WWU
MÜNSTER

Verfahrensdokumentation mit SecDoc

Thorsten Küfer
Nina Meyer-Pachur
Dustin Gawron

wissen.leben

ZENTRUM FÜR
INFORMATIONS
VERARBEITUNG

Übersicht

- Motivation
- Funktionsübersicht
- Ausblick
- Diskussion

Motivation

Einhaltung rechtlicher Vorgaben (Compliance) aus der Datenschutzgrundverordnung

- Dokumentationspflichten (Art. 30 DSGVO)
- Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO)
- Umsetzung geeigneter Schutzmaßnahmen (Art. 32 DSGVO)

Ziel

- Schutz der personenbezogenen Daten des Betroffenen
- Wahrung des Grundrechts auf informationelle Selbstbestimmung

Motivation

Begriffsbestimmungen (Art. 4 DSGVO)

- **Was sind *personenbezogene Daten*?**

„Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.“

Motivation

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

- „Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen."
  - **Wer ist *Verantwortlicher*?**

  „Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden."

  → „Verantwortlicher" im Sinne der DSGVO ist die WWU

Motivation

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

- „Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen."
  - **Was ist eine *Verarbeitungstätigkeit*?**

    „Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie 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."

Folgen

- Dienstliche Pflicht zur Verfahrensdokumentation? Ja (sobald pers. bez. Daten betroffen sind)
- Dokumentation muss vor Ort geschehen. Nur dort ist das Verfahren bekannt.
- Verfahrensübersicht bei DSB gesammelt für Anfrage der Aufsichtsbehörde.
- Umsetzung möglichst effizient gestalten
  - Vorlagen u.a. von GDD und ZENDAS vorhanden
  - Vom ZIV für die WWU in Web-Workflow umgesetzt

Vorteile

Ziel: Möglichst einfaches Ausfüllen und Verwalten der Verfahrensdokumentation

- Ausfüllen im Browser, (geschützter) Zugriff von überall
- Automatisches Speichern
- Datenvorschläge für Personen, Organisationseinheiten, Software, Endgeräte
- Integrierte Hilfen
- PDF-Erzeugung
- HTML-Schnipsel Erzeugung zur Verwendung in Datenschutzerklärung (Informationspflichten, Art. 13/14 DSGVO)
- Strukturierte Ablage in Datenbank

Technische Realisierung

- Single Page Web Application
  - Umgesetzt mit HTML5, CSS, JavaScript, PHP, SQLite
  - Verwendet Bootstrap3 (Twitter) und dafür entwickeltes Wizard-Theme (Creative TIM)
- Open Source (MIT Lizenz)
- Code im WWU-Gitlab einsehbar
  - https://zivgitlab.uni-muenster.de/tk23279/bootstrap-wizard

Livedemo

https://www.uni-muenster.de/ZIV.CERT/secdoc/

Ausblick

- Zugriff für Bearbeitung über Gruppenmitgliedschaften
- Auswertungen der Verfahren
  - Verfahrensüberblick nach Organisationseinheiten oder WWU gesamt
- Weiterverarbeitung für Risikoanalyse (insbes. Art. 35 Datenschutzfolgeabschätzung)
  - Dafür evtl. externes Tool (SerNet verinice)
- Gemeinsame Weiterentwicklung mit anderen interessierten Hochschulen

Diskussion