Die Datenschutzreform an Hochschulen Technische 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

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, Datensicherungs- und Datenkontrollmaßnahmen 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

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

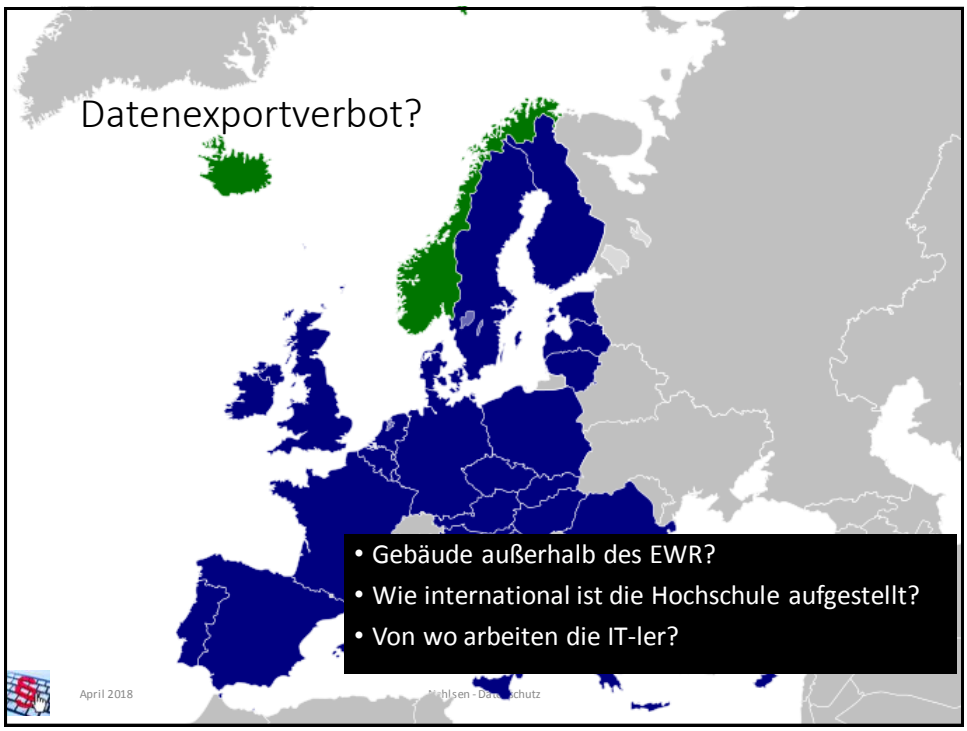
Vorstand: Gerlinde Meier, geb. 21.02.1986

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
…	…	…	…	…	…	…	…	…	…

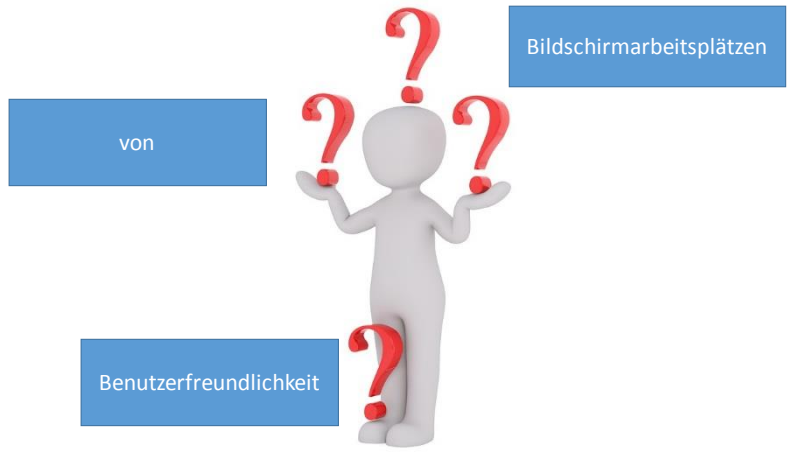
Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ 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



Protection by desing and by default

6.5 Anforderungen an die Benutzerfreundlichkeit von Bildschirmarbeitsplätzen

(1) Beim Betreiben der Bildschirmarbeitsplätze hat der Arbeitgeber dafür zu sorgen, dass der Arbeitsplatz den Arbeitsaufgaben angemessen gestaltet ist. Er hat insbesondere geeignete Softwaresysteme bereitzustellen.

(2) Die Bildschirmgeräte und die Software müssen entsprechend den Kenntnissen und Erfahrungen der Beschäftigten im Hinblick auf die jeweilige Arbeitsaufgabe angepasst werden können.

(3) Das Softwaresystem muss den Beschäftigten Angaben über die jeweiligen Dialogabläufe machen.

(4) Die Bildschirmgeräte und die Software müssen es den Beschäftigten ermöglichen, die Dialogabläufe zu beeinflussen. Sie müssen eventuelle Fehler bei der Handhabung beschreiben und eine Fehlerbeseitigung mit begrenztem Arbeitsaufwand erlauben.

(5) Eine Kontrolle der Arbeit hinsichtlich der qualitativen oder quantitativen Ergebnisse darf ohne Wissen der Beschäftigten nicht durchgeführt werden.

data protection by design & data protection by default

- Datenverarbeitung auf das notwendig beschränken
- Ziel der Datenminimierung aktiv verfolgen
- Umsetzung der Betroffenenrechte sicherstellen
- (Automatische) Datenlöschbarkeit
- Nutzerführung vor Datenfreigaben
- Datenschutzmaßnahmen implementieren

data protection by design & data protection by default

Soft- und Hardware mit Blick auf Datenschutzfreundlichkeit wählen

Beispiele

- ➔ Softwarefunktionen sind angemessen dokumentiert
- ➔ Hardware ohne „voreingestellte“ Herstellerzugriffe
- ➔ „Intro“ beim ersten Login in ein Portal

➔ Einsatz von Pseudonymen z.B. auf Nutzeroberfläche

➔ Richtiger Einsatz von Verschlüsselung

➔ Rollen und Rechtemanagement

➔ Sichtbarkeit in Portalen erst nach Nutzerinteraktion

➔ Datensparsame Einstellungen bei Telemetrie

Was gehört in getrennte Datenbanken

- Videoüberwachung (Löschen nach spätestens zwei Monaten)
- Datensicherungsmaßnahmen
- Datenschutzkontrollmaßnahmen
- Daten für Störungsbeseitigung (Internet, E-Mail)
- Benutzerprofile für das jeweilige Telemedienangebot (Moodle, Teams, Wiki …)

…

Funktionalitäten von Lösungen/Datenbanken?

- Abruf und Ausgabe einer Kopie der personenbezogen Daten
- Berichtigung der „aktiven“ Daten (z.B. Namensänderung)
- Einschränkung der Bearbeitung / Sperrung von Daten
  - ➔ Nur noch Speichern erlaubt, bis zur Löschfrist
    Beste Umsetzung: Ausschließliche Leserechte für bestimmte Rollen
- Löschen von Datensätzen
- Datenexportmöglichkeit

Wünschenswertes

- Flags für Datensätze
  Beispiele
  - Besondere Kategorien personenbezogener Daten
  - Einwilligungen von Kindern
- Datenübermittlungsprotokolle

Funktionalitäten von Benutzeroberflächen

- Verlinken oder Anlegen von Impressum und Datenschutz
- Gesicherter Zugang
- Sichere Eingabe und Transfer von Login-Daten
- Login mit Pseudonym (wenn nicht dem Dienst zu widerlaufend)
- Sprachenauswahl (Deutsch, Englisch, + Sonderfälle)
- Self-Service
  - Auskunft
  - Kopie der Daten
  - Löschen des Accounts
  - Je nach Anwendungsfall ggf. auch eigenständige Berichtigungsmöglichkeiten

Datenschutzrisiken

Physische, materielle oder immaterielle Schäden der Betroffenen

Insbesondere

- 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

Verletzung des Schutzes personenbezogener Daten

Vertraulichkeit	Integrität	Verfügbarkeit
• Weitergabe der Daten an unberechtigte Dritte • Verknüpfung der Daten mit anderen Daten • Nutzung für unzulässige Zwecke • Unbefugte Einsichtnahme • Andere Verletzung der Vertraulichkeit	• Nicht mehr aktuelle Daten wurden genutzt • Daten wurden verfälscht • Herkunft der Daten nicht bekannt / feststellbar • Andere Verletzung der Integrität	• Wichtige Daten sind dauerhaft nicht mehr verfügbar • Wichtige Daten waren zeitweise nicht ausreichend verfügbar • Andere Verletzung der Verfügbarkeit
Lösungsbeispiele		
• Verschlüsselung • Rollen und Rechtemanagement • Gerätekontrolle • Fernlöschung	• Regelmäßige Prüfung auf Malware • Signaturen • Prüfwerte	• Verfügbarkeit vorab festlegen (SLA) • Regelmäßige Sicherungen • Redundanz • Cluster

Weitere Maßnahmen gegen Datenschutzvorfälle

Vorfall	Maßnahme
Gerät verloren	**Fernlöschung, Inventarisierung, Verschlüsselung**
Unterlagen verloren oder an einem unsicheren Platz gelagert	**Hausordnung, Regelungen zu mobilen und Telearbeitsplätzen**
Hackerangriff, Schadsoftware, Phishing	**Umfassende Informationssicherheitskonzepte**
Nicht datenschutzgerechte Entsorgung	**Rahmenverträge und Kommunikation**
Missbrauch von Zugriffsrechten	Eingehende Belehrungen und ggf. Kontrollen
Unbeabsichtigte Veröffentlichung	Prüfschritte vor Veröffentlichungen
Webportal zeigte falsche / fremde Daten an	Kontrollen
Personenbezogene Daten an falschen Empfänger gesendet	Funktionen in E-Mail-Programmen Ggf. Sonderfällen mit tiefgreifendem Rechtemanagement

Nebenpunkt Datenklassifizierung

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
Identifizierbare personenbezogene Daten	Art. 1 Abs. 1 Alt. 1 DSGVO	Ja
Personenbezogene Daten unter Berufsgeheimnis	Erwägungsgrund 85 DSGVO	Gesteigert
Personenbezogene Daten unter Sozialgeheimnis, Steuergeheimnis oder besonderen Amtsgeheimnis		Gesteigert
Besondere Verarbeitungsformen, insbesondere große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen	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

Wie stelle ich meine Sophos-Enterprise-Konsole ein?

- Richtlinie zum Virenschutz auf Endgeräten
- Richtlinie zum Virenschutz bei zentralen Dateiablagen
- Erarbeiten des geeigneter Voreinstellungen des Virenschutzes für die Anwendergruppen (z.B. Verwaltung, Lehrstuhl, Virenforschungsprojekt, Administratoren)
- Schutz von Sophos gegen unerwünschte Veränderungen des Programms
- Verteilen der Voreinstellungen
- Schulungen und Informationen für Mitarbeiter zum Einsatz von Sophos
- Zentrale Sammlung aller "Viren"-Befall-Meldungen mit Maßnahme (White-List, Quarantäne, Löschung, Systemscan nach Befall)
- Kontrollmöglichkeit, ob alle Geräte über die aktuelle Version von Sophos (inklusive der neuen Signaturen)verfügen
- Prozess zur Bewertung der Vorfälle um ggf. die Meldefristen einzuhalten
- Prüfen von Schnittstellen Spamabwehr zu Virenschutz

Legalisieren von Cloudangeboten (Beispiele)

Dropbox über Dropbox Education (recht teuer)
➔ Anwenderwahl „Kostenlos Teamdrive oder kostenpflichtig Dropbox“

Skype über Skype for business / Office 365 Education A1 (ohne Entgelte)
➔ Professorenwunsch nach Skype
➔ Weitere Alternativdienste, u.a.
- Sway statt Prezi
- Stream statt Youtube
- Teams statt Slack

Google über Google for Education (ohne Entgelte)
➔ Institutionalisierte Google-Accounts
➔ Chromebox für Browserterminals (z.B.: Bibliothek)
➔ Mobile Device Management

Apple School Manger
➔ Institutionalisierte Apple-Accounts
➔ Noch keine taugliche Auftragsverarbeitung iCloud, Facetime und iMessage vorhanden

Datenschutzmanagement

Kein rein technisches Thema, Schwerpunkt in der Organisation
➔ Schnellste Lösung: Einhalten des Aktenplans

An den Hochschulen
- Datenschutz-Geschäftsordnung
- Antrags, Formular – und Meldemanagement
- Fristen für Vorgänge
  - Unmittelbar
  - 72 Stunden
  - Ein Monat
- Checklisten für technische Anforderungen
  https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Reihe_node.html

Tools:

https://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen/index.php

https://www.rehm-datenschutz.de/fachinformationen/datenschutz-management-software-eine-effiziente-hilfe-zur-datenschutz-dokumentation/

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/