

Typische Datenschutzfehler bei Webseiten und sozialen Medien?



Sommerakademie
am 12. September 2022
in Kiel

Wolfram Felber

0431 988-1652
ULD43@datenschutzzentrum.de
<https://www.datenschutzzentrum.de/>



www.datenschutzzentrum.de

Eingangsfragen

- Selber hosten (lassen) oder Social-Media-Plattformen nutzen?
 - Rechtslage gemeinsame Verantwortlichkeit
- Wie baue ich meine Seite?
 - Was ist erforderlich?
- Welche rechtlichen Vorgaben muss ich beachten?
 - TTDSG und DSGVO, TMG
 - Welche Verarbeitungen kann ich nur mit / ohne vorherige Einwilligung durchführen?
 - Typische Anwendungsfehler

Eigene Webseite oder Plattform?

- Wozu brauche ich die Webseite?
 - Unternehmenspräsentation?
 - Verein? NGO?
 - Dienstleistungen anbieten?
 - Veranstaltungen bewerben?
 - Waren absetzen? Shop?
 - Interaktion mit Nutzer:innen/Kund:innen?
 - Online-Presse?
 - Öffentlichkeitsarbeit der öff. Hand?
 - Vermarktung von Werbepläätzen auf Webseite?

Eigene Webseite/App oder Seite auf Social Media Plattform?

eigene Webseite	Seiten auf Social Media Plattformen
Gewisser initialer Aufwand (Dienstleister suchen)	wenig initialer Aufwand (Angebot am Markt für jeden leicht verfügbar)
Gewisse Kosten für Betrieb	Wenig Kosten für Erstellung
Volle Verantwortlichkeit	nur teilweise Verantwortlichkeit
Interaktionsmöglichkeiten müssen gebaut werden	Plattform baut auf Interaktion auf
Reichweitenmessung kann nur bedingt hinzugefügt werden	Reichweitenmessung integriert
Volle Verantwortlichkeit = volle Kontrolle = volle Entscheidungshoheit	teilweise Verantwortlichkeit = wenig Entscheidungsmöglichkeiten bzgl. Architektur und Gestaltung keine Kontrolle
Drittstaatenproblematik handhabbar	Drittstaatenproblematik
Schlanke Webseite = wenig Aufwand, um rechtskonformen Betrieb zu erreichen	Teil eines Systems = großer Aufwand, um rechtskonformen Betrieb zu erreichen (tönerne Füße)

Gemeinsame Verantwortlichkeit

- Bei Betrieb einer Seite auf Plattform: Rspr. zu „Fanpages“
 - Reichweite der gemeinsamen Verantwortlichkeit nicht auf Insights beschränkt
 - Pflichten als Verantwortlicher:
 - Art. 5 Abs. 1 DSGVO:
 - a) Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
 - b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden
 - c) ...
 - Art. 5 Abs. 2 DSGVO: Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können!

TTDSG

- Seit Dezember 2021 (Umsetzung der Cookie-Richtlinie aus 2009)
- Anbieter von Telemediendiensten = Seitenbetreiber
- § 25 TTDSG:

„Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen **eingewilligt** hat. [...]“

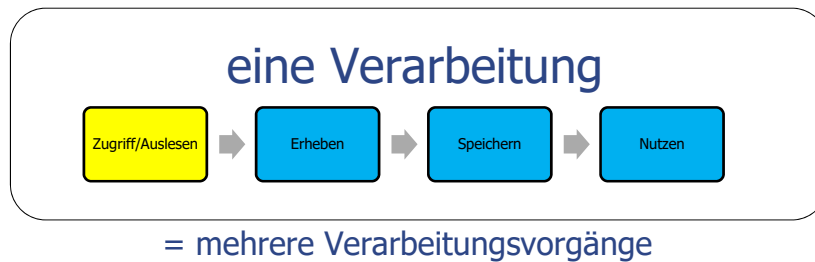
Ausnahme:
unbedingt erforderlich, damit ein **vom Nutzer ausdrücklich gewünschter Telemediendienst** zur Verfügung gestellt werden kann

Beispiele: Shopfunktion, Karten, Chatfunktion, usw. (hinreichend granular)

(s. DSK-Orientierungshilfe für Anbieter:innen von Telemediendiensten
[in Konsultationsphase])

Cookies auf Webseiten

- TTDSG und DSGVO



- = zwei Einwilligungen?
- -> eine Einwilligungshandlung!

Drittstaatentransfer

- Art. 44 DSGVO:

Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten

 - Wann ist es ein Transfer?

Bsp.: Niederlassung des Dienstleisters in EU, Zentrale in den USA

 - reicht Zugriffsmöglichkeit aus Drittstaat schon aus?
 - Risiko = Verarbeitung?
 - Bsp.: Google Fonts? LG München
 - Reichen nicht einfach SCCs aus?

Kurze Antwort: Einfach? Nein!
 - Wie lange noch? Und dann? Privacy Harbor?

ULD  www.datenschutzzentrum.de

Cookies auf Webseiten

- TTDSG und DSGVO



Leitlinien
Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679
angenommen am 25. Mai 2018

Gelegentliche und nicht wiederholte Übermittlungen

Der EDSA weist darauf hin, dass der Begriff „gelegentlich“ in Erwägungsgrund 111 und der Begriff „nicht wiederholt“ im Zusammenhang mit der Ausnahme zur Wahrung „zwingender berechtigter Interessen“ nach Artikel 49 Absatz 1 Unterabsatz 2 verwendet werden. Diese Begriffe deuten darauf hin, dass solche Übermittlungen zwar öfter als einmal, aber nicht regelmäßig erfolgen dürfen und sich außerhalb gewöhnlicher Abläufe zutragen, beispielsweise unter zufälligen, unvorhergesehenen Umständen und in beliebigen Zeitabständen. Eine Datenübermittlung etwa, die im Rahmen einer dauerhaften Beziehung zwischen dem Datenexporteur und einem bestimmten Datenimporteur regelmäßig erfolgt, ist grundsätzlich als systematisch und wiederholt anzusehen und kann deshalb nicht als gelegentlich oder nicht wiederholt betrachtet werden. Außerdem gilt etwa eine Übermittlung im Allgemeinen als nicht gelegentlich oder wiederholt, wenn der Datenimporteur eine generelle direkte Zugriffsmöglichkeit auf eine Datenbank hat (zum Beispiel über eine Schnittstelle zu einer IT-Anwendung).

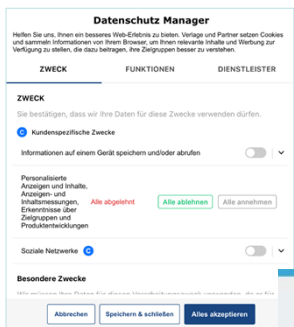
- = drei Einwilligungen?

Sommerakademie 2022: DS-Fehler bei Webseiten und sozialen Medien 9

ULD  www.datenschutzzentrum.de

Ablehnen auf erster Ebene?

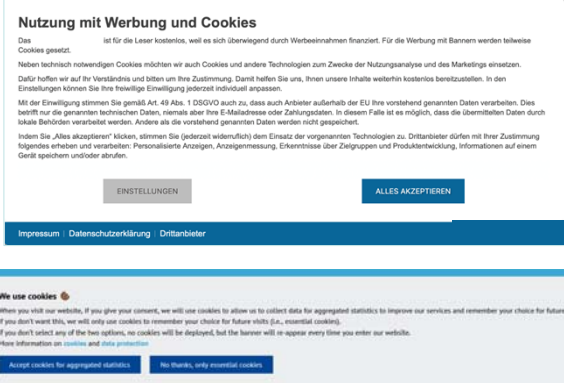
- Der sächsische Rochade-Test!



Datenschutz Manager

Helfen Sie uns, Ihnen ein besseres Web-Erlebnis zu bieten. Verlage und Partner setzen Cookies und sammeln Informationen von Ihrem Browser, um Ihnen relevantere Inhalte und Werbung zur Verfügung zu stellen, die dazu beitragen, Ihre Zielgruppen besser zu verstehen.

ZWECK	FUNKTIONEN	DIENSTLEISTER
<p>ZWECK</p> <p>Sie bestätigen, dass wir Ihre Daten für diese Zwecke verwenden dürfen.</p> <p>Kundenspezifische Zwecke</p> <p>Informationen auf einem Gerät speichern und/oder abrufen <input type="checkbox"/></p> <p>Personalisierte Anzeigen und Inhalte, Anzeigen- und Schaltflächenanfragen, Erkenntnisse über Zielgruppen und Produktentwicklungen</p> <p>Alle abgelehnt <input type="button" value="Alle ablehnen"/> <input type="button" value="Alle annehmen"/></p> <p>Soziale Netzwerke <input type="checkbox"/></p> <p>Besondere Zwecke</p> <p><input type="button" value="Abbrechen"/> <input type="button" value="Speichern & schließen"/> <input type="button" value="Alles akzeptieren"/></p>		



Nutzung mit Werbung und Cookies

Das ist für die Leser kostenlos, weil es sich überwiegend durch Werbeeinnahmen finanziert. Für die Werbung mit Bannern werden teilweise Cookies gesetzt.

Neben technisch notwendigen Cookies möchten wir auch Cookies und andere Technologien zum Zwecke der Nutzungsanalyse und des Marketing einsetzen. Dafür helfen wir auf Ihr Verständnis und bitten um Ihre Zustimmung. Damit helfen Sie uns, Ihren unsere Inhalte weiterhin kostenlos bereitzustellen. In den Einstellungen können Sie Ihre freiwillige Einwilligung jederzeit individuell anpassen.

Mit der Einwilligung stimmen Sie gemäß Art. 49 Abs. 1 DSGVO auch zu, dass auch Anbieter außerhalb der EU Ihre vorstehend genannten Daten verarbeiten. Dies betrifft nur die genannten technischen Daten, niemals aber Ihre E-Mail-Adresse oder Zahlungsdaten. In diesem Falle ist es möglich, dass die übermittelten Daten durch lokale Behörden verarbeitet werden. Anders als die vorstehend genannten Daten werden nicht gespeichert.

Indem Sie „Alles akzeptieren“ klicken, stimmen Sie (jederzeit widerruflich) dem Einsatz der vorgenannten Technologien zu. Drittanbieter dürfen mit Ihrer Zustimmung folgendes erheben und verarbeiten: Personalisierte Anzeigen, Anzeigenmessung, Erkenntnisse über Zielgruppen und Produktentwicklung, Informationen auf einem Gerät speichern und/oder abrufen.

[Impressum](#) | [Datenschutzerklärung](#) | [Drittanbieter](#)

We use cookies

When you visit our website, if you give your comment, we will use cookies to allow us to collect data for aggregated statistics to improve our services and remember your choice for future visits. If you don't want this, we will only use cookies to remember your choice for future visits (i.e., essential cookies).

If you don't select any of the first options, no cookies will be deployed, but the banner will re-appear every time you enter our website.

[More information on cookies and data protection](#)

Sommerakademie 2022: DS-Fehler bei Webseiten und sozialen Medien 10

Cookie-Banner

- no cookies -> no banner?
- no non-essential cookies -> no banner?

„Diese Webseite verwendet ausschließlich für die Funktionen der Website zwingend erforderliche Cookies. [Datenschutzerklärung](#) [OK]“

Diese Webseite verwendet ausschließlich für die Funktionen der Website zwingend erforderliche Cookies.
Datenschutzerklärung

OK

Cookie-Banner

- Cookie-Banner: Wie soll es gestaltet sein?
 - Dark Pattern / Nudging / Dysfunktionalität

Arbeit des EDSA an Guidelines zu Dark Patterns:

- Overloading
- Skipping
- Stirring
- Hinderling
- Fickle
- Left in the dark

Example 26: The interface uses a toggle switch to allow users to give or withdraw consent. However, the way the toggle is designed does not make it clear in which position it is and if users have given consent or not. Indeed, the position of the toggle does not match the colour. If the toggle is on the right side, which is usually associated with the activation of the feature ("switch on"), the colour of the switch is red, which usually signifies that a feature is turned off. Conversely, when the switch is on the left side, usually meaning the feature is turned off, the toggle background colour is green, which is normally associated with an active option.

Use 1 of personal data 

Use 2 of personal data 

Paywall

- Marktkonform? DSGVO-konform? Einer meinungspluralen Gesellschaft zuträglich?

Wie wollen Sie: nutzen?	
<p>mit Werbung</p> <p>Besuchen Sie zeit.de wie gewohnt mit Werbung und Tracking. Details zum Tracking finden Sie in der Datenschutzerklärung und im Privacy Center.</p> <p>EINVERSTANDEN</p> <p><small>Zustimmung jederzeit über den Link Privacy Einstellungen am Ende jeder Seite widerrufbar.</small></p>	<p>Pur</p> <p>Nutzen Sie zeit.de mit weniger Werbung und ohne Werbetacking für 120 €/Woche (für Digital-Abonnenten nur 0,40 €/Woche).</p> <p>JETZT ABONNIEREN</p> <p><small>Bereits PUR-Abonnent? Hier anmelden.</small></p>
<p><small>Für die Nutzung mit Werbung: Wir erheben personenbezogene Daten und übermitteln diese auch an Drittanbieter, die uns helfen, unser Webangebot zu verbessern und zu finanzieren. Eine Verarbeitung der auf Ihrem Gerät gespeicherten Informationen wie z.B. Cookies oder persönliche Identifikatoren, IP-Adressen sowie Ihres individuellen Nutzungsverhaltens erfolgt dabei zu den folgenden Zwecken:</small></p> <ul style="list-style-type: none"> ▶ Informationen auf einem Gerät speichern und/oder abrufen ▶ Personalisierte Anzeigen und Inhalte, Anzeigen- und Inhaltsmessungen, Erkenntnisse über Zielgruppen und Produktentwicklungen 	

PIMS

- § 26 TTDSG: Anerkannte Dienste zur Einwilligungsverwaltung, Endnutzereinstellungen
 - nutzerfreundliche und wettbewerbskonforme Verfahren und technische Anwendungen zur Einholung und Verwaltung der Einwilligung
(= kategorische Einwilligung?)

vs.

- DSGVO-Einwilligung: „für den konkreten Fall“ (ErwGr. 32)
(Wann) kommt die VO?

Was ist erforderlich?

Never ending story:

„Mein Service, meine Regeln!“

vs.

die „**core contract theory**“ des EDSA

54. Da Datenschutz ein Grundrecht ist, das in Artikel 8 der Charta der Grundrechte der Europäischen Union verankert ist, und unter Berücksichtigung der Tatsache, dass eines der Hauptziele der DSGVO darin besteht, betroffenen Personen Kontrolle über die sie betreffenden Informationen zu verschaffen, können **personenbezogene Daten nicht als Handelsware betrachtet** werden. Selbst wenn die betroffene Person der Verarbeitung personenbezogener Daten zustimmen kann,²⁹ kann sie ihre Grundrechte nicht im Rahmen dieser Vereinbarung eintauschen.³⁰

Reichweitenmessung

Bin ich sexy?

Muss ich das wissen?

§ 25 TTDSG: erforderlich? Keine wirtschaftliche Betrachtung! Ergebnis (-)

Darf ich das wissen?

Reichweitenmessung, die nicht § 25 TTDSG unterfällt
Zulässigkeit nach DSGVO? Art. 6 Abs. 4 DSGVO?

Fragen?

Fragen!