Analyse: Cookies - Datenschutzerklärung

1. Rechtsgrundlage[1]

Rechtlich müssen beim Einsatz von Cookies und ähnlichen Technologien zwei Schritte unterschieden werden:

1. Die Speicherung von und Zugriff auf Endeinrichtungen: Die RL 2002/58/EG idF 2009/136/EG vom 25. 11. 2009 (sog "Cookie-Richtlinie" – umgesetzt im TKG in Österreich) verlangt die Einwilligung des Website-Nutzers für das Setzen von Cookies durch den Website-Betreiber. Nach hM gilt dies auch für alle anderen Online-Trackingmethoden (Web Storage, Flash Cookies, Browser Fingerprinting etc).
2. die nachfolgende Verarbeitung personenbezogener Daten gemäß DSGVO:
    a. Cookies werden nur ein einziges Mal in der gesamten DSGVO erwähnt werden, nämlich in Erwägungsgrund 30: "Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren." Aus dem Gesetzestext wird jedoch eindeutig klar, dass das Gesetz die Informationen, die sich aus Cookies ergeben, unter personenbezogene Daten subsumiert.
    b. Eine Ermittlung und Verarbeitung dieser Daten ist nur zulässig, wenn der Teilnehmer oder Nutzer seine aktive Einwilligung[2] für den konkreten Fall erteilt und diese Einwilligung nicht auf einem Opt-Out Ansatz beruht.

2. rechtskonformer Cookie Banner - Information und Zustimmung zu Verwendung von Cookies:

- ✓ Generell sollte der Einsatz von Cookies nach Möglichkeit minimiert werden. Zu diesem Zweck sollte die Website periodisch überprüft werden.
- ✓ Angaben im Cookie Banner
    - Angaben zur Einwilligung und zum Widerruf derselben;
        - Der Benutzer muss seine Zustimmung zB durch einen Bestätigungsklick in einer Infobox aktiv erteilen, bevor noch Cookies gesetzt werden – mittlerweile darf das Feld zum Akzeptieren der Cookies nicht mehr farblich hervorgehoben werden, sondern alle Auswahlfelder müssen dieselbe Optik haben
        - Vor Erteilen der aktiven Einwilligung über das Cookie-Banner dürfen ausschließlich Cookies verwendet werden, für die gem § 165 Abs 3 TKG 2021 keine Einwilligung erforderlich ist – siehe dazu unten in der Tabelle „unbedingt erforderliche Cookies“. Warenkorb-Cookies, Cookies zum Speichern der Einwilligung etc dürfen erst gesetzt werden, nachdem der Benutzer diese Dienste tatsächlich angefordert hat (dh ein Produkt in den Warenkorb legt oder eine Entscheidung im Cookie-Banner trifft).
        - Angaben zur Freiwilligkeit gemäß Art. 7 Abs. 4 DSGVO der Einwilligung: Dem Nutzer müssen bspw. trotz Ablehnen der Cookie-Nutzung alle Inhalte offenstehen.
    - Weiters ist der Benutzer darauf hinzuweisen, dass er die Verwendung von Cookies durch entsprechende Einstellung seines Browsers ablehnen kann. Die Ermöglichung von Cookie-Einstellungen muss mittels einer einfach zu bedienenden Konfigurationsplattform möglich sein.
    - Wird auf der ersten Ebene eines Consent-Banners eine Einwilligung eingeholt, gilt der Grundsatz, dass Nutzer auf dieser Ebene bereits erkennen müssen, wofür sie die Einwilligung erteilen sollen. Dies bedeutet, dass ersichtlich sein muss,
        - wer auf die jeweilige Endeinrichtung zugreift,

---

[1] *Hans-Jürgen Pollirer*, Checkliste datenschutzgerechte Cookie-Banner, Dako 2022/18 (38); Rainer Kessler/Jutta Sonja Oberlin, DSGVO-konforme Verwendung von Cookies und anderen Trackingmethoden, CB 2020, 63 (64); Carlo Piltz/Philip Schweers, Neue Orientierungshilfe der Datenschutzkonferenz zum Einsatz von Cookies und ähnlichen Technologien, DSB 2022, 22 (22)

[2] EuGH Urteil C-673/17 vom 1. 10. 2019

- in welcher Form,
- zu welchem Zweck und
- welche Funktionsdauer bspw. gesetzte Cookies haben.

- Ansonsten mittels Verlinkung zur Datenschutzerklärung – siehe dazu nächster Punkt
- Einsatz einer Consent Management Platform: Bei einer Consent Management Platform handelt es sich um ein System, das die datenschutzrechtlichen Einwilligungen über das Cookie-Banner speichert. Typischerweise werden dabei Kennnummern (IDs) eingesetzt, die mittels Cookies gespeichert werden, um die Erteilung der Einwilligung nachzuweisen. Bei der Auswahl der Software ist auf DSGVO-Konformität zu achten, insb stellen sich dabei Fragen zur Übermittlung in Drittländer (über eingesetzte Auftragsverarbeiter) und zur Rechtsgrundlage der weiteren Verarbeitung dieser Daten.

3. Datenschutzerklärung: Information über die gesetzten Cookies sowie deren Zwecke

- ✓ Der knappe Text des Cookie-Banners muss in wenigen Sekunden gelesen werden können. Er erlaubt nur die Wiedergabe der allernotwendigsten Informationen. Alle ergänzenden Informationen zu Cookie-Anbietern, Speicherdauer, Verwendungszweck etc müssen in der Datenschutzerklärung zu finden sein. Sie muss direkt über das Cookie-Banner aufgerufen werden können.
  - Detailinformationen über eingesetzte Cookies: Kategorien eingesetzter Cookies (siehe dazu die Tabelle unten)
  - welche personenbezogenen Daten ermittelt, verarbeiten und übermittelt werden,
  - auf welcher Rechtsgrundlage und
  - für welche Zwecke dies erfolgt (konkrete Beschreibung der Zwecke der Folgeverarbeitung - es soll ausdrücklich nicht ausreichen, wenn als Zwecke z.B. nur Verbesserung der Erfahrung des Nutzers, Werbezwecke, IT-Sicherheitszwecke angegeben werden.)
  - für wie lange die Daten gespeichert werden.
- ✓ Die Informationen müssen aktuell und richtig sein. Sie müssen alle eingesetzten Maßnahmen und Anbieter behandeln, dürfen aber nicht "auf Vorrat" über diese hinausgehen. Dies setzt ihre regelmäßige Aktualisierung und die laufende Abstimmung mit Trackingmaßnahmen voraus.

4. Bestandsaufnahme, Kategorisierung der eingesetzten Cookies und Rechtsgrundlagen

Rechtsgrundlagen		Cookies Kategorie
TKG – Rechtsgrundlage für das Setzen der Cookies	*DSGVO - Rechtsgrundlage für die Verarbeitung der Daten, die über Cookies erfasst werden*	
Keine Einwilligung erforderlich		
Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz: Mit dieser etwas kryptischen Formulierung ist nach hM die Antwort des Webservers an den Benutzer gemeint. Wird ein Cookie allein für diesen Zweck eingesetzt, ist keine Einwilligung erforderlich. Unter diese Bestimmung fallen die "technischen" Cookies, die für Lastenausgleich, Session Management oder andere Anforderungen von Hard- und Software zwingend benötigt werden. Bereitstellung eines vom Benutzer ausdrücklich gewünschten Dienstes der Informationsgesellschaft: Auch diese Cookies bedürfen keiner Einwilligung, sofern sie für die Bereitstellung unbedingt erforderlich sind und der Dienst "ausdrücklich gewünscht" wurde. Dies hat ua	Erfüllung eines Vertrages und vorvertragliche Maßnahmen: Die Rechtsgrundlage des Art 6 Abs 1 lit b DSGVO kann zur Anwendung kommen, wenn über Cookies erfasste Daten für die Vertragserfüllung erforderlich sind. Das kann zB iZm Warenkorb- oder Authentifizierungs-Cookies der Fall sein.	**Unbedingt erforderliche Cookies:** Das sind solche, die zwingend erforderlich sind, damit die Website und ihre Funktionen ordnungsgemäß funktionieren. Einerseits sind dies rein "technische" Cookies, die zB zur Lastverteilung auf mehrere Server oder für den Betrieb der Webserver-Software zwingend benötigt werden. Andererseits umfasst diese Kategorie auch Cookies, die für einen vom Benutzer angeforderten Dienst unbedingt erforderlich sind, zB Authentifizierungs-Cookies für den Login-Bereich oder Warenkorb-Cookies für einen Webshop.

Konsequenzen für den Zeitpunkt ihres Einsatzes: Im Regelfall dürfen sie nicht schon beim Aufruf der Website gesetzt werden, sondern erst, sobald ein Benutzer den Dienst anfordert, zB einen Artikel in den Warenkorb legt, sich zu einem passwortgeschützten Bereich anmeldet oder eine Entscheidung im Cookie-Banner trifft.	Der Anwendungsbereich ist eng auszulegen. Gegebenenfalls ist nachzuweisen, dass ohne diese Cookie-Daten keine Vertragserfüllung möglich ist.	Auch Cookies, die zur Speicherung der Einwilligung oder Ablehnung dienen, werden dieser Kategorie zugerechnet.
Einwilligung erforderlich		
Einwilligung: Diese wird für alle Cookies, die nicht zu den oben angeführten "unbedingt erforderlichen Cookies" zählen, benötigt. Für die Einwilligung gelten alle bereits aus der DSGVO bekannten Anforderungen, dh sie muss gem Art 4 Z 11 DSGVO freiwillig, bestimmt, informiert, unmissverständlich, eindeutig und aktiv sowie gem Art 7 Abs 3 DSGVO jederzeit widerrufbar sein.	**Einwilligung:** Die gem § 165 Abs 3 TKG 2021 eingeholte Einwilligung zu Cookies kann gleichzeitig gem Art 6 Abs 1 lit a DSGVO als Rechtsgrundlage für die weitere Verarbeitung herangezogen werden. Dies setzt insb voraus, dass die Besucher über das Cookie-Banner und/oder die Datenschutzerklärung der Website vollständig über Zwecke und Umstände der Verarbeitung informiert werden. In der OH Telemedien 2021 geht die DSK davon aus, dass die Einwilligung nach § 25 Abs. 1 TTDSG zusammen mit der Einwilligung nach Art. 6 Abs. 1 a) DSGVO erklärt werden kann, solange der Telemedienanbieter/Verantwortlicher ausreichend klarstellt, dass die Einwilligung den gesamten Lebenssachverhalt umfasst. Das bedeutet z.B., dass nach Ansicht der DSK im Banner die Folgeverarbeitung (z.B. die Auswertung der erhobenen Daten zur Erstellung von Werbeprofilen) mit angesprochen werden muss. **Sonderfall internationaler Datenverkehr:** Für die rechtmäßige Übermittlung von personenbezogenen Daten in unsichere Drittländer sind zusätzliche Schritte bei der Wahl der Rechtsgrundlage, den Sicherheitsmaßnahmen und der Gestaltung der Informationen erforderlich. Für solche zusätzlichen Sicherheitsgarantien ist der Verantwortliche in der EU, in Kooperation mit dem Datenimporteur in den USA, verantwortlich – siehe dazu im Anschluss an die Tabelle. In Ausnahmefällen kann der Datentransfer auf eine ausdrückliche Einwilligung gem Art 49 Abs 1 lit a DSGVO gestützt werden. Diese Möglichkeit besteht jedoch nur für den Einzel- und nicht den Regelfall, wie der EDSA in seinen Leitlinien 2/2018 kritisch festhält. Die Einwilligung ist daher keine	Funktions-Cookies: Diese Cookies sind nicht unbedingt notwendig, erhöhen aber die Benutzerfreundlichkeit der Website, zB durch Speicherung der Spracheinstellung, Schriftgröße oder Einstellungen zur Barrierefreiheit. Webanalyse- oder Webstatistik-Cookies: Mit diesem Cookie-Typ werden Informationen über das Verhalten der Nutzer auf der Website erhoben. Er identifiziert populäre Bereiche der Website oder misst Ladezeiten der verschiedenen Browser. Oft läuft darüber auch das "Conversion Tracking", mit dem der Einfluss auf den Verkaufserfolg gemessen wird. Beispiele für diesen Cookie-Typ sind Google Analytics und Matomo. Marketing-Cookies (auch als Werbe- oder Targeting-Cookies bezeichnet): Dieser Cookie-Typ wird vom Websitebetreiber und von Dritten genutzt, um das Verhalten der Nutzer zu analysieren und sie in Kategorien einzuordnen, um ihnen anschließend personalisierte Werbung zukommen zu lassen. Beispiele für diesen Cookie-Typ sind Google Ads, Doubleclick und Facebook Pixel.

	praktikable Rechtsgrundlage für den Datentransfer in Drittländer und insb den Einsatz von US-Trackinganbietern.	
	Berechtigtes Interesse: Auch Art 6 Abs 1 lit f DSGVO kann zur Anwendung gelangen, stellt allerdings eher die Ausnahme dar. In den meisten Fällen liegen derartigen Verarbeitungen Cookies zugrunde, die einwilligungsbedürftig sind, sodass Art 6 Abs 1 lit a DSGVO die geeignete Rechtsgrundlage darstellt. Für die Inanspruchnahme müssen jedenfalls **drei Voraussetzungen** vorliegen: a) Bestehen eines berechtigten Interesses; b) Erforderlichkeit, dh es darf kein geeignetes milderes Mittel vorliegen; c) eine Interessenabwägung im Einzelfall zwischen Websitebetreiber und Benutzer. Summa summarum verbleibt bei Anwendung dieser Rechtsgrundlage ein hohes Restrisiko, dass sie als ungeeignet gewertet wird.	

Die DSGVO nennt folgende Fälle einer zulässigen Datenübermittlung an ein Drittland bzw. eine internationale Organisation:

Angemessenheitsbeschluss der Kommission

Datenübermittlungen auf der Grundlage eines Angemessenheitsbeschlusses bedürfen keiner besonderen Genehmigung durch die Aufsichtsbehörde.

Angemessenheitsbeschlüsse (Durchführungsrechtsakte der Kommission) müssen einen Mechanismus für eine regelmäßige Überprüfung, die mindestens alle 4 Jahre zu erfolgen hat, vorsehen. Die Kommission überwacht fortlaufend die Entwicklung in den entsprechenden Drittländern und widerruft, ändert oder setzt die Beschlüsse im Wege von Durchführungsrechtsakten aus, soweit Informationen vorliegen, dass das Drittland kein angemessenes Schutzniveau gewährleistet.

Angemessenheitsbeschlüsse bestehen derzeit für die Staaten Andorra, Argentinien, Färöer Inseln, Guernsey, Insel Man, Israel, Japan, Jersey, Kanada, Neuseeland, Schweiz, Südkorea, Uruguay und das Vereinigte Königreich (UK).

Vorliegen geeigneter Garantien

Ohne Genehmigung der Aufsichtsbehörde können diese geeigneten Garantien bestehen, in:

- verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules), die von der zuständigen Aufsichtsbehörde genehmigt worden sind.

- Standarddatenschutzklauseln, die von der Kommission erlassen oder von einer Aufsichtsbehörde angenommen und von der Kommission genehmigt worden sind.

  Achtung: Die Übergangsfrist der alten Standarddatenschutzklauseln, die von der Kommission erlassen wurden, laufen aus. Diese können nur mehr bis zum 27. Dezember 2022 herangezogen werden. Dann müssen die neuen Standarddatenschutzklauseln verwendet werden.

- genehmigten Verhaltensregeln oder einem genehmigten Zertifizierungsmechanismus (beide zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen).

Hinweis:
Zu beachten sind auch die Informationspflichten für den Fall, dass Daten an ein Drittland (bzw. eine internationale Organisation) übermittelt werden sollen. Zudem müssen Übermittlungen in Drittländer (bzw. eine internationale Organisation) in das Verzeichnis von Verarbeitungstätigkeiten aufgenommen werden.

5. Falls Voraussetzungen vorliegen: Datenschutzfolgenabschätzung

Bei Vorliegen der Voraussetzungen muss eine Datenschutzfolgeabschätzung (DSFA) gemäß Art. 35 DSGVO durchgeführt werden, um im Folgeschritt Maßnahmen ergreifen zu können. Ob die Voraussetzungen vorliegen, kann anhand von Kontrollfragen geprüft werden:

1. Werden personenbezogene Daten verarbeitet?
2. Wurde die Datenverarbeitungsaktivität bereits als mit hohem Risiko bewertet?
3. Findet eine automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung statt?
4. Findet eine systematische Überwachung statt?
5. Werden vertrauliche oder höchstpersönliche Daten verarbeitet?
6. Findet eine Datenverarbeitung in großem Umfang statt?
7. Werden Datensätze abgeglichen und/oder zusammengeführt?
8. Werden Daten von schutzbedürftigen Datensubjekten verarbeitet?
9. Ist eine innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen angedacht?
10. Werden betroffene Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrages gehindert?