# Webseiten

**Webseiten** meint für diesen Artikel vor allem solche Seiten die frei zugänglich im Internet stehen. Sie stellen eine besondere Herausforderung für den Datenschutz dar, weil sie das Aushängeschild einer Organisation darstellen. In teilweise abgeschwächter Form gelten die Aussagen in diesem Artikel natürlich auch für Seiten, die nur geschlossenen Gruppen zugänglich sind (**Intranet**).

Webseiten bedeuten zwangsläufig, dass Personenbezogene Daten verarbeitet werden.

## Personenbezogene Daten

### IP-Adresse

Das betrifft zunächst die IP-Adressen der Nutzer der Webseite.[1)] Damit sind auch alle darauf aufbauenden Verarbeitungen durch Analysetools grundsätzlich Verarbeitungen personenbezogener Daten.

### Cookies

Ein weiteres eher technisches Thema sind Cookies. Cookies sollten möglichst sparsam eingesetzt werden auch wenn sie nur dem Komfort des Webseitenbesuchers dienen und sich am Ende des Besuchs selbst löschen (Session-Cookies). Auf weitergehende Cookies (Tracking-Cookies) sollte möglichst komplett verzichtet werden.

### Einbindung von Drittanbietern

Auch Angebot von Drittanbietern sollten sparsam genutzt werden: Like-Button, Zählpixel und ähnliche Gadgets[2)] helfen vor allem den jeweiligen Anbietern Nutzerprofile zu erstellen. Eine ungefährlichere Alternative ist es, wenn beispielsweise ein Link zu einer Facebookseite in die Webseite integriert werden soll, nur eine Graphik mit einem einfachen Hyperlink zu verwenden. Damit fließen erst dann Daten zu Facebook, wenn der Webseitenbesucher auf Link klickt (und folglich willentlich auf eine Seite von Facebook geht).

### Personenbezogene Daten in den Inhalten von Webseiten

Ein weiteres typisches Thema ist, dass auf einer Webseite für die Inhalte Daten von Menschen, insbesondere Mitarbeitern, verwendet werden. Das können zum Beispiel Bilder sein oder auch Kontaktdaten, wie Telefonnummer oder Emailadresse. Auch dadurch liegt eine Verarbeitung personenbezogener Daten vor.

# Rechtmäßigkeit der Verarbeitung

## Besucher

Wie immer bei der Verarbeitung personenbezogener Daten ist dies nur zulässig, wenn die Rechtmäßigkeit der Verarbeitung sichergestellt ist. Für Besucher von Webseiten wird als Rechtfertigungsgrund vielfach auf die Einwilligung mit all ihren Nachteilen zurückgegriffen werden müssen (Details siehe Artikel Einwilligung). Allerdings sollten gerade öffentliche Einrichtungen bedenken, dass die Nutzung von Webseiten nicht immer freiwillig ist sondern bisweilen einem faktischen Zwang unterliegt, der teilweise wesentlich stärker ist, als dass was eher für die Privatwirtschaft unter dem Stichwort Kopplungsverbot diskutiert wird: Wenn an einer Hochschule eine Lehrveranstaltung nur sinnvoll besucht wird, wenn gleichzeitig notwendige Unterlagen für die Lehrveranstaltung nur über moodle zur Verfügung gestellt werden (Skripten, E-Learning-Bausteine, digitale Kopien aus Lehrbüchern soweit zulässig) dann ist die Einwilligung der Studierenden in die Verarbeitung personenbezogener Daten bei moodle keinesfalls mehr freiwillig und folglich unwirksam.

## Inhalte von Webseiten

Auch wenn die Inhalte von Webseiten personenbezogene Daten beinhalten wird der erste Impuls häufig lauten, Einwilligung einzuholen. Gerade bei Mitarbeitern (Siehe auch Beschäftigtendatenschutz.) sind aufgrund von Art. 88 DSGVO und darauf gestützt § 26 BDSG bzw. die jeweiligen Landesdatenschutzgesetze die Hürden für eine wirksame Einwilligung außerordentlich hoch. Eine Alternative sind vergütete Model-Verträge mit der Folge, dass der Rechtfertigungsgrund nicht mehr die Einwilligung sondern die Erfüllung eines Vertrages ist. Auch die Erfüllung einer rechtlichen Verpflichtung und die Wahrnehmung einer Aufgabe kommen in Betracht. Allerdings sollte auch der Grundsatz der Datenminimierung bzw. das Erforderlichkeitsprinzip strikt beachtet werden. Dienstliche(!) Emails und Telefonnummern sowie Sprechzeiten und in der Regel auch die Namen zuständiger Mitarbeiter werden also meist erforderlich sein. Ob sich eine Mitarbeiterin in Mutterschutz/Elternzeit befindet, ist dagegen nicht erforderlich anzugeben.

# Betroffenenrechte

Unabhängig von Rechtfertigungsgrund sind die Betroffenenrechte zu wahren.

## Infrastruktur für Widerruf/Widerspruch

Das bedeutet insbesondere, dass für den Fall von Einwilligungslösungen eine funktionierende Infrastruktur für die unverzügliche Bearbeitung eines etwaigen Widerrufs der Einwilligung vorgehalten werden muss.

Soweit ein Widerspruch zulässig ist, muss auch dafür die nötige Infrastruktur vorgehalten werden.

### Datenschutzerklärung

Das bekannteste Thema ist sicherlich die Datenschutzerklärung. Es gibt eine gewisse Palette von Generatoren, die teilweise auch eine recht ordentliche Qualität liefern. Allerdings gibt es eine Tendenz gerade von automatisch erstellten Datenschutzerklärungen, Besucher mit irrelevanten Informationen zu überschütten (z.B. Informationen über die Rechtmäßigkeit der Verarbeitung zum Schutz lebenswichtiger Interessen bei einer harmlosen Webseite). Hier ist weniger in der Regel mehr. Nicht beachtet wird im Übrigen regelmäßig, dass auch für andere Gruppen von betroffenen Personen (z.B. abgebildete Mitarbeiter) Datenschutzerklärungen zur Verfügung gestellt werden müssen - allerdings in der Regel nicht öffentlich sondern nur für die betroffenen Personen.

Zur Erreichbarkeit der Datenschutzerklärung: Auch wenn es Ausnahmen gibt, sollte für eine gute Handhabbarkeit eine 1-Klick Politik gelten: Die Datenschutzerklärung sollte für einen Besucher von jeder (Unter-)Seite aus mit einem Klick erreichbar sein.

Für Mitarbeiter genügt es aber in der Regel, wenn alle betroffenen Arbeitnehmer die Datenschutzerklärung mit geringem Aufwand im Intranet heraussuchen können.

## Sicherheit der Verarbeitung

Personenbezogene Daten müssen sicher verarbeitet werden (Vgl. Art. 32 DSGVO). Wichtigster Punkt dürfte die Verschlüsselung sein.

## To Do

- Sparsamer Umgang mit Cookies
- Vorsicht bei Einbindung von Drittanbietern
- Datenschutzerklärung für Besucher mit einem Click erreichbar
- Verschlüsselung
- Standardisiertes CMS verwenden (vor allem, wenn Nutzer Eingaben tätigen können und/oder eine Datenbank angebunden ist)
- Personenbezogene Daten nur im Rahmen der Rechtsgrundlagen und der Erforderlichkeit online stellen
    - namentlich benannte Ansprechpartner und dienstliche Telefonnummern sind in der Regel in Ordnung
    - nicht in Ordnung sind in aller Regel weitergehende persönliche Daten: Familienstand, Elternzeit, Kinder, Geburtstag

Artikel

1)
Der EuGH ordnet IP Adressen immer als personenbezogenes Datum ein. Vgl. heise.de:EuGH korrigiert Urteil zum Datenschutz von IP-Adressen

2)
Vgl. in der Wikipedia Zählpixel und in der englischen Wikipedia Web beacon und Facebook like button