WWU
MÜNSTER

Grundsätze der DSGVO im Hinblick auf sciebo

Dr. Dominik Rudolph, WWU Münster

wissen.leben

ZENTRUM FÜR
INFORMATIONS
VERARBEITUNG

Grundsätzliches

- Tritt am 25. Mai 2018 unmittelbar in Kraft, kann nicht durch nationale Gesetze abgemildert werden
- Orientiert sich stark am bisherigen deutschen Datenschutzrecht
- „personenbezogene Daten“ [sind] 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann; … (Art. 4)
- Keine Bußgelder bei Verstößen für Behörden und öffentliche Einrichtungen (§ 43 Abs. 2 BDSG 2018); wohl aber Schadensersatz und Haftung gegenüber Endnutzern

WWU MÜNSTER

Wesentliche Änderungen durch die DSGVO

- Stärkung der Rechte des Endnutzers auf Information, Zugang und Löschung
- Grundsatz von datenschutzfreundlichen Voreinstellungen („Privacy by default“) und Datenschutz durch Technik („Privacy by design“) (Art. 25)
- Übermittlung der Daten an den Endnutzer oder einen anderen Anbieter auf Antrag (Datenportabilität)
- Pflicht zur Meldung von Verstößen an Behörde und Betroffene
- Neue Regelung zu Verantwortlichkeiten bei Auftragsdatenverarbeitung (u.a. gemeinsame Verantwortlichkeit, Auftragnehmer nun auch gegenüber Endnutzer verantwortlich)
- Datenschutzfolgeabschätzung als Vorab-Risikobewertung

Mögliche Grundlagen der Datenverarbeitung

Art. 6

- Einwilligung des Nutzers (Opt-in), möglichst schriftlich (Art. 6 (1a))
- Erfüllung eines Vertrages (Art. 6 (1b))
- Berechtigtes Interesse (d.h. zur Erfüllung des Geschäftszweckes erforderlich) (Art. 6 (4a-e))
- Gesetzliche Vorgabe (Art. 6 (1c)

Informationspflichten

Die Nutzern müssen aktiv über folgendes informiert werden (z.B. in AGB) (Art. 13-14):

- Kontaktdaten des Verantwortlichen und die des Datenschutzbeauftragten
- Zweck der Datenverarbeitung
- Kategorien der verarbeiteten Daten
- Die Rechtsgrundlagen zur Verarbeitung der Daten
- Aufbewahrungsfristen
- Potentielle Empfänger der Daten
- Ob Daten außerhalb der EU übermittelt werden

Informationspflichten

Hinweis auf Rechte:

- Recht auf eine Kopie der Daten (Art. 15 (3))
- Beschwerderecht bei Datenschutzbehörde (Art. 13 (2d))
- Recht zum Zurückziehen der Einwilligung (Widerruf) (Art. 7 (3) und Art. 21) oder zur Löschung der Daten (Art. 17)

Recht auf Auskunft

- Nutzer haben das Recht, auf Antrag zu erfahren, welche Daten über sie verarbeitet werden (Art. 15) und zwar:
  - **Ob** personenbezogene Daten verarbeitet werden oder nicht
  - **Warum** die Daten verarbeitet werden (Zweck)
  - **Welche** Daten verarbeitet werden (Kategorien)
  - **Wie** die Daten verarbeitet werden (z.B. Speicherung, Dauer, Weitergabe)
- Ihnen muss eine Kopie ihrer gespeicherten personenbezogenen Daten übermittelt werden
- Sie müssen keinen Grund angeben

Recht auf Datenlöschung / “Vergessenwerden“

Nutzer haben das Recht, die Löschung ihrer Daten zu verlangen (Art. 17), außer (Art. 17 (3)):

- Gesetzliche Aufbewahrungspflichten stehen entgegen
- Daten sind zum Recht auf freie Meinungsäußerung wichtig (für uns nicht relevant)
- Öffentliches Interesse wiegt schwerer (z.B. wiss. Forschung; für uns eher nicht relevant)

- Keine Pflicht zur Löschung, wenn Daten angemessen anonymisiert wurden

→ Hinweis in Datenschutzvereinbarung, Workflow zur weitgehend automatischen Datenlöschung etablieren

WWU
MÜNSTER

Recht auf Datenübertragbarkeit

Nutzer haben das Recht, die sie betreffenden personenbezogenen Daten, die sie bereitgestellt haben, in einem strukturierten, maschinenlesbaren Format zu erhalten (z. B. XML, JSON, CSV usw.). PDF ist nicht ausreichend. (Art. 20)

→ Hinweis in Datenschutzvereinbarung, Workflow zur Übermittlung der Datenpakete einrichten

Antragsweg zur Rechteausübung

- Nutzer müssen auf elektronischem Wege Anträge zur Ausübung ihrer Rechte (Recht auf Auskunft, Berichtigung, Löschung, Übertragbarkeit usw.) stellen können. Diese müssen binnen eines Monats, spätestens binnen 3 Monaten bearbeitet werden (Art. 12 (3))
- Der Antragsteller muss seine Identität auf Anfrage bestätigen können (Art. 12 (2) und (6))
- Abweisung nur mit Angabe von Gründen und Hinweis auf Beschwerdemöglichkeit bei der Datenschutzbehörde und Einlegung eines gerichtlichen Rechtsbehelfs (Art. 12 (4))
- Bei offenkundig unbegründeten oder, insbesondere im Fall von häufiger Wiederholung, exzessiven Anfragen kann die Bearbeitung verweigert werden (Art. 12 (5))

→ Verweis auf Kontaktformular in Datenschutzhinweis einbauen. Standardantworten für Standartanfragen, Abweisung und Bearbeitungsstatus erstellen. Prüfen, wie Identität geprüft wird

Aufbewahrungsfristen

- Aufbewahrung „so kurz wie möglich“, (Art. 5 (1e)) („Speicherbegrenzung), jedoch keine konkrete Frist in der DSGVO
- Pflicht zur regelmäßigen Aktualisierung von Daten (Art. 5 (1d)
- Es müssen selbst Fristen zur Aufbewahrung und ggf. Aktualisierung von Daten festgelegt werden (Art. 24)

WWU MÜNSTER

Umfang der gespeicherten Daten

- Die Datenerhebung muss dem Zweck angemessen sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“) (Art. 5 (1c)
- Entscheidung über das notwendige Maß liegt beim Verantwortlichen für den Dienst (Art. 5 (2) („Rechenschaftspflicht“)

Vom Anbieter zu prüfende Punkte

- Risikofolgeabschätzung erstellen
- Informationspflichten: Hinweistexte anpassen, auf Rechte hinweisen
- Rechte der Nutzer: Antragsweg, Workflows zur Löschung und Datenübertragung etablieren
- Umfang der Datenspeicherung: welche Daten werden verarbeitet?
- Aufbewahrungsfristen: wie lang ist die Speicherung erforderlich?
- Klärung der Verantwortlichkeiten bei Auftragsverarbeitung

WWU MÜNSTER

Maßnahmenplan

- Welche **personenbezogene Daten** werden verarbeitet? (insbes. Metadaten)
- Überprüfen von AGB, Datenschutzerklärungen, Impressum, laufenden Verträgen, Website-Einstellungen, etc.
- Was sind die **Zwecke** der Datenverarbeitungen?
- Was ist die **Rechtsgrundlage** der Datenverarbeitung? Liegt eine Einwilligung vor?
- Wie werden die Informationspflichten (nach der DSGVO) erfüllt?
- Wie werden die **Betroffenenrechte** (nach der DSGVO) erfüllt?
- Welche **Datensicherheitsmaßnahmen** sind vorhanden?
- Welche Vorkehrungen gegen **Datenschutzverletzungen** existieren
- Wie ist **privacy by design**/**privacy by default** implementiert?

Konkrete Maßnahmen bei sciebo

- Erarbeitung von DSGVO-konformen Schriftstücken (Nutzungsbedingungen, Impressum, Verträge) durch Juristen des Institut für Informations-, Telekommunikations- und Medienrecht der WWU
- Ausarbeitung neuer Vertragskonstrukte für die Beziehung zu Endnutzern sowie zwischen den Teilnehmerhochschulen:
  - Plan: die WWU Münster wird Anbieter gegenüber dem Endnutzer, gemeinsame Verantwortlichkeit durch Verträge mit einzelnen Hochschulen geregelt
  - Nutzer stimmen direkt mit der Registrierung bestimmten Funktionen (z.B. Auffindbarkeit) zu
  - Konsortialteilnehmer sind gemeinsam Verantwortliche im Sinne des Datenschutzes im Hinblick auf Metadaten
  - WWU ist Auftragsverarbeiter aus Sicht des Endkunden für die hochgeladenen Inhaltsdaten
  - Welche Daten in sciebo gespeichert werden, bleibt dem Endnutzer überlassen

WWU MÜNSTER

Zusammenfassung der relevanten Stellen aus der DSGVO

- **Art. 6:** Erlaubnistatbestände für Datenverarbeitung (insbesondere wichtig für die Weiterleitung der Bestandsdaten über die Nutzer von der Heimathochschule an den Cloudanbieter)
- **Art. 12-23:** Informationspflichten und Auskunftsrechte des Betroffenen
- **Art. 24:** Pflichten des Verantwortlichen
- **Art: 25:** Privacy by default und by design
- **Art. 26:** Relevante Pflichten bei gemeinsamer Verantwortlichkeit
- **Art. 28:** Regelungen zur Auftragsdatenverarbeitung (mindestens im Verhältnis zum Endnutzer relevant, ggf. auch im Auftrag einer anderen Hochschule)