Datenschutzdokumentation

Johannes Nehlsen

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

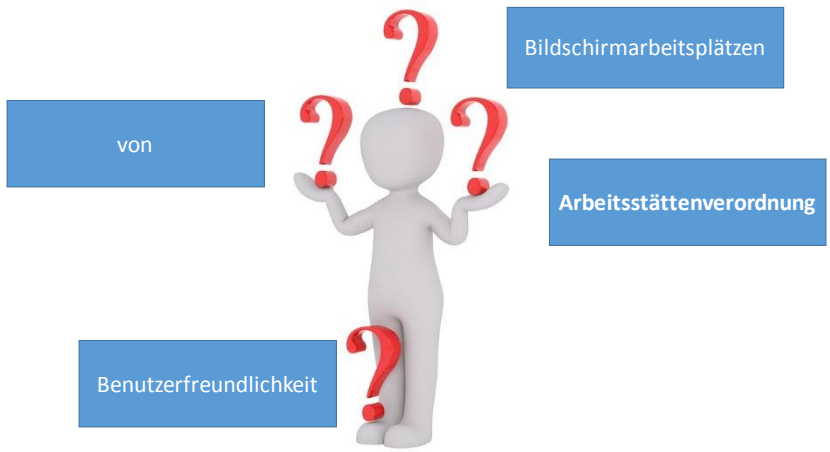
Stabsstelle IT-Recht – Eine Stelle – Eine Person

- Datenschutz im Rechenzentrum
- Digitalisierung der Lehre
- E-Government für Hochschulen
- Informationssicherheitsrecht
- Vertragsberatung IT-Beschaffung
- Beratung um Softwarelizenzverträge
- Wissensvermittlung

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 Sonderfälle
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

Protection by design and by default



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

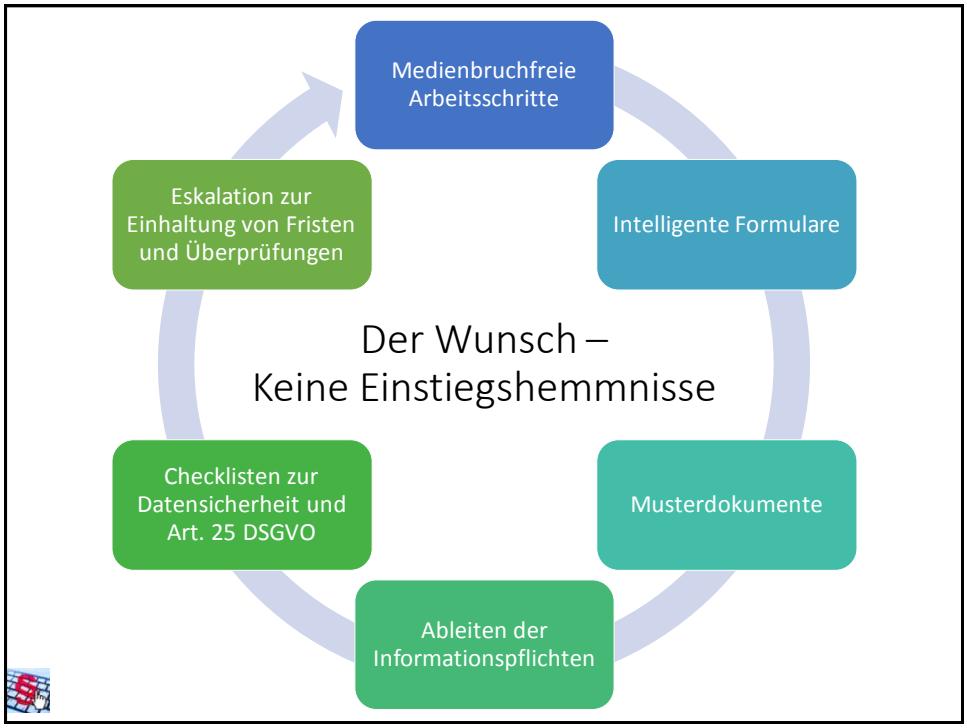
Umsetzung der Datenschutzanforderungen

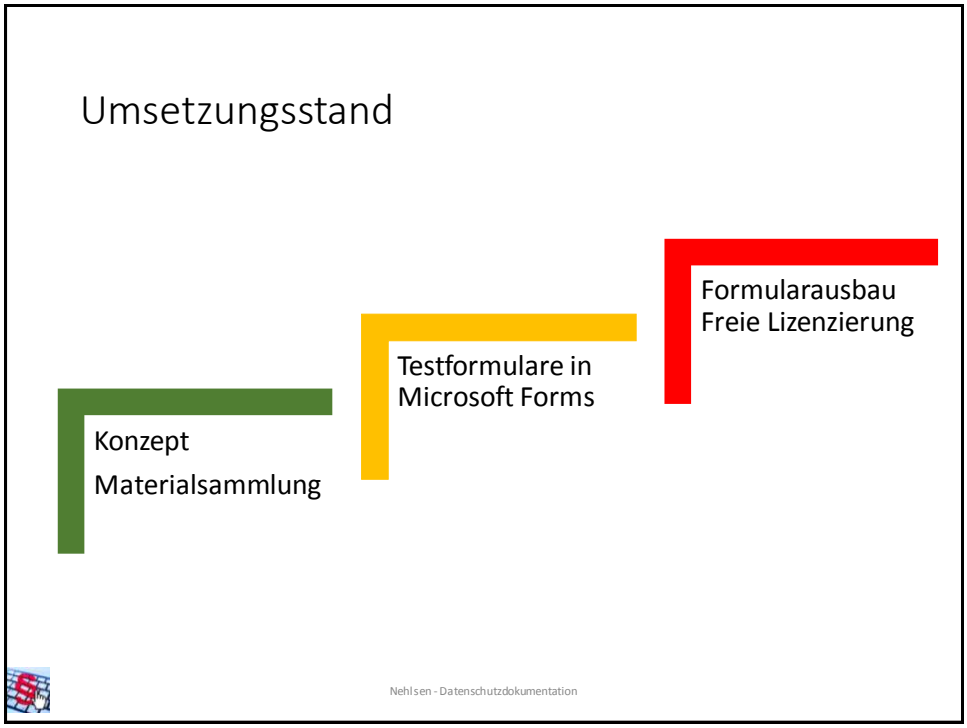
Kein rein technisches Thema, Schwerpunkt in der Organisation

➔ Bestehende Lösung für Behörden: Einhalten des Aktenplans

An den Hochschulen

- Informationsgewinnung
  - Mitglieder, Gäste, Kooperationspartner, Dienstleister
  - Dienstleistungsverzeichnisse und zentrale IT-Systeme (IDM, AD, SCCM, SAM)
  - Inventare
- Datenschutz-Geschäftsordnung
- Antragformulare
- Prüfliste für typische Risiken
- Checklisten für technische Mindestanforderungen
- Meldeprozesse


Medienbruchfreie Arbeitsschritte
Intelligente Formulare
Musterdokumente
Ableiten der Informationspflichten
Checklisten zur Datensicherheit und Art. 25 DSGVO
Eskalation zur Einhaltung von Fristen und Überprüfungen
Der Wunsch –
Keine Einstiegshemmnisse


Umsetzungsstand
Konzept
Materialsammlung
Testformulare in Microsoft Forms
Formularausbau
Freie Lizenzierung
Nehlsen - Datenschutzdokumentation

Die Materialien

- Das Gesetz
- Arbeitshilfen und Dokumente
  - Bayerischer Landesdatenschutzbeauftragter
    Erste Informationen und Hilfestellungen
    Online-Meldeformulare
  - Bayerisches Landesamt für Datenschutzaufsicht
    Orientierungshilfen als „Hilfefunktion“
  - Bayerisches Innenministerium
    Arbeitshilfen
  - Kommentar Datenschutz in Bayern
    Datenschutzfolgeabschätzung auf einer Seite
  - Code of Conduct von GÉANT
    Informationspflichten, TOM
  - CNIL für Art. 32 DSGVO
  - Eigenes Kurzmuster
    Kooperation und
    Art. 28 inklusive EU-Standardvertragsklauseln

Linksammlung

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

Was ist zu dokumentieren?

Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO

Verantwortliche + Kontaktinformationen
- ➔Alleinig
- ➔Gemeinsam + Vereinbarung (Art. 26 DSGVO)
- ➔Auftragsverarbeiter + Vertrag und Weisungen (Artt. 28 und 29 DSGVO)

Deren Datenschutzbeauftragte + Kontaktinformationen

Einwilligungen

Erfüllung der Informationspflichten

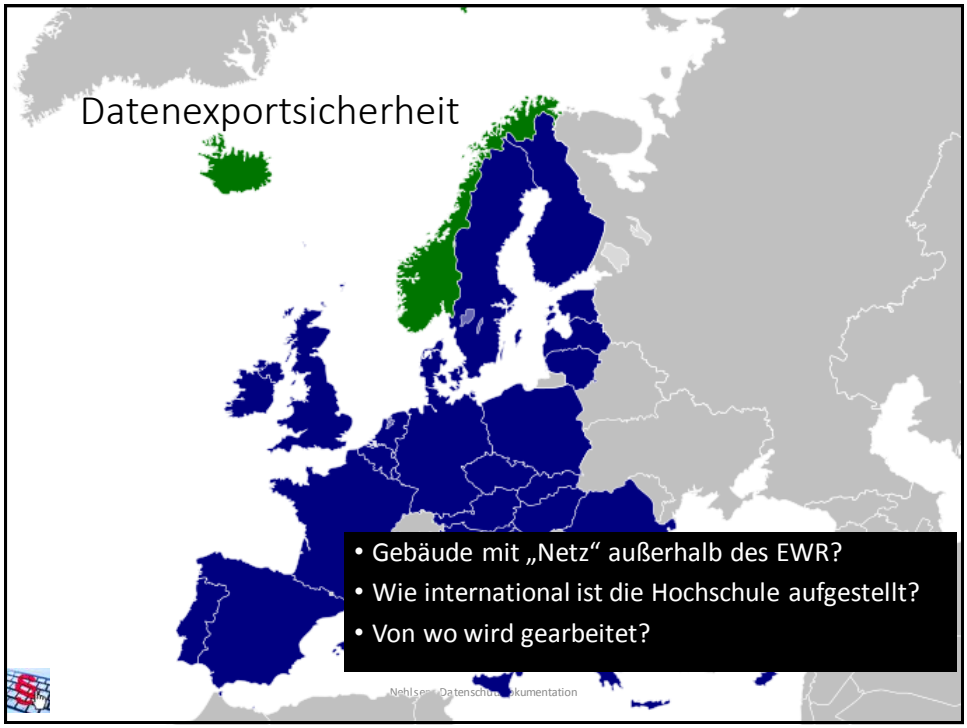
Technische wie organisatorische Maßnahmen Artt. 24, 32, 25

Verarbeitungstätigkeiten (Verzeichnisse) Art. 30

Datenschutzfolgeabschätzung Artt. 35, 36

Einige Sonderfälle:

Verhaltensregeln, Art. 40, Zertifizierungen Art. 42, Garantien Art. 46, Identifizierung, Art. 11 Abs. 2; Missbrauch von Betroffenenrechten , Art. 12 Abs. 5; Erfolgloses Widerspruchsrecht, Art. 21 Abs. 1



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, gute Inventarisierung**
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 In Sonderfällen auch tiefgreifendes Rechtemanagement

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)
- Selfservice
  - Auskunft
  - Kopie der Daten
  - Löschen des Accounts
  - Je nach Anwendungsfall ggf. auch eigenständige Berichtigungsmöglichkeiten

Datenschutzrisiken – Beispiele für Schäden

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

Zusammenfassung

Über den Verantwortlichen
- Was macht und wo ist meine Einrichtung?
- Gemeinsam Verarbeitungstätigkeiten sammeln (Muster BayLDA)

Zu Gunsten der Betroffenen durch den Verantwortlichen
- Informationspflichten
- Einwilligungen

Für die Verantwortlichen
- Verzeichnis der Verarbeitungstätigkeiten
- Datensicherheitsmaßnahmen
- Datenschutzvorfälle

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/

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