

DSB FAQ zum Thema Cookies und Datenschutz, Stand 25.5.2022

1. Was versteht man grundsätzlich unter Cookies?

Vereinfacht gesagt versteht man unter Cookies kleine Textdateien, die am Endgerät – also etwa am Computer oder Smartphone – bzw. im Browser abgespeichert werden, wenn eine Website im Internetbrowser aufgerufen wird. Diese Textdateien können u.a. vom Webserver einer solchen Website ausgelesen werden.

Es gibt verschiedene Arten von Cookies. Eine Eingruppierung kann anhand ihrer Lebensdauer vorgenommen werden (etwa Sitzungscookies und persistente Cookies) oder anhand der Domain, zu der sie gehören (etwa Erstanbieter- und Drittanbieter-Cookies). Wenn der Webserver, der die Internetseite speist, Cookies auf dem Computer oder dem mobilen Endgerät des Nutzers speichert, spricht man von „HTTP-Header-Cookies“. Ferner können Cookies mittels JavaScript-Code gespeichert werden, der sich auf der Seite befindet oder dort referenziert wird (siehe die Schlussanträge des Generalanwalts in der Rechtssache C-673/17 Rz 40 mwN).

Beispiel: Eine Website wird in fünf verschiedenen Sprachversionen angeboten. Beim erstmaligen Aufruf der Website wählen Sie die Sprachversion „Deutsch“ aus. Auf Ihrem Endgerät wird nun eine Textdatei (ein „persistentes Cookie“) samt der Information hinterlegt, dass Sie die Website in der deutschen Sprache verwenden wollen. Wenn Sie die Cookies nicht löschen und mit demselben Browser die Website erneut aufrufen, so weiß die Website aufgrund des hinterlegten Cookies, dass die Website in deutscher Sprache angezeigt werden soll.

Die folgenden Informationen dienen dazu, die häufigsten Fragen zum Thema Cookies und Datenschutz zu beantworten.

2. Was ist der rechtliche Rahmen für den Einsatz von Cookies?

Die Zulässigkeit für das Setzen oder Auslesen von Cookies ist grundsätzlich in Art. 5 Abs. 3 der [Richtlinie 2002/58/EG](#) idgF. geregelt, welcher auf nationaler Ebene in § 165 Abs. 3 TKG 2021 umgesetzt wurde.

Zusammengefasst kann gesagt werden, dass Cookies beim Aufruf einer Website nur dann ohne Einwilligung gesetzt oder ausgelesen werden dürfen, wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Nutzer oder Benutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann („technisch notwendige Cookies“).

Für alle „technisch nicht notwendigen Cookies“ (siehe Frage 5) muss eine **Einwilligung** eingeholt werden. Beim Bau einer Website ist dringend darauf zu achten, dass keine „technisch nicht notwendigen Cookies“ vor dem Einholen einer Einwilligung gesetzt werden.

Die Bedingungen für eine solche Einwilligung richten sich nach Art. 4 Z 11 und Art. 7 DSGVO (siehe den [Bescheid der DSB vom 30. November 2018, GZ: DSB-D122.931/0003-DSB/2018](#)).

Zur Vollständigkeit ist festzuhalten, dass § 165 Abs. 3 TKG 2021 nicht nur für das Setzen oder Auslesen von Cookies auf Websites gilt, sondern allgemein für die technische Speicherung oder dem Zugang von Daten auf Endgeräten. Die gegenständlichen FAQ widmen sich aufgrund der Praxisrelevanz jedoch ausschließlich dem Thema Cookies und Datenschutz.

3. Kann ich mich über den unzulässigen Einsatz von Cookies bei der Datenschutzbehörde beschweren?

Auf nationaler Ebene obliegt der Vollzug eines Verstoßes gegen § 165 Abs. 3 TKG 2021 den Fernmeldebehörden.

Eine Zuständigkeit der Datenschutzbehörde kann aber dennoch gegeben sein, wenn als Folge des Einsatzes von Cookies personenbezogene Daten gemäß Art. 4 Z 1 DSGVO verarbeitet werden (siehe Frage 4).

Beispiel: Eine Website setzt Tracking-Cookies zum Zweck der personalisierten Werbung ohne Einwilligung und Information der Website-Besucher ein. Da Tracking-Cookies keine „technisch notwendigen Cookies“ sind, liegt für den Einsatz der Tracking-Cookies ein Verstoß gegen § 165 Abs. 3 TKG 2021 vor. Sofern als Folge des unzulässigen Einsatzes der Tracking-Cookies auch personenbezogene Daten in Form von Online-Kennungen verarbeitet und insbesondere ein Profil zum Auspielen von personalisierter Werbung erstellt wird, kann für diese Folgeverarbeitung eine Beschwerde bei der Datenschutzbehörde eingebracht werden.

Es wird empfohlen, im Rahmen einer derartigen Beschwerde folgende Informationen an die Datenschutzbehörde zu übermitteln:

- Um welche Website handelt es sich (Angabe der Website-Adresse)?
- Wann konkret (Datum, Uhrzeit) haben Sie die beschwerdegegenständliche Website besucht?
- Haben Sie eine Einwilligung abgegeben (zB. auf den Button „Cookies akzeptieren“ geklickt)?
- Haben Sie die beschwerdegegenständliche Website zwischenzeitig öfter besucht?

Sofern Sie technische Expertise besitzen, können Sie zusätzlich zur Beschwerde auch eine Liste oder einen Screenshot mit jenen Cookies übermitteln, die am Endgerät gesetzt wurden. Zur Erstellung einer solchen Liste können Sie zum Beispiel den [WebsiteEvidenceCollector](#) des Europäischen Datenschutzbeauftragten verwenden. Die Übermittlung einer solchen Liste oder eines Screenshots ist zur Beschwerdeeingabe aber nicht erforderlich.

4. Sind Cookies personenbezogene Daten?

Cookies (oder besser gesagt: die in Cookies enthaltenen Informationen) sind nicht *per se* als personenbezogene oder nicht-personenbezogene Daten nach Art. 4 Z 1 DSGVO zu qualifizieren.

Es kommt immer auf die Umstände des Einzelfalls an, insbesondere, welche Informationen in den Cookies enthalten sind und auf welche Weise diese Informationen miteinander kombiniert werden können.

Beispiel: Eine Website wird in fünf verschiedenen Sprachversionen angeboten. Beim erstmaligen Aufruf der Website wählen Sie die Sprachversion „Deutsch“ aus. Auf Ihrem Endgerät wird nun eine Textdatei (ein „Cookie“) samt der Information hinterlegt, dass Sie die Website in der deutschen Sprache verwenden wollen. Sofern diese Information (also Ihre Auswahl zur Spracheinstellung Deutsch) nicht mit Ihnen in Verbindung gebracht werden kann, handelt es sich um ein nicht-personenbezogenes Datum. Sofern der Website-Betreiber Ihre Spracheinstellung mit Ihnen in

Verbindung bringen kann, zum Beispiel, weil Sie sich im Online-Shop der Website registrieren, handelt es sich um ein personenbezogenes Datum.

Es kann sein, dass Cookies auch sogenannte Universally Unique Identifier (UUID) beinhalten. Dabei handelt es sich vereinfacht gesagt um nutzerspezifische Identifikatoren, mit denen Endgeräte von Benutzern markiert werden. Die DSGVO spricht gemäß Erwägungsgrund 30 auch von Online-Kennungen.

Zwar handelt es sich bei einer solchen Online-Kennung grundsätzlich nur um eine Markierung eines Endgeräts. Es gibt jedoch viele Mittel und Wege, ein Endgerät mit einer konkreten Person in Verbindung zu bringen, zum Beispiel, wenn sich eine Person auf der jeweiligen Website registriert oder ein Kontaktformular ausfüllt.

In manchen Fällen kann eine derartige Online-Kennung samt dazugehörigen Nutzerinformationen auch mit einem Profil auf einer Social Media Plattform in Verbindung gebracht werden (siehe dazu den [Bescheid der DSB vom 22. Dezember 2021, GZ: D155.027, 2021-0.586.257](#), nicht rk).

5. Wann sind Cookies „technisch notwendig“?

Für den Einsatz von „technisch notwendigen Cookies“ muss keine Einwilligung der Website-Besucher eingeholt werden (siehe Frage 2).

Weder die Richtlinie 2002/58/EG noch das TKG 2021 enthalten eine Aufzählung, was unter „technisch notwendigen Cookies“ konkret zu verstehen ist. Allerdings enthält die [Opinion 04/2012 on Cookie Consent Exemption, WP 194, 00879/12/EN](#) der ehemaligen Art. 29 Gruppe Kriterien zur Beurteilung, ob Cookies iSd Art. 5 Abs. 3 der Richtlinie 2002/58/EG idgF aus technischer Sicht notwendig sind. Die Datenschutzbehörde empfiehlt, die Empfehlungen der ehemaligen Art. 29 WP im Zweifelsfall heranzuziehen.

Aus Sicht der Datenschutzbehörde sind folgende Dienste aus technischer Sicht notwendig (und können daher entsprechende Cookies ohne Einwilligung gesetzt werden):

- notwendige Sitzungsverwaltung (etwa Cookies zum Speichern des Warenkorbs im Rahmen eines Onlinekaufs oder Cookies zum Speichern des Login Status);
- Eingaben bei einem Online-Formular, wenn zum Abschicken des Formulars eine Eingabe über mehrere Unterseiten einer Website notwendig ist;
- die Information über den Einwilligungsstatus, sofern hierfür keine eindeutige Online-Kennung vergeben wird.

Aus technischer Sicht nicht notwendig (und daher einwilligungsbedürftig) sind insbesondere jene Dienste, die das Nutzerverhalten von Personen auf der jeweiligen Website oder über mehrere Websites oder Endgeräte aufzeichnen und auswerten. Hierzu zählen aus Sicht der Datenschutzbehörde insbesondere Plugins von Social Media Diensten oder Werbenetzwerken, deren Implementierung zur Folge hat, dass personenbezogene Daten der Website-Besucher an Dritte übermittelt werden.

Nach Judikatur der DSB und des BVwG ist Art. 5 Abs. 3 der Richtlinie 2002/58/EG idgF. auch nicht im Sinne einer „wirtschaftlichen Notwendigkeit“ zu interpretieren“. Dies bedeutet, dass Werbe-Cookies zum Auspielen von personalisierter Werbung nicht „technisch notwendig“ werden, bloß weil das Auspielen von personalisierter Werbung zur Finanzierung des Betriebs der Website notwendig ist (siehe das [Erkenntnis des BVwG vom 12. März 2019, GZ: W214 2223400-1](#)).

6. Was ist ein Cookie-Banner und brauche ich einen Cookie-Banner für meine Website?

Ein Cookie-Banner ist ein Fenster, welches beim Aufruf einer gewissen Website (mit leerem Browserprofil) auftaucht. Dieses Fenster wird üblicherweise dazu verwendet, die Einwilligung des Website-Besuchers für das Setzen und Auslesen von Cookies einzuholen.

Eine solche Einwilligung muss aber nur dann vom Website-Besucher eingeholt werden, wenn „technisch nicht notwendige“ Cookies (siehe Frage 5) verwendet werden.

Sofern keine „technisch nicht notwendigen“ Cookies auf der Website verwendet werden, ist auch keine Einwilligung und somit kein Cookie-Banner notwendig.

7. Wie muss ein Cookie-Banner gestaltet sein, sodass eine wirksame Einwilligung vorliegt?

Grundsätzlich steht es dem Website-Betreiber offen, den Cookie-Banner nach seinen Vorstellungen zu gestalten. Zu beachten gilt jedoch, dass sich die Bedingungen für die Einwilligung nach Art. 4 Z 11 und Art. 7 DSGVO richten (siehe Frage 2).

Eine Einwilligung für das Setzen und Auslesen von „technisch nicht notwendigen“ Cookies sowie für die darauffolgende Datenverarbeitung ist daher nur wirksam, wenn die entsprechenden Vorgaben der DSGVO vollständig eingehalten werden.

Nach Ansicht der Datenschutzbehörde ist bei der Gestaltung eines Cookie-Banners daher jedenfalls Folgendes zu beachten:

- Erst Einwilligung, dann Cookies: Die Einwilligung ist vorab einzuholen. Beim Bau einer Website ist dringend darauf zu achten, dass keine „technisch nicht notwendigen Cookies“ vor dem Einholen einer Einwilligung gesetzt werden.
- Bewusstsein der betroffenen Person: Der betroffenen Person muss klar sein, dass sie eine Einwilligung abgibt. Ein Weitersurfen ohne Interaktion mit dem Cookie-Banner oder ein „versteckter Einwilligungsbutton“, der irrtümlich ausgewählt wird, kann nicht als unmissverständliche Einwilligung gewertet werden. Ebenso wenig kann von einer Einwilligung ausgegangen werden, bloß, weil eine betroffene Person das Setzen oder Auslesen von Cookies in den Browsereinstellungen grundsätzlich zulässt;
- Privacy by default: Die betroffene Person muss sich proaktiv für die Einwilligung entscheiden. Voreinstellungen oder vorangekreuzte Boxen im Cookie-Banner sind unzulässig;
- freiwillig: Die Einwilligung muss freiwillig erfolgen. Der betroffenen Person dürfen keine Nachteile angedroht werden und sie darf keine Nachteile erleiden, wenn sie keine Einwilligung abgibt. Grundsätzlich ist es unzulässig, der betroffenen Person den Zugang zur Website im Falle der Nichtabgabe der Einwilligung zu verweigern (siehe aber Frage 9);
- Widerrufsmöglichkeit: Im Cookie-Banner muss klar und deutlich beschrieben werden, wo bzw. wie die Einwilligung widerrufen werden kann. Der Widerruf muss so einfach sein wie die Erteilung der Einwilligung;
- Erfüllung der Informationspflicht: Der betroffenen Person, muss klar sein, wofür die Einwilligung abgegeben wird. Dies setzt voraus, dass die Informationspflichten vollständig erfüllt werden (siehe Frage 11);
- Nichtabgabe einer Einwilligung ist so einfach wie die Abgabe der Einwilligung: Die Nichtabgabe einer Einwilligung (bzw. das Weitersurfen ohne Einwilligung) muss genauso einfach sein wie die Abgabe der Einwilligung. Mit anderen Worten: Für die Nichtabgabe einer Einwilligung dürfen nicht mehr Interaktionen mit dem Cookie-Banner notwendig sein, als für die Abgabe der Einwilligung. Von der

betroffenen Person kann nicht verlangt werden, dass sie auf einer Schaltfläche erst auf einer zweiten oder dritten Ebene die Entscheidung treffen kann, keine Einwilligung abzugeben.;

- keine unfairen Praktiken: Die betroffene Person darf weder unmittelbar noch subtil zur Abgabe einer Einwilligung gedrängt werden (kein „nudging“). Es ist unzulässig, den Button zur Nichtabgabe einer Einwilligung (bzw. zum Weitersurfen ohne Einwilligung) derart zu gestalten oder zu positionieren, dass dieser Button weniger prominent ist als der Button zur Abgabe einer Einwilligung.

8. Muss der Button zur Abgabe einer Einwilligung eine andere Farbe haben als der Button zur Nichtabgabe einer Einwilligung?

Es kann keine allgemeingültige Aussage darüber getroffen werden, welche Farben ein Button innerhalb eines Cookie-Banners haben muss. Maßstab für die Gültigkeit einer Einwilligung ist u.a., dass keine unfairen Praktiken verwendet werden (siehe Frage 7). Es kommt daher auf eine Einzelfallbeurteilung an.

Wenn die Farbauswahl dazu führt, dass der Button zur Nichtabgabe einer Einwilligung (bzw. zum Weitersurfen ohne Einwilligung) weniger gut sichtbar ist als der Button zur Abgabe einer Einwilligung, könnte dies zur Ungültigkeit der Einwilligungserklärung führen.

Beispiel: Ein Cookie-Banner hat einen weißen Hintergrund. Der Button zur Abgabe einer Einwilligung ist rot, der Button zur Nichtabgabe einer Einwilligung (bzw. zum Weitersurfen ohne Einwilligung) ist weiß. Da der erste Button (rot) auf dem weißen Hintergrund gut sichtbar ist, der zweite Button (ebenso weiß) jedoch kaum wahrgenommen werden kann, kann von keiner gültigen Einwilligungserklärung ausgegangen werden. Die betroffene Person hatte nämlich keine zwei gleichwertigen Optionen bei ihrer Entscheidung.

9. Was ist unter „pay or okay“ zu verstehen und ist das zulässig?

Grundsätzlich ist zwischen „Paywall“ und „Cookiewall“ zu unterscheiden.

Bei einer „Paywall“ wird ein Nutzer beim Besuch der Website aufgefordert, für den Zutritt zur Website Geld zu bezahlen. Dies hat grundsätzlich nichts mit Cookies zutun und ist zulässig, da ein jeder Website-Betreiber darüber entscheiden kann, ob der Zugang zum Inhalt seiner Website entgeltlich ist.

Davon zu unterscheiden ist wiederum die „Cookiewall“. Bei einer „Cookiewall“ kann man für den Zutritt zur Website entweder Geld bezahlen, alternativ kann die Einwilligung für den Einsatz von Cookies (üblicherweise Werbe-Cookies zum Auspielen von personalisierter Werbung) abgegeben werden. Umgangssprachlich bezeichnet man dies auch als „pay or okay“.

Die Datenschutzbehörde hat bereits ausgesprochen, dass „pay or okay“ dem Grunde nach zulässig ist und ein Bezahlen für den Zugang zu einer Website eine Alternative zur Einwilligung darstellen kann (siehe den [Bescheid der DSB vom 20. August 2019, GZ: DSB-D122.974/0001-DSB/2019](#)).

Für diese Entscheidung der Datenschutzbehörde spricht, dass offenbar auch der europäische Gesetzgeber davon ausgeht, dass personenbezogene Daten – zumindest im gewissen Ausmaß – für den Erhalt einer Leistung bereitgestellt werden können (siehe die [Richtlinie \(EU\) 2019/770](#) idgF.). **Es ist jedoch ausdrücklich festzuhalten, dass dies die aktuelle Ansicht der Datenschutzbehörde darstellt und zu dieser Frage keine Judikatur des Europäischen Gerichtshofs vorhanden ist.**

Nach Ansicht der Datenschutzbehörde müssen beim Einsatz von „pay or okay“ jedoch zumindest folgende Punkte beachtet werden:

- die vollständige Einhaltung aller datenschutzrechtlichen Bestimmungen (insbesondere der DSGVO) für jene Datenverarbeitung, die aufgrund der Einwilligung („okay“) erfolgt;

- es handelt sich um keine Behörden oder sonstige öffentliche Stellen;
- keine Exklusivität in Bezug auf die angebotenen Inhalte oder Dienstleistungen, d.h. Unternehmen mit einem ausdrücklich öffentlichen (Versorgungs-) Auftrag oder Universaldienstleister können „pay or okay“ nicht zulässigerweise verwenden;
- keine Monopol- oder Quasi-Monopolstellung des Unternehmens am Markt;
- ein angemessener und fairer Preis für die Bezahlalternative („pay“), d.h. die Bezahlalternative darf nicht *pro forma* zu einem völlig unrealistisch hohen Preis angeboten werden;
- wenn sich ein Nutzer mithilfe der Bezahlalternative Zugang zur Website verschafft, so dürfen diesfalls keine personenbezogenen Daten zum Zwecke der personalisierten Werbung verarbeitet werden.

10. Muss ich Website-Besucher immer darüber informieren, wenn ich Cookies verwende?

Das kommt darauf an, welche Cookies verwendet werden.

Zur Beantwortung dieser Frage unterscheidet man am besten zwischen der Informationspflicht für das Setzen und Auslesen von Cookies und der Informationspflicht für die darauffolgende Datenverarbeitung.

Die Informationspflicht für das Setzen und Auslesen von „technisch nicht notwendigen“ Cookies (siehe Frage 5) ergibt sich Art. 5 Abs. 3 der Richtlinie 2002/58/EG idgF. Es gilt zu beachten, dass diese Informationspflicht jedenfalls für „technisch nicht notwendigen“ Cookies nach Judikatur des Europäischen Gerichtshofs stets gilt und es nicht darauf ankommt, ob es sich bei den Cookies um personenbezogene oder nicht-personenbezogene Daten handelt (siehe das Urteil des EuGH vom 1. Oktober 2019, C-673/17 Rz 69 ff).

Sofern als Folge des Setzens oder Auslesens von Cookies jedoch personenbezogene Daten verarbeitet werden (siehe Frage 4), besteht zusätzlich auch die Informationspflicht gemäß Art. 13 f DSGVO.

11. Wie erfülle ich die Informationspflicht für die Verwendung von Cookies auf meiner Website?

Die folgenden Ausführungen stehen unter der Prämisse, dass Sie Website-Besucher gemäß Art. 13 f DSGVO über die Datenverarbeitung informieren müssen (siehe Frage 6).

Oft muss eine große Menge an Informationen zur Verfügung gestellt werden. Im digitalen Bereich, also zum Beispiel auf einer Website, kann daher der sogenannte „Mehrebenen-Ansatz“ verfolgt werden (siehe dazu die [Leitlinien für Transparenz gemäß der Verordnung 2016/679](#) der ehemaligen Art. 29 WP, 17/DE, WP 260 rev.01 S. 23 ff).

Vereinfacht gesagt können auf der ersten Ebene, also im Cookie-Banner (siehe Frage 6), die grundlegenden Informationen zur Verfügung gestellt werden. Im Cookie-Banner ist ein Link zur Datenschutzerklärung einzufügen. In dieser Datenschutzerklärung werden auf zweiter Ebene dann die Informationen vollständig zur Verfügung gestellt.

Auf der ersten Ebene sollten nach Ansicht der Datenschutzbehörde jedenfalls folgende grundlegende Informationen zur Verfügung gestellt werden:

- die Identität des Verantwortlichen;
- eine genaue Beschreibung der Verarbeitungszwecke;
- die Rechtsgrundlage der Datenverarbeitung (d.h. die Einwilligung);

- der Hinweis darauf, dass die Einwilligung jederzeit und ohne Angabe eines Grunds widerrufen werden kann, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

- wie bzw. wo die Einwilligung widerrufen werden kann.

12. Kann ich Standards der Werbebranche oder „Cookie Consent Tools“ für die Gestaltung eines Cookie-Banners verwenden?

Grundsätzlich ja, sofern hierbei die datenschutzrechtlichen Bestimmungen (insbesondere der DSGVO) vollständig eingehalten werden.

Die Datenschutzbehörde rät jedoch dringend davon ab, derartige Standards oder Tools unhinterfragt zu verwenden. Nur weil diese im Internet angeboten werden, bedeutet dies nicht automatisch, dass eine Konformität mit den datenschutzrechtlichen Bestimmungen gegeben ist.

Bitte lesen Sie sich daher diese FAQ vollständig durch und konsultieren Sie im Zweifel einen Rechtsberater Ihres Vertrauens.

13. Bin ich der datenschutzrechtliche Verantwortliche, wenn auf meiner Website Cookies gesetzt oder ausgelesen werden?

Wenn Sie als Website-Betreiber die Entscheidung treffen, dass Cookies oder sonstige Dienste auf Ihrer Website zum Einsatz kommen, so sind Sie aus datenschutzrechtlicher Sicht für diese Datenverarbeitung (zumindest im gewissen Ausmaß) gemäß Art. 4 Z 7 DSGVO als Verantwortlicher oder gemeinsam Verantwortlicher nach Art. 26 DSGVO zu qualifizieren. Voraussetzung ist nur, dass personenbezogene Daten verarbeitet werden.

Hierbei spielt es keine Rolle, ob die Cookies auf Ihrer Website vom Webserver an den Browser des Website-Besuchers gesendet werden oder ob sie bloß Java-Script Code auf Ihrer Website einbauen, die im Browser des Website-Besuchers Cookies erzeugen.

Ebenso spielt es keine Rolle, ob Sie Zugang zu den personenbezogenen Daten haben, also zum Beispiel zu dem seitens des Werbenetzwerks erstellten Interessenprofils des Website-Besuchers (siehe das [Urteil des EuGH vom 10. Juli 2018, C-25/17 Rz 69](#)).

Wenn Sie aus Eigeninteresse Cookies oder sonstige Dienste auf Ihrer Website einbauen (zum Beispiel um durch Auspielen personalisierter Werbung Geld zu verdienen) und hierbei personenbezogene Daten verarbeitet werden, sind Sie nach Ansicht der Datenschutzbehörde (zumindest im gewissen Ausmaß) datenschutzrechtlicher Verantwortlicher.