# Informationspflichten auf Webseiten

Stand 28.06.2018

Dieses Dokument soll eine Hilfe dafür geben,

- in welchen Fällen Hinweise zur Erfüllung der Informationspflichten (ähnlich der früheren Datenschutzerklärung) bei einem Webauftritt notwendig sind,
- was inhaltlich enthalten sein muss und
- worauf nach der Erfahrung von ZENDAS ein besonderes Augenmerk zu richten ist.

Wenn man sich mit dem Thema beschäftigt, muss man als erstes verstehen, was der rechtliche Hintergrund ist.

## 1. Warum?

Nahezu bei jedem Webauftritt fand sich schon bislang eine Datenschutzerklärung. Der rechtliche Hintergrund war § 13 Abs. 1 des Telemediengesetzes (TMG). Danach hatte der Diensteanbieter „den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG […] in allgemein verständlicher Form zu unterrichten."

Nach dem 25.05.2018, also dem Zeitpunkt, ab dem die Regelungen der Datenschutz-Grundverordnung (DS-GVO) ihre Geltung entfalten haben, wird wohl überwiegend vertreten, dass § 13 TMG nicht mehr zur Anwendung kommt[1].

Damit gelten auch für die Datenverarbeitung bei Telemedien die Regelungen der DS-GVO.

Und diese sieht bei **der Erhebung von personenbezogenen Daten** Informationspflichten vor (Art. 13 und Art. 14 DS-GVO). Es bedarf dieser Informationen also dann, wenn beim Aufruf bzw. auf den Webseiten personenbezogene Daten erhoben werden.

[1] Siehe „Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 26. April 2018; abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Positionsbestimmung-TMG.pdf

Der Begriff „Datenschutzerklärung“ ist möglicherweise vor diesem Hintergrund verwirrend, weil man mit ihm die frühere Rechtslage nach TMG assoziiert. Um zu verdeutlichen, dass der rechtliche Hintergrund jetzt ein anderer ist, werden wir im Folgenden von den „Informationspflichten nach Art. 13 DS-GVO“ sprechen[2].

## 2. Was muss inhaltlich rein?

### 2.1. Welche Situationen müssen beschrieben werden? Und wo?

Bei einem Webauftritt wird man wohl zwei Situationen unterscheiden müssen:

a) Personenbezogene Daten werden schon beim Aufruf einer Webseite erhoben (insbesondere Protokolldaten, beim Einsatz von Cookies, bei Nutzung von Analyseprogrammen (z.B. Piwik/Matomo)).
b) Personenbezogene Daten werden auf bestimmten Webseiten vom Nutzer erhoben, um bestimmte Dienste anzubieten (z.B. Newsletterbestellung, Kontakt- und Anmeldeformulare, Login zum Zugang zu einem geschützten Bereich).

Die unter a) genannte Situation ist die, die auf jeden Fall in die „Informationen nach Art. 13 DS-GVO“ auf eine Webseite gehören, auf die also gleichberechtigt wie das Impressum verlinkt wird[3].

Viele verantwortliche Stellen (=Verantwortlicher im Sinne der DS-GVO) „packen“ in diese „Informationen nach Art. 13 DS-GVO“ (eine Bezeichnung nach wie vor als „Datenschutzerklärung“ ist nach unserem Dafürhalten unschädlich) alles rein. D.h. dort finden sich auch die Informationen für den Fall einer Newsletterbestellung und eines Kontaktformulars. Das führt dann dazu, dass diese Informationen sehr lang werden.

Auf der Seite, auf der die eigentliche Datenerhebung stattfindet, müsste dann unseres Erachtens mindestens ein Link sein auf die allgemeinen „Informationen nach Art. 13 DS-GVO“. Vor dem Hintergrund der Rechenschaftspflichten sollte sich der Verantwortliche überlegen, ob nicht sogar ein Kästchen zum Anhaken vorgesehen wird („Mir wurden Informationen zum Datenschutz [LINK] bei der Erhebung mitgeteilt und zur Verfügung gestellt“).

[2] Interessant in diesem Zusammenhang, dass der LfDI BW in seinem Webauftritt statt „Datenschutzerklärung“ einen Menüpunkt „Informationen gemäß Art. 13 DS-GVO“ hat; siehe https://www.baden-wuerttemberg.datenschutz.de/datenschutz/.
[3] Bei der Frage „**Wo müssen die Informationen platziert sein?“**, wird man sich an den bisherigen Anforderungen an das Impressum orientieren können: https://www.zendas.de/themen/internetrecht/impressum.html

Hinweis: Machen Sie bitte kein Kästchen zum Anhaken mit dem Text „Ich habe die Informationen zum Datenschutz gelesen und bin damit einverstanden“. Dies wäre eine **Einwilligung**. Um die geht es hier aber gerade nicht, sondern es geht (lediglich) um die Erfüllung der Informationspflichten, die sich der Verantwortliche möglichst dokumentieren lassen sollte.

Statt jegliche Datenerhebungen des gesamten Webauftritts zentral auf eine Seite zu packen, besteht auch die Möglichkeit, in die „Informationen nach Art. 13 DS-GVO“ nur das reinzuschreiben, was die Erhebung personenbezogener Daten beim Aufruf einer Webseite allgemein betrifft (also entsprechend der früheren Datenschutzerklärung nach Telemediengesetz; Situation a)), und die Informationen, die bei Datenerhebungen auf anderen Seiten des Webauftritts (Situation b)) notwendig werden, auch direkt dort zu geben (also – um bei dem Beispiel zu bleiben - auf der Seite der Newsletterbestellung und beim Kontaktformular).

Aus unserer Sicht wird durch eine solche Aufteilung mehr Transparenz hergestellt als bei einer einzigen, im Zweifel sehr langen „Information nach Art. 13 DS-GVO“.

Dies hängt jedoch auch davon ab, in welchem Umfang Datenerhebungen in der Webpräsenz stattfinden.

Letztlich ist dieses „Wo?**“** derzeit wohl eine „Glaubensfrage“ und erst die Zukunft wird es weisen, was Rechtsprechung und Aufsichtsbehörden dazu meinen.

## 2.2. Welche Informationen müssen rein?

Welche Hinweise in den „Informationen nach Art. 13 DS-GVO“ gegeben werden müssen, ergibt sich aus unserer Webseite „Informationspflichten nach DS-GVO bei Datenerhebung“[4], insbesondere der dortigen Tabelle.

Es ist zu beachten, dass in dem Fall, in dem Daten zwar beim Betroffenen erhoben werden, aber ohne seine Kenntnis, die Informationspflichten nach Art. 14 Abs. 1 lit. d DS-GVO (wie im Falle einer Erhebung bei Dritten) zu erfüllen sind.
Konkret: Die IP-Adresse wird beim Aufruf einer Webseite in der Regel protokolliert. Dies geschieht aber schon im Moment des Seitenaufrufs und ohne dass der Nutzer davon Kenntnis erhält. Damit muss auch über die „Datenkategorien, die verarbeitet werden“ (also im Beispiel die IP-Adresse) informiert werden[5].

[4] https://www.zendas.de/themen/informationspflichten.html
[5] Siehe S. 2 im Kurzpapier Nr. 10 der Datenschutzkonferenz „Informationspflichten bei Dritt- und Direkterhebung“, abrufbar unter https://www.lda.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf

Typische Konstellationen, die mit den erforderlichen Angaben in den „Informationen nach Art. 13 DS-GVO“ beschrieben werden müssen, sind:

- Schreiben von Protokolldaten: Aus der Rechtsprechung des EuGH folgt, dass IP-Adressen grundsätzlich als personenbezogene Daten zu qualifizieren sind[6].
- Cookies: Das Thema Cookies muss unter dem Gesichtspunkt der „Informationen nach Art. 13 DS-GVO“ nur dann behandelt werden, wenn in irgendeiner Form dadurch personenbezogene Daten erhoben werden, beispielsweise eine ID, die einer Person zugeordnet werden kann.
  Daher ist für jedes Cookie zu klären, welchen Inhalt es hat und was der Zweck ist.

## 2.3. Wo liegen die Problempunkte?

### 2.3.1. Aufbau

Die erste Fragestellung dürfte sein, wie die „Informationen nach Art. 13 DS-GVO“ aufgebaut werden. Dies hängt auch davon ab, wie die verantwortliche Stelle für sich die Frage entscheidet, ob sie **eine zentrale** Information vorhalten möchte (siehe Punkt 2.1.).

Nach unserer Erfahrung bietet sich folgende Gliederung an:

a. Verantwortlicher
b. Datenschutzbeauftragter
c. Beschreibung der einzelnen Erhebungsvorgänge (nachstehend einige Beispiele):
    aa. Bereitstellung der Webseite und Erstellung von Logfiles
        i. Beschreibung und Kategorien von Daten
        ii. Zweck
        iii. Rechtsgrundlage
        iv. Empfänger
        v. Dauer der Speicherung
        vi. Folgen der Nichtangabe, Widerspruchs- bzw. Beseitigungsmöglichkeit
    bb. Nutzung von Cookies
        i. …
    cc. Nutzung von Matomo
        i. …
    dd. …
d. Ihre Rechte
e. Ggf. Informationen zu Social-Media-Elementen: Hinweis auf nicht unmittelbare Einbettung

[6] https://www.zendas.de/themen/protokollierung/telemediendienst/eugh.html

### 2.3.2. Kontaktdaten des/der Datenschutzbeauftragte/n

Bitte achten Sie darauf, dass von der Person des/der Datenschutzbeauftragte/n **kein Name** anzugeben ist. Das Gesetz fordert in Art. 13 Abs. 1 lit. b DS-GVO nur dessen/deren Kontaktdaten (übrigens im Unterschied zu den Angaben zum Verantwortlichen, bei dem immer auch der Name anzugeben ist, vgl. Art. 13 Abs. 1 lit. a DS-GVO).

### 2.3.3. Cookies

Wie oben schon angesprochen bereitet das Thema Cookies oft erhebliche Probleme. Es muss mit den Webseitenverantwortlichen geklärt werden, welche Cookies zu welchem Zweck gesetzt werden und ob dadurch personenbezogene Daten erhoben werden. Ist letzteres der Fall, muss darüber umfassend aufgeklärt werden.

### 2.3.4. Tracking

Oft eng verknüpft mit dem Thema Cookies ist die Frage, ob der Nutzer getrackt wird. Ist dies personenbezogen der Fall, müssen dazu die Informationen nach Art. 13 DS-GVO gegeben werden.

### 2.3.5. Social Media Plugins / Einbettung Inhalte von Drittanbietern (z.B. Google Maps)

Auf Websites sollen oft Komponenten von verschiedenen Drittanbietern eingesetzt werden, um weitere Inhalte zur Verfügung zu stellen. Dazu gehören z.B. YouTube- und Vimeo-Videos sowie Share- und Like-Buttons von Social Media-Plattformen.
Würden die von den Drittanbietern zur Verfügung gestellten Social-Media-Elemente unmittelbar in die Webseite eingebettet werden, würden schon beim Laden der Webseite, auf der sie integriert sind, die URL der gerade geladenen Webseite, die IP-Adresse sowie ggf. weitere Informationen (z.B. Browsertyp) an den Drittanbieter übermittelt sowie ggf. Cookies der Drittanbieter gesetzt. Das Ganze geschähe auch dann, wenn die Nutzer nicht bei dem Drittanbieter angemeldet oder dessen Mitglied sind.
Wären die Nutzer zusätzlich beim Aufruf der Webseite bei dem Drittanbieter angemeldet, könnte er weitere Informationen ihren dortigen Benutzerkonten zuordnen (z.B. welches Video der Nutzer aufruft, welchen Kommentar der Nutzer abgibt, welche Informationen der Nutzer teilt, etc.).

Datenschutzrechtlich wäre diese vom Webseitenbetreiber zumindest mit veranlasste Weitergabe von personenbezogenen Daten **nur auf der Basis der Einwilligung** möglich.

Deshalb dürfen aus datenschutzrechtlicher Sicht Social-Media-Elemente von Drittanbietern **nicht direkt eingebettet** werden. **Vielmehr müssen Lösungen zum Einsatz kommen, bei denen erst nach einem bewussten Anklicken des Social-Media-Elements eine Verbindung zum Server des Drittanbieters aufgebaut und die damit verbundene Datenverarbeitung ausgelöst wird.**

Diese Lösungen sind oft unter den Begriffen „Zwei-Klick-Lösung", „Shariff" oder – neu – „Embetty" zu finden.

Da der Begriff „Social Media Plugins" unscharf ist: Denken Sie bitte daran, dass dies für die Einbindung auch weiterer Inhalte von Drittanbietern dient, z.B. bei der Einbindung von Kartendiensten.
Wenn sich keine Zwei-Klick-Lösung umsetzen lässt, bleibt im Grunde nur der Weg, die Inhalte – natürlich unter Klärung der urheberrechtlichen Fragestellungen – lokal zu speichern und vom eigenen Server auszuliefern.

### 2.3.6. Rechtsgrundlage

Oft ist es alles andere als einfach, sich über die Rechtsgrundlage klar zu werden. Aus der Formulierung „mindestens" in Art. 6 DS-GVO wird auch deutlich, dass mehrere Tatbestände dieser Vorschrift einschlägig sein können.

Die Frage nach der Rechtsgrundlage stellt sich für Hochschulen insbesondere, weil im Grunde immer an Art. 6 Abs. 1 lit. e DS-GVO in Verbindung mit Absatz 3 in Verbindung mit einer Vorschrift des Landesrechts (z.B. § 4 LDSG BW) zu denken ist. Denn Hochschulen arbeiten „in Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt" – dies ist durch das Hochschulrecht geregelt. Dies ist aber nach unserer Auffassung nicht die einzig denkbare Rechtsgrundlage:

**Beispiel: Newsletter**

Auch einen Newsletter gibt die Hochschule in Erfüllung ihrer Aufgaben heraus – so ist z.B. nach § 2 Abs. 8 Landeshochschulgesetz BW die Unterrichtung der Öffentlichkeit über die Erfüllung der Aufgaben und erzielten Ergebnisse Aufgabe der Hochschule. Also ist die Rechtsgrundlage Art. 6 Abs. 1 lit. e DS-GVO in Verbindung mit Absatz 3 in Verbindung mit § 4 LDSG BW?

Tragen sich für den Newsletter die betroffenen Personen selbst ein und wird ein Double-Opt-in durchgeführt, kann man auch an die Einwilligung als Rechtsgrundlage denken –

also Art. 6 Abs. 1 lit. a DS-GVO (so macht es übrigens der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Baden-Württemberg bei seinem Newsletter).

Und im Grunde gibt man doch mit der Angabe der E-Mailadresse bei einer Newsletterbestellung eine Willensäußerung ab, dass man gerne den Newsletter beziehen möchte, die Eintragung in den Verteiler ist die Annahme – also kann man an einen Vertrag denken und damit an die Rechtsgrundlage Art. 6 Abs. 1 lit. b DS-GVO.

Dieses einfache Beispiel zeigt, wie schwierig eine klare Festlegung ist. Da auch nicht nur **eine** Rechtsgrundlage einschlägig sein muss, sind möglicherweise auch alle aufgezählten richtig.
In der Praxis führt dies dazu, dass unterschiedliche Stellen auch unterschiedliche Rechtsgrundlage für ein- und denselben Sachverhalt in ihre „Informationen nach Art. 13 DS-GVO“ schreiben.

Hier wird leider erst mit der Zeit durch Aufsichtsbehörden und/oder Rechtsprechung Rechtssicherheit entstehen können.

**Beispiel: Protokollierung von IP-Adressen**

Eine Protokollierung von IP-Adressen bei einem Webserver dient – so oft die Begründung – der Sicherstellung des ordnungsgemäßen Betriebs.
Was ist die Rechtsgrundlage dafür?

Die Hochschule darf ihren Webserver nur in Erfüllung ihrer Aufgaben betreiben, also ist an Art. 6 Abs. 1 lit. e DS-GVO in Verbindung mit Absatz 3 in Verbindung mit § 4 LDSG BW als Rechtsgrundlage zu denken.

Stutzig macht aber Erwägungsgrund 49 der DS-GVO, der im Zusammenhang mit Daten zur Gewährleistung der Netz- und Informationssicherheit davon spricht, dass auch „Behörden“ ein „berechtigtes Interesse“ daran haben. Mit den „berechtigten Interessen“ wird die Referenz zu Art. 6 Abs. 1 lit. f DS-GVO hergestellt. Buchstabe f gilt allerdings „nicht für die von Behörde in Erfüllung ihrer Aufgaben vorgenommenen Verarbeitung“. Also ein Widerspruch zwischen Rechtsnorm und Erwägungsgrund, der Behörden doch ausdrücklich nennt?
Es gibt die Argumentation, dass die eingeschränkte Geltung des Art. 6 Abs. 1 lit. f DS-GVO daher rührt, dass der Grundsatz des Gesetzesvorbehalts für staatliches Handeln nicht umgangen werden soll. Dieses zeichnet sich durch eine Sonderrechtsbeziehung zwischen Bürger und Behörde, oftmals auch durch ein Über-/Unterordnungsverhältnis

aus. An einem solchen fehlt es aber bei einem Webauftritt. Hier treten sich Behörde und Nutzer wie Privatrechtssubjekte gegenüber.
Nach dieser Argumentation kann also die Rechtsgrundlage für die Protokolldaten Art. 6 Abs. 1 lit. f DS-GVO sein.

### 2.3.7. Empfänger

Denken Sie daran, dass Empfänger nach der DS-GVO nicht nur externe Personen/Stellen sind, sondern auch hochschulinterne Personen und Stellen (das steht in Art. 4 Nr. 9 DS-GVO). Diese sind in den „Informationen nach Art. 13 DS-GVO“ zu benennen.

- Wenn also bei einer Konferenzanmeldung Catering angeboten wird, das die Hochschule hinterher bezahlt, geht in aller Regel an die Haushaltsabteilung eine Teilnehmerliste – diese ist dann als Empfänger zu nennen.
- Bei einer Stellenausschreibung sind Empfänger der Bewerbungsunterlagen nicht nur die Auswahlkommission der Untereinheit, sondern die Personalabteilung sowie Personalvertretung und ggf. die verschiedenen Beauftragten (Schwerbehindertenvertretung, Beauftragte für Chancengleichheit).
- Protokolldateien des Webservers, die zur Sicherstellung des ordnungsgemäßen Betriebs geschrieben werden, werden ggf. an Ermittlungsorgane weiter gegeben.

### 2.3.8. Dauer der Speicherung

Probleme bereitet in der Praxis oft die Angabe der Speicherdauer. Unzureichend dürften Formulierungen sein, die lapidar ausführen, „das Kriterium für die Dauer der Speicherung von personenbezogenen Daten ist die jeweilige gesetzliche Aufbewahrungsfrist“.
Dies entspricht nicht den Anforderungen von Art. 12 DS-GVO nach transparenten, verständlichen und präzisen Ausführungen.

Ohnehin muss die verantwortliche Stelle im Rahmen des Verzeichnisses von Verarbeitungstätigkeiten Farbe zur Speicherdauer bekennen. Daher müssen sowieso klare Festlegungen zur Speicherdauer getroffen werden.

> **Beispiel Protokolldaten**: Werden IP-Adressen in den Protokolldaten zur Sicherstellung des ordnungsgemäßen Betriebs gespeichert, so hat der BGH für Telekommunikationsdienste eine Speicherdauer von 7 Tagen nicht beanstandet[7]. Diese Rechtsprechung wird nach Ansicht auch der Bundesbeauftragten für den Datenschutz und

[7] Urteil vom 03.04.2014 (III ZR 391/13), abrufbar unter http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=68350&pos=0&anz=

die Informationsfreiheit auf Telemediendienste übertragen[8]. Das Argument, dass die Rechtsprechung eine längere Speicherung nicht ausgeschlossen hat, ist zwar grundsätzlich richtig. Jedoch hat der BGH in seiner Rechtsprechung betont, dass dann, wenn eine kürzere Speicherung als 7 Tage ausreichend ist, die kürzere Speicherdauer umzusetzen ist. Möchte man länger als 7 Tage speichern, hat man erheblichen Argumentationsaufwand und Rechtsunsicherheit, wie dies die Rechtsprechung beurteilen wird. Daher ist von einer längeren Speicherung als 7 Tage abzuraten.

### 2.3.9. Rechte

Die betroffenen Personen sind über das Bestehen von bestimmten Rechten aufzuklären – und zwar nach Art. 12 DS-GVO „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“.
Folgende Rechte kommen in Betracht:

- Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Datenverarbeitung.
- Recht auf Datenübertragbarkeit
- Recht auf Widerruf einer Einwilligung und die Tatsache, dass die Rechtmäßigkeit der Verarbeitung aufgrund der Einwilligung bis zum Widerruf nicht berührt wird.

Das führt oft dazu, dass sich unüberlegt diese ganze Latte von Rechten in den „Informationen nach Art. 13 DS-GVO“ findet.

- Dabei wird nicht bedacht, dass auf das Recht auf Widerruf einer Einwilligung nur hinzuweisen ist, wenn auch tatsächlich eine Einwilligung eingeholt wurde. Ist das nicht der Fall und beinhalten die Informationen nach Art. 13 DS-GVO dennoch das Widerrufsrecht, führt das nach unserem Dafürhalten zur Verwirrung und stellt somit die Verständlichkeit der Information in Frage.

- Vergleichbares gilt für das Recht auf Datenübertragbarkeit. Dieses Recht besteht nach Art. 20 Abs. 1 DS-GVO nur, wenn die Verarbeitung auf einer Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO, Art. 9 Abs. 2 lit. a DS-GVO) oder auf einem Vertrag (Art. 6 Abs. 1 lit. b DS-GVO) beruht. Dieses Recht gilt jedoch nach Art. 20 Abs. 3 S. 2 DS-GVO nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.
  Anders gesagt: Ob das Recht auf Datenübertragbarkeit wirklich besteht, sollte man prüfen, bevor man den betroffenen Personen mitteilt, dass sie dieses Recht haben.

[8] Pressemitteilung der BfDI vom 20.10.2016, abrufbar unter https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2016/15_BfDIBegruesstUrteilEuGHIPAdressen.html

Ansonsten bestehen wieder Bedenken, ob die Informationen ausreichend verständlich sind.