Die Datenschutzreform an Hochschulen im Alltag

Johannes Nehlsen

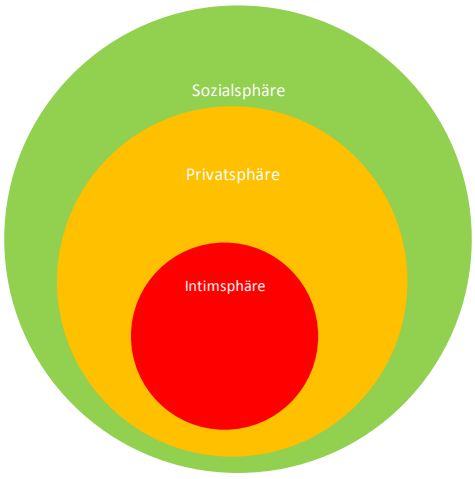
Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen
c/o Rechenzentrum Universität Würzburg

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 mit seinem Sphärenmodell
- Entscheidungsfreiheit
- Mehr Information und Transparenz, wenn Wahlfreiheit nicht besteht oder höhere Risiken bestehen

Kein Datenschutz

Anonyme Daten

EuGH Urteil vom 19.10.2016 C-582/14

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

… einen Personenbezug herzustellen

Maßgeblicher Zeitpunkt ist der jeweilige Verarbeitungsvorgang

➔Regelmäßig prüfen, ob inzwischen personenbezogene Daten vorliegen

Daten von Verstorbenen

Keine Anwendung der Datenschutzgesetze, aber:

➔ Allgemeines postmortales Persönlichkeitsrecht

⇔Verblassen mit der Zeit

Daten mit Informationen über Dritte

➔ Bisher kaum in Diskussion

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

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

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

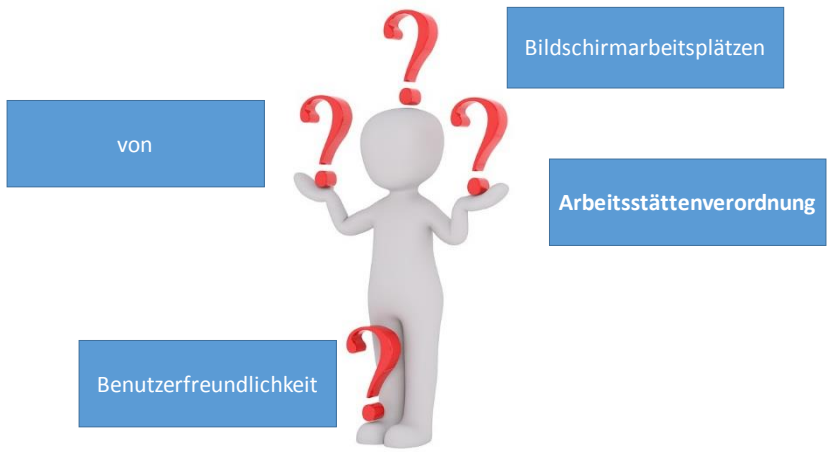
Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Hans Klausen 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

Protection by design and by default



Verarbeitung von personenbezogen Daten

- Lasse ich mich vom Datenschutzbeauftragten beraten?
- Sonderfall wissenschaftliche Forschung
- Dürfen die personenbezogenen Daten verarbeitet werden?
  Die meinen Rechtsgrundlagen finden sich im bayerischen Hochschulgesetz, der bayerischen Haushaltsordnung, im bayerischen E-Government-Gesetz oder im Telekommunikationsgesetz sowie im Telemediengesetz (strittig)
- Darf ich Dritten Daten mitteilen?
- Liegt eine Dokumentation für die Verarbeitung vor?
- Sind die Betroffenen informiert?
- Verarbeite ich den Daten auf Systemen mit ausreichender Sicherheit?
- Ist mir bekannt, dass ich jeden Datenschutzvorfall dokumentieren muss? Und bei Risiken die Aufsichtsbehörde und bei hohen Risiken auch die Betroffen informiert werden müssen?

Datenschutzrisiken – Beispiele für Schäden

- Diskriminierung
- Identitätsdiebstahl oder –betrug
- Finanzielle Verluste
- Rufschädigung
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten
- Unbefugte Aufhebung der Pseudonymisierung
- Andere erhebliche wirtschaftliche oder gesellschaftliche Nachteilen

Nebenprodukt Datenklassifizierung

Datenkategorie	Norm	Standardschutzbedarf
Nicht personenbezogene Daten	Art. 2 Abs. 1 DSGVO	Nicht nach Datenschutz
Identifizierbare personenbezogene Daten	Art. 1 Abs. 1 Alt. 2 DSGVO	Ja
Pseudonyme personenbezogene Daten	Erwägungsgrund 26 DSGVO	Ja
Personenbezogene Daten unter Berufsgeheimnis	Erwägungsgrund 85 DSGVO	Gesteigert
Personenbezogene Daten unter Sozialgeheimnis, Steuergeheimnis oder besonderem Amtsgeheimnis		Gesteigert
Besondere Verarbeitungsformen, • insbesondere große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen • Daten von Minderjährigen	Erwägungsgrund 75 DSGVO	Gesteigert bis erheblich gesteigert
Besondere Kategorien personenbezogener Daten: • rassische und ethnische Herkunft • politische Meinungen, • religiöse oder weltanschauliche Überzeugungen • Gewerkschaftszugehörigkeit • genetischen Daten, • biometrischen Daten • Gesundheitsdaten oder • Daten zum Sexualleben • Daten der sexuellen Orientierung	Art. 9 DSGVO	Erheblich gesteigert
Personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten	Art. 10 DSGVO	Erheblich gesteigert

Wann sind personenbezogenen Daten löschen?

Allgemein:
Wenn diese für die Verarbeitungszwecke nicht mehr erforderlich sind.

Besonderheit für öffentliche Stellen:
Anbieten aller Unterlagen vor „Löschung“ an das Archiv
Ein Unterlassen kann die Tatbestand der Urkundenunterdrückung erfüllen!

Wesentliche Löschfristen
- Verkehrsdaten und Steuerungsdaten 7 Tage (§ 100 Abs. 1 TKG)
- Protokolldaten von Zugriffen etwa 1 Jahr (ggf. 3 Jahre)
- Vorgaben aus Hochschulsatzungen
- Haushaltsrecht meistens 3 – 30 Jahre
- Allgemeine Auffangnorm 30 Jahre (Art. 6 Abs. 1 S. 2 BayArchiG)

Was kann ich tun?

- Verarbeitung der Daten ausschließlich auf dienstlichen Geräten
- Nur im Ausnahmefall Webanwendungen auf privaten Geräten
- Aktualisieren und regelmäßige Updates des Betriebssystem
- Aktualisieren und regelmäßige Updates der Anwendungen, insbesondere Webbrowser
- Verschlüsselung von Datenträgern und mobilen Endgeräten
- Ablage relevanter Dokumente grundsätzlich auf Netzlaufwerken
- Verwalten und Kontrollieren der Zugriffsrechte auf Netzlaufwerken
- Verwenden von Passwortmanagern

Ihr IT-Support kann Sie bei der Umsetzung bestens unterstützen!

Was kann ich tun? Teil 2

- Bei Verlassen des Büros
  - Absperren der Türen und Verschließen der Fenster
  - Aufräumen und Wegsperren von Unterlagen
  - Bildschirmsperre / Ausschalten des PCs
- Datenschutzkonforme Entsorgung von Papier und Datenträgern
  - Beschaffung eines Akten-Schredders
  - Datenträger IT-Support oder ggf. über Spezialfirma entsorgen
- Datenschutzvorfälle mindestens dem Vorgesetzten und Datenschutzbeauftragtem melden
- Einhalten der goldenen Regeln zur IT-Sicherheit
- Erlaubnis vor dem Einsatz neuer Dienste einholen (Vorgesetzte, Datenschutzbeauftragte, Einkauf, Personalräte)
- IT-Sicherheitsvorfälle dem Systemverantwortlichen und dem IT-Support des Rechenzentrums melden

Welche Rechte habe ich?

- Anspruch auf Information, wenn meine personenbezogen Daten verarbeitet werden
- Widerruf von Einwilligungen
- Auskunftsrecht
- Recht auf Berichtigung
- Recht auf Löschung („Recht auf Vergessenwerden“)
- Recht auf Einschränkung der Verarbeitung

Selten im öffentlichen Bereich

- Recht auf Datenübertragbarkeit
- Widerspruchsrecht

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/dsgvo