

Social Media und eingebettete Komponenten von Drittanbietern

Hintergründe und Praxistipps

Datenschutzerklärung

Wer personenbezogene Daten- dazu gehört auch die IP-Adresse – verarbeitet, muss die Informationspflichten der Datenschutz-Grundverordnung (DSGVO) beachten. Das gilt auch für Webseiten. In der Praxis hat sich eingebürgert, dies in einer eigenen „Datenschutzerklärung“ zu tun. Diese sollte für sich stehen, also z.B. neben dem Impressum (nicht zu empfehlen: im Impressum) und mit einem eigenen Button angesteuert werden können. Außerdem kann und soll die Datenschutzerklärung auch dazu genutzt werden, Datenverarbeitungen nachvollziehbar (transparent) darzustellen (Transparenzgebot).

Tipp:

Die Datenschutzerklärung sollte von allen Sub-Seiten aus einfach (generell zu empfehlen: maximal zwei Klicks) erreichbar sein. Beispiel: Menüleiste am unteren oder oberen Bildschirmrand.

Der Nutzer (die DSGVO spricht vom „Betroffenen“) ist jedenfalls über folgende Punkte aufzuklären (Informationspflichten; Art 13, 14 DSGVO):

- Name/Firma und Kontaktdaten des Verantwortlichen (und allenfalls des Datenschutzbeauftragten)
- Zweck der Verarbeitung (vom Verantwortlichen zu definieren)
- Rechtsgrundlage (inkl. konkretem berechtigten Interesse) der Verarbeitung (von der DSGVO vorgegeben; Art 6 DSGVO)
- Kategorien der Empfänger der Daten
- Angabe, ob Daten in ein Drittland übertragen werden (diesfalls mit Angabe angemessener Garantien zur Einhaltung des Datenschutzes)
- Speicherdauer oder Kriterien der Speicherdauer
- Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch; bei Einwilligung: Widerrufsmöglichkeit der Einwilligung)
- Beschwerdemöglichkeit bei der Datenschutzbehörde
- Gegebenenfalls Auswirkungen von automatischen Entscheidungsprozessen inkl. Profiling
- Kategorien der bei Dritten erhobenen Daten
- Datenquelle bei von Dritten erhobenen Daten

Das Telekommunikationsgesetz (TKG) sieht eigene Informationspflichten für Datenverarbeitungen auf Webseiten (Cookies) vor: Es ist darüber zu informieren,

- welche Daten ermittelt, verarbeitet oder an Dritte übermittelt werden,
- auf welcher Rechtsgrundlage (z.B. aufgrund eines Vertrages, eines speziellen Gesetzes) und
- für welche Zwecke dies erfolgt und
- wie lange die Daten gespeichert werden.

Diese Informationspflichten decken sich größtenteils mit den allgemeinen Informationspflichten der DSGVO, weshalb die Informationen nach dem TKG gemeinsam mit den Informationen nach der DSGVO dem Betroffenen zur Verfügung gestellt werden können.

EuGH-Entscheidung Facebook Fanpage

In der EuGH-Entscheidung C-210/16 hat der EuGH ausgesprochen, dass nicht nur Facebook selbst, sondern auch der Betreiber einer Fanseite („Fanpage“) auf Facebook für die Daten, die Facebook von Besuchern der Fanseite erhebt, verantwortlich ist, also gemeinsam mit Facebook die Position des Verantwortlichen einnimmt. Diese Entscheidung ist zwar noch zur Vorgängerbestimmung der DSGVO ergangen, wird aber auch für die DSGVO berücksichtigt werden müssen.

Eine Konsequenz der Entscheidung besteht darin, dass auch für Seiten innerhalb von Facebook eine Datenschutzerklärung zur Erfüllung aller Informationspflichten erforderlich ist, insbesondere also welche Cookies gesetzt bzw. welche Daten zu welchen Zwecken auf Basis welcher Rechtsgrundlage erhoben werden.

Außerdem verlangt Art 26 DSGVO für diese Form der „gemeinsamen Verantwortlichen“ eine transparente Vereinbarung zwischen den gemeinsam Verantwortlichen, also zwischen dem Betreiber der Seite und Facebook, wer welche Informationspflichten (Art 13 u 14 DSGVO) erfüllt und wer den sonstigen Verpflichtungen der DSGVO nachkommt (insbes den Betroffenenrechten wie z.B. dem Auskunftsrecht).

Generell darf auch bei einer gemeinsamen Verantwortlichkeit eine Datenverarbeitung immer nur auf einer entsprechenden Rechtsgrundlage erfolgen.

Besondere Vorsicht ist geboten, wenn die Seite auch von außerhalb von Facebook angesteuert werden kann und Facebook so auch Daten von Besuchern erhält, die über kein Facebook-Konto verfügen. Hier kann jedenfalls nicht damit argumentiert werden, dass als Rechtsgrundlage für die Datenverarbeitung eine Zustimmung über die AGB von Facebook vorliegt.

Tipp:

Jede (unternehmerische) Seite auf Facebook sollte zumindest eine möglichst transparente Datenschutzerklärung enthalten.

Eingebettete Komponenten von Drittanbietern

Werden in die eigene Webseite Komponenten von Drittanbietern eingefügt, dann muss geklärt werden, ob von diesen Drittanbietern bzw. deren Webseiten Daten erhoben und verarbeitet werden (was bei „Gratisangeboten“ so gut wie immer der Fall ist) und was mit den Daten geschieht. Da jede Website im Hinblick auf Datenschutz möglichst transparent erstellt werden muss, sollten diese Informationen in die eigene Datenschutzerklärung integriert bzw. die Datenströme so gut wie möglich beschrieben werden.

Tipp:

Empfehlenswert ist eine Beschreibung in der eigenen Datenschutzerklärung (manche Anbieter bieten Mustertexte an) sowie zusätzlich eine Verlinkung auf die Datenschutzerklärung der jeweiligen Anbieter.

Auch hier darf eine Datenverarbeitung immer nur auf einer entsprechenden Rechtsgrundlage erfolgen.

Werden Webanalyse-Tools eingesetzt, wird in der Regel ein Auftragsverarbeiter-Vertrag geschlossen werden müssen. Dabei ist auch die Zuverlässigkeit des Auftragsverarbeiters zu prüfen, also die Frage, ob durch diesen die Einhaltung der jeweils erforderlichen technisch-organisatorischen Datensicherheitsmaßnahmen gewährleisten kann. Außerdem hat sich die Praxis eingebürgert, die IP-Adresse durch Löschung der letzten 8 Bit zu pseudonymisieren. Dadurch ist nur mehr eine grobe Lokalisierung möglich.

Einbetten von Social Media Plug-Ins (EuGH-Entscheidung Facebook-Like-Button)

Verwendet eine Website einen Facebook-Like Button, so überträgt der Button beim Laden der Seite die IP-Adresse, die Webbrowser-Kennung sowie Datum und Zeit des Aufrufs unabhängig davon, ob der Button angeklickt wurde oder der Nutzer über einen Facebook-Account verfügt an den Social Media Anbieter Facebook.

Der EuGH hat in der Entscheidung C-40/17 bei eingebetteten Social Media Plug-Ins wie im konkreten Anlassfall dem „Gefällt mir“-Button von Facebook ausgesprochen, dass für den Vorgang der Erhebung und der Weiterleitung der Daten an den Social Media Betreiber eine gemeinsame Verantwortung des Webseiten-Betreibers und des Social Media Anbieters vorliegt. Diese Verantwortung bezieht sich aber in der Regel nicht auf die Verarbeitungen durch den Social Media Anbieter nach der Übermittlung der Daten an ihn, sondern nur auf die Erhebung und Übermittlung der Daten. Neben einer entsprechenden Information über diesen Vorgang in der Datenschutzerklärung (siehe Ausführungen bereits oben), ist auch das Vorliegen einer Rechtmäßigkeitsgrundlage erforderlich. Dies wird bei eingebetteten Social Media Plug-Ins in der Regel eine Einwilligungserklärung sein.

Darüber hinaus ist jeder Betreiber einer Webseite verpflichtet, seine Webseite so datenschutzfreundlich wie möglich zu gestalten („privacy by design“).

Tipp:

In der Praxis hat es sich eingebürgert, ein zwei-Stufen-System zu verwenden, das erst beim zweiten Klick zum original Facebook-Button führt. So wird verhindert, dass auch Daten von Webseiten-Besuchern ausgelesen werden, die nicht gleichzeitig Nutzer von Facebook sind und damit den AGB von Facebook nicht zugestimmt haben. Als „Best Practice“ hat sich das „Shariff-Verfahren“ (ein Nachfolger des „Zwei-Klick-Verfahrens“) gezeigt.

Auf diese Weise kann auch die Einwilligungserklärung für die Erhebung und Übermittlung der Daten an den Social Media Betreiber eingeholt werden.

Rechtsgrund Einwilligung (opt in) und ihr Widerruf (opt out)

Nach dem TKG kann die Einwilligung als Rechtsgrundlage für eine Datenverarbeitung auch in der Browsereinstellung des Nutzers, die Cookies zulässt, gesehen werden. Das setzt aber voraus, dass die Nutzer (Betroffene) wissen, dass sie ihre Browser entsprechend konfigurieren müssen bzw. können und zu welchen Datenanwendungen sie ihre Einwilligung geben. Die Einwilligung muss immer durch ein „aktives Tun“ erfolgen. Daher hat es sich in der Praxis eingebürgert, dass sogenannte Cookie-Fenster aufpoppen, die über die Datenverarbeitung informieren und auf die Datenschutzerklärung verlinken, in der dann alle Informationen vollständig enthalten sind. Vorgekreuzte Einwilligungen sind jedenfalls unzulässig. Damit erfolgt die Einwilligung in der Praxis über ein aktives Anklicken im Cookie-Fenster (EuGH in der Entscheidung Planet 49).

Außerdem muss jede Einwilligung jederzeit widerrufbar sein. Darauf muss bereits bei der Einwilligung hingewiesen werden. Das heißt, dass auch für die Einwilligungen über die Browsereinstellungen ein geeignetes „opt out“ vorgesehen werden muss.

Tipp:

Eine Möglichkeit bestünde auch darin, die Nutzung der Website auch in einer (allenfalls eingeschränkten) Variante ohne Cookies anzubieten. Das aufpoppende Cookie-Fenster sollte zur Sicherheit nicht nur weggeklickt werden müssen, sondern besser auch eine kurze Einwilligungserklärung enthalten sein (Bsp: „akzeptiert“). Die genauere Erklärung der Funktionsweise des Cookies kann dann in der verlinkten Datenschutzerklärung erfolgen.

Best-Practice-Beispiel für die allenfalls notwendige Einwilligung zu Cookies: [Auswirkungen der EuGH-Judikatur auf die Einbindung von Cookies \(Planet 49\)](#).

Fazit

Ein allgemeines „Muster“, das nur abgeschrieben oder kopiert werden muss, ist daher nicht möglich bzw. bietet das beliebte „copy and paste“ nur den oberflächlichen Anschein, DSGVO-konform zu sein. Die Informationspflichten hängen immer vom Aufbau und den Funktionen der jeweiligen Webseite ab. Dazu ist nicht nur juristisches Wissen zur DSGVO notwendig, sondern auch ein erhebliches technisches Grundverständnis. Wir empfehlen daher für eine DSGVO-konforme Webseite spezialisierte IT-Dienstleister oder Unternehmensberater einzusetzen.

Darauf spezialisierte Anbieter finden Sie unter: [Unternehmensliste im WKO Firmen A-Z](#)

Weitere Informationen auf wko.at

- Checkliste für die Verwendung von Cookies: [Checkliste für Cookies und Webanalyse im Webshop](#).
- Informationen zur Einwilligung: [Datenverarbeitung im Webshop und auf der Website | Einwilligungserklärung - Cookies - Datenschutzerklärung](#)

Stand: 07.04.2021