

Nur, soweit diese als „Unternehmen“ am Wettbewerb teilnehmen
- Medizinische Labore
- Fachkundekurse

Eher nicht im Wettbewerb
- Weiterbildungsangebote
- Sprachkurse
- Weiterbildungsmaster (staatlicher Abschluss)

Warum sonst keine?
- Gesetzmäßigkeit des Verwaltungshandelns
- Unmittelbare Grundrechtsbindung der Verwaltung
- Datenschutzverstößen fallen auch die die Zuständigkeit der Aufsichtsbehörde, nicht nur in die der Datenschutzaufsicht!

Meldewege (Datenschutzvorfall)

- Meldung an die Aufsichtsbehörde innerhalb von 72 Stunden
  - Außer Prognose ergibt kein Risiko für die Rechte und Freiheiten natürlicher Personen
- Verhinderung von Meldungen durch
  - Verschlüsselung
  - Fernlöschung
  - Datenschutzkonforme Entsorgung
- Inhalt der Meldung
  https://www.datenschutz-bayern.de/service/data_breach.html
- Sind Betroffene auch aus anderen Mitgliedstaaten?
- Zudem immer Dokumentieren, auch wenn keine Meldepflicht!
  - Sachverhalt (Fakten)
  - Auswirkungen für Betroffene
  - Ergriffene Abhilfemaßnahmen

Unverzichtbare Schritte

- Meldeprozess bei Datenschutzverstößen schaffen
- Arbeitsgruppe zur Datenschutzreform
- Datenschutzinformationen aktualisieren
  - Internetauftritt
  - Lernplattformen
  - Einschreibung
  - Einstellung
- Dokumentation auffüllen

Offene Punkte

- Gefragte (Cloud-)Dienste schaffen oder legalisieren?
- Folge-Webinare und Informationsbündelung

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt:
Johannes Nehlsen
Tel.: 0931/31-84217
rz-stabsstelle-it-recht@uni-wuerzburg.de

https://www.rz.uni-wuerzburg.de/dienste/it-recht/