Datenschutzrechtliche Bewertung des Projekts „OA-Statistik“

I. Sachverhalt

- Erzeugung von **Nutzungsstatistiken** durch Auswertung von Dokumentenaufrufen bei **Repositorien** und Anfragen an **Linkresolverserver**
- **Erhebung und Verwendung** von bei der Nutzung anfallenden/erzeugten Daten wie IP-Adresse des Nutzers, Tag und Uhrzeit der Ausführung, Dateipfad und Dateiname des angeforderten Dokuments, HTTP-Methode, HTTP-Statuscode, Größe des angeforderten Dokuments in Byte, übertragene Byte, Spezifikation des vom Nutzer eingesetzten Clients (User-Agent), bibliotheksinterne Dokumenten-ID, Referrer-Angabe im HTTP-Header, ggf. Accept-Header
- **Bereinigung** um Mehrfachzugriffe unter derselben IP-Adresse innerhalb bestimmter Zeitfenster (server- und einrichtungsübergreifend) sowie um automatisierte Dokumentenaufrufe (insb. Crawler)
- Erfassung und Pseudonymisierung der Daten durch **Data-Provider**, Auswertung der Daten durch **Service-Provider**

II. Datenschutzrechtliche Bewertung

1. Anwendbares Recht

Datenschutzrechtliche Anforderungen gelten nur bei der Verarbeitung **personenbezogener Daten**:

Personenbezogene Daten sind Einzelangaben über **persönliche oder sachliche Verhältnisse** einer **bestimmten oder bestimmbaren** natürlichen **Person** (Betroffener).

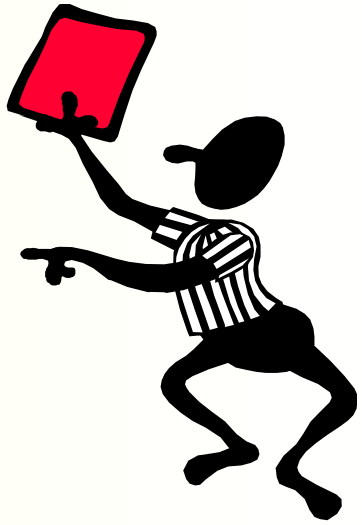
(§ 3 Abs. 1 LDSG)

IP-Adresse als personenbezogenes Datum; damit sind alle mit der IP-Adresse gespeicherten Daten personenbezogen

2. Verarbeitung von personenbezogenen Daten

Grundregel:

Was nicht ausdrücklich erlaubt ist, ist verboten.

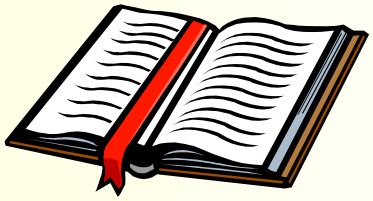


(sog. *Verbot mit Erlaubnisvorbehalt*)

3. Einschränkungen des Grundrechts

Zwei Möglichkeiten, in das Grundrecht auf informationelle Selbstbestimmung **in zulässiger Weise einzugreifen**:

1. **Rechtsvorschrift**



2. **Einwilligung** des Betroffenen

4. Datenschutzrechtliche Regelungen

Hochschulrecht

Personalrecht

Bereichsspezifische Regelungen

Statistikrecht

Medienrecht

Haben Vorrang vor den allgemeinen Datenschutzgesetzen!

Bundesdatenschutzgesetz

BDSG

Gilt für:

- Bundesbehörden
- Nicht-öffentliche Stellen
  z.B. Firmen, Vereine

Landesdatenschutzgesetz

LDSG

Gilt für:

- **Landesbehörden**
- Kommunen

6. Spezialregelung: Telemediengesetz (TMG)

a) Telemediendienst: (+) für Repositorien und Linkresolver

b) Anbieter-Nutzer-Verhältnis (keine rein dienstliche/studienbezogene Nutzung): (+)

Folge: datenschutzrechtliche Spezialvorschriften des TMG gelten

7. Verantwortlichkeit

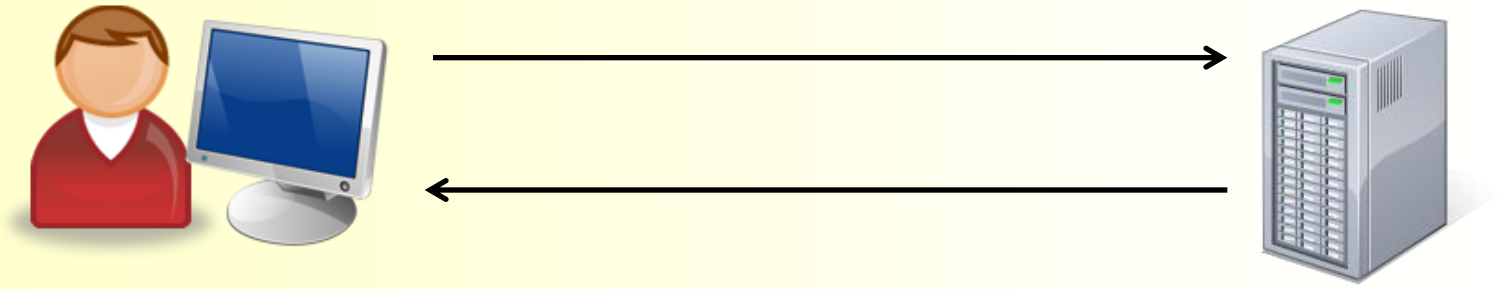
Verantwortlich für Einhaltung der datenschutzrechtlichen Bestimmungen: **Diensteanbieter/verantwortliche Stelle**

= diejenige juristische Person, die den Dienst zur Verfügung stellt (z. B. Universität, nicht Universitätsbibliothek als bloß funktionale Einheit)

Im Projekt OA-Statistik:

- **Data-Provider**
- **(Service-Provider)**

8. Verarbeitungsschritte beim Data-Provider



1. Webserver verarbeitet Nutzungsdaten zur Anzeige der Inhalte
2. Webserver speichert Nutzungsdaten in Webserver-Logfile
3. Weitere Verarbeitung (Pseudonymisierung, Übertragung an Serviceprovider)

9. Schritt 1: temporäre Verarbeitung von Nutzungsdaten zur Anzeige der Inhalte

Erlaubnisvorschrift: § 15 Abs. 1 TMG

Diensteanbieter (Data-Provider) darf personenbezogene Daten eines Nutzers nur erheben und verwenden, **soweit** dies **erforderlich** ist, um die **Inanspruchnahme von Telemedien zu ermöglichen**

Technisch sind für Diensterbringung **sämtliche** von den Data-Providern zu erfassenden **Daten erforderlich** (bis auf den Referrer) ; Referrer wird vom Client automatisch an den Webserver gesandt

10. Schritt 2: Speicherung der Nutzungsdaten in Webserverlogfiles und weitere Verarbeitung

- Nutzungsdaten müssen grundsätzlich unmittelbar nach Ende des Nutzungsvorgangs **gelöscht** werden
- **Ausnahme**: § 15 Abs. 3 TMG - für Zwecke der **Werbung**, der **Marktforschung** oder zur **bedarfsgerechten Gestaltung der Telemedien** dürfen pseudonyme Nutzungsprofile erstellt werden
- Open-Access-Statistik dient zumindest der bedarfsgerechten Gestaltung der Telemedien
- **Erforderlichkeitsgrundsatz** muss gewahrt sein! Insb. bei Speicherung des **Accept-Headers** fraglich. Nach Auffassung des ULD Auswertung des **Referrers** zulässig, wenn zwingend erforderlich für zulässige Nutzungsprofile

11. Pseudonyme Nutzungsprofile

Nutzungsdaten müssen **pseudonymisiert** werden!

= Ersetzen der personenbeziehbaren Daten durch Identifikationsmerkmale, die die Bestimmung der Betroffenen ausschließen oder wesentlich erschweren

Konsequenz: für den die Daten pseudonymisierenden Diensteanbieter sind die Daten weiterhin personenbezogen, für **Dritte** sind die Daten **anonym**

=> Data-Provider müssen IP-Adressen unverzüglich nach Erfassung durch Pseudonym ersetzen

12. Pseudonymisierung

- Unveränderte IP-Adressen sind **keine Pseudonyme**
- Daher: Pseudonymisierung durch **kryptologische Hashfunktion** (SHA-256), die aus IP-Adresse und zufällig erzeugtem Salt einen **Hashwert** generiert
- Salt ist **Geheimnis** und muss deshalb regelmäßig geändert werden (monatlich) und darf Dritten (insb. Service-Provider) nicht bekannt gegeben werden
- Alle **Data-Provider** können **dasselbe Salt** verwenden, solange sie keine Nutzungsdaten untereinander übermitteln

13. Kein Widerspruch des Nutzers

- Nutzer haben nach § 15 Abs. 3 TMG **Widerspruchsrecht** gegen Erstellung von Nutzungsprofilen (Opt-Out); hierauf müssen sie hingewiesen werden
- muss effektiv wahrgenommen werden können (z. B. Button-Lösung): **keine überhöhten Anforderungen** an Ausübung stellen; (Hinweispflicht beim Einsatz von Cookies beachten; temporäre Cookies verwenden)
- bei Widerspruch: Nutzungsdaten müssen **unmittelbar** nach Ende des Nutzungsvorgangs **gelöscht** werden, wenn Speicherung nicht anderweitig gerechtfertigt (alternativ: Erhebung/Verwendung nur **anonymer** Daten -> Anonymisierung der IP-Adresse)

14. Datenweitergabe an den Serviceprovider

- Serviceprovider kennt das Salt nicht. Damit sind Nutzungsdaten für diesen **anonym**. Weitergabe der Nutzungsdaten bedarf deshalb keiner datenschutzrechtlichen Rechtfertigung.
- Serviceprovider muss **keine datenschutzrechtlichen Anforderungen erfüllen**, da er keine personenbezogenen Daten verarbeitet

15. Allgemeine Informationspflichten der Data-Provider

- nach § 13 Abs. 1 TMG Unterrichtung d. Nutzer zu Beginn der Nutzung insb. über **die Art, den Umfang und die Zwecke** der Erhebung und Verwendung personenbezogener Daten („Datenschutzerklärung“) einschließlich Einsatz von Cookies
- vollständig, für Durchschnittsnutzer verständlich, jederzeit abrufbar

16. Verfahrensverzeichnis

- Nach Landesrecht muss verantwortliche Stelle (hier: Data-Provider) Verzeichnis führen, das **Informationen über die automatisierten Verfahren enthält**, mit denen personenbezogene Daten verarbeitet werden (prüfen, ob nach Landesrecht verbindliche Muster existieren!)
- in dieses ist Datenverarbeitung beim und durch den jeweiligen Data-Provider aufzunehmen
- enthält **öffentlichen** und (i. d. R.) **nichtöffentlichen** Teil

17. Auskunftsanspruch der Nutzer

- Betroffene haben grundsätzlich Anspruch auf **Auskunft** über die über sie gespeicherten **personenbezogenen Daten**
- Kommt im Projekt aufgrund der kurzzeitigen Speicherung personenbezogener Daten beim Data-Provider nicht in Betracht
- Service-Provider hat nur **anonyme Daten** gespeichert; hier besteht kein Auskunftsanspruch

(Beachte: allgemeine Informationspflicht der Nutzer nach § 13 Abs. 1 TMG und öffentlichen Teil des Verfahrensverzeichnisses)

18. Technische und organisatorische Maßnahmen

- Umsetzung der nach § 13 Abs. 4 TMG vorgeschriebenen technischen und organisatorischen Maßnahmen zum Datenschutz, d. h. Maßnahmen, die sicherstellen, dass
  - der Nutzer die Nutzung des Dienstes jederzeit beenden kann,
  - die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder ggf. gesperrt werden,
  - der Nutzer die Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
  - die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,
  - Nutzungsprofile nach § 15 Abs. 3 nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.

Fragen oder Anmerkungen zu diesem Thema?