III. Datenschutz im Internet: Cookies, Social Media etc

44. Gilt das Datenschutzrecht auch im Internet?

Ja, selbstverständlich. Die DSGVO wurde gerade zu dem Zweck erlassen, in den letzten Jahren entstandene, überwiegend web-basierte Phänomene wie Profiling, GPS-Tracking oder Echtzeit-Videoüberwachung wirksam zu regulieren. Daher sind sämtliche Datenverarbeitungsvorgänge, die über das Internet erfolgen, nach den Regeln der DSGVO zu beurteilen. Insbesondere müssen sie also auf einer Rechtsgrundlage gemäß Art 6 oder 9 DSGVO beruhen und es müssen die Informationspflichten der Art 13 und 14 DSGVO erfüllt werden.

Neben der DSGVO gelten in diesem Bereich auch die E-Privacy-Richtlinie 2002/58/EG und die Cookie-Richtlinie 2009/136/EG bzw deren nationale Umsetzungen, die vor allem im Telekommunikationsgesetz erfolgten. Diese Rechtsnormen sollen in Kürze jedoch von einer zurzeit noch im Entwurf vorliegenden E-Privacy-Verordnung abgelöst werden, die neben der DSGVO gelten und diese im Bereich der elektronischen Kommunikation ergänzen wird.

45. Sind IP-Adressen personenbezogene Daten?

Ja. Wie bereits ausgeführt (siehe Frage 5), sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Identifizierbar ist eine Person auch dann, wenn sie zwar nicht vom Datenverarbeiter selbst, sondern überhaupt mit nach allgemeinem Ermessen wahrscheinlichen Mitteln identifiziert werden kann. Da bei IP-Adressen üblicherweise die Möglichkeit besteht, herauszufinden, welche Person hinter ihnen steht, sind diese als personenbezogene Daten zu werten.

46. Ist die Protokollierung von Daten am Webserver zulässig?

Die Protokollierung einzelner bei jedem Aufruf einer Website anfallender Daten (zB IP-Adresse, Datum und Uhrzeit, verwendete Browser, Referrer) ist zwar aufgrund der Erfassung von IP-Adressen datenschutzrechtlich beachtlich, grundsätzlich aber zulässig.

Für diese Protokollierung bestehen nämlich üblicherweise berechtigte Interessen des Websitebetreibers, der diese Daten benötigt, um im Falle von Sicherheitsverletzungen Auswertungen vorzunehmen. Ebenso können anhand dieser Daten Nutzungsstatistiken erstellt werden.

Zu wahren sind dabei die Grundsätze der Speicherbegrenzung und der Datenminimierung. Das bedeutet einerseits, dass die protokollierten Daten nur so lange gespeichert werden dürfen, wie sie benötigt werden; da ein Angriff auf einen Webserver unter Umständen erst nach einiger Zeit entdeckt werden kann, wird eine Speicherdauer von einigen Monaten aber jedenfalls angemessen sein. Andererseits sollten die erhobenen IP-Adressen wenn möglich – also insbesondere bei der Führung von Statistiken – pseudonymisiert werden.

Zudem sind die betroffenen Personen in der Datenschutzinformation gemäß Art 13 und 14 DSGVO über die Verarbeitung ihrer Daten im Rahmen der Protokollierung zu informieren (siehe Frage 68).

47. Was ist zu beachten, wenn ich auf meiner Website Cookies setze?

Die Verwendung von Cookies ist nur dann datenschutzrechtlich relevant, wenn dabei personenbezogene Daten verarbeitet werden. Hier kommt es darauf an, ob es für den Verwender eines Cookies möglich ist, einen Bezug zu einer konkreten Person herzustellen. Das ist etwa dann der Fall, wenn Userkennungen, E-Mail-Adressen oder IP-Adressen verarbeitet werden.

Werden Cookies verwendet, muss der Anbieter des Web-Dienstes (also meist der Websitebetreiber) gemäß § 96 Abs 3 TKG den Nutzer schon vor dem erstmaligen Setzen des Cookies darüber informieren, welche personenbezogenen Daten ermittelt, verarbeitet und übermittelt werden, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Darüber hinaus muss der Nutzer vor Setzung des Cookies seine Einwilligung zu dessen Verwendung erteilen (dazu sogleich, Frage 49).

Eine Ausnahme von dieser Informations- und Einwilligungspflicht besteht aber dann, wenn die Verwendung des Cookies unbedingt erforderlich ist, damit der Anbieter des Web-Dienstes eine vom Nutzer ausdrücklich gewünschte Funktion zur Verfügung stellen kann. Dies trifft für gewöhnlich bei Session-IDs zu, die die Nutzung einer Website ermöglichen, ohne innerhalb einer Sitzung dieselben Daten mehrmals eingeben zu müssen (zB durch neuerliches Einloggen); ebenso sind Cookies notwendig, um einen elektronischen Warenkorb anbieten zu können.

Nicht unter diese Ausnahme fallen Cookies, die nicht technisch, sondern aus anderen Gründen „notwendig" sind, um einen Web-Dienst anzubieten. Daher unterliegt etwa ein Cookie zum Behavioral Advertising auch dann nicht dieser Ausnahme, wenn dessen Setzung die einzige Einnahmequelle einer Website ist. Ebenso können Analysecookies wie zB Besucherzählung nicht darunter eingeordnet werden, auch wenn sie aus der Sicht eines Websitebetreibers nützlich sein mögen. Derartige Cookies dürfen demnach nur nach Informationserteilung und Einwilligung gesetzt werden.

48. Wie muss der Nutzer über die Setzung von Cookies informiert werden?

Nutzern müssen bereits vor dem erstmaligen Setzen eines Cookies umfassende Informationen erteilt werden. Dafür eignen sich Pop-up-Fenster, Banner oder eindeutige und gut sichtbare Bildschirmsymbole auf einer Website, mit denen eine Seite verlinkt wird, die diese Informationen enthält. Dabei muss jedenfalls sichergestellt sein, dass die Informationen für den Nutzer klar ersichtlich sind, was zB dann nicht der Fall sein kann, wenn diese in AGB oder Datenschutzerklärungen „versteckt" werden. Die in der Praxis gängigste Variante ist dabei ein Banner, der bei Öffnen einer Website am Bildschirmrand erscheint und auf eine Information über Cookies hinweist, die per Link aufgerufen werden kann.

Die erteilten Informationen müssen so klar und verständlich wie möglich zur Verfügung gestellt werden. Sie haben daher vor allem folgende Inhalte zu umfassen:

- Kategorien der verarbeiteten personenbezogenen Daten (zB IP-Adresse, Benutzername),
- Rechtsgrundlage der Verarbeitung (zB berechtigte Interessen gemäß Art 6 Abs 1 lit f DSGVO),
- Verwendungszweck des Cookies (zB Nachverfolgung des Nutzerverhaltens),
- Speicherdauer der Daten,
- Identität des Webservers, der den Cookie setzt (insbesondere bei Third-Party-Cookies),
- mögliche Datenempfänger,
- Deaktivierungs- und Löschungsmöglichkeiten der Nutzer (zB durch Browser-Einstellungen).

49. Wie wird eine Einwilligung zur Setzung von Cookies wirksam eingeholt?

Eine wirksame Einwilligung zur Verwendung von Cookies erfordert jedenfalls, dass der Nutzer zuvor umfangreich informiert wurde und eine ausdrückliche Handlung oder andere aktive Verhaltensweise setzt, die als Zustimmung zu werten ist.

Eine solche ausdrückliche Handlung ist jedenfalls das Anklicken eines Links oder eines Buttons („Wenn Sie mit der Verwendung von Cookies einverstanden sind, klicken Sie hier").

Laut der Art-29-Datenschutzgruppe ist es jedoch ebenfalls als Zustimmung zu werten, wenn der Nutzer bei voller Kenntnis der Sachlage weiter auf die Website zugreift. Demzufolge reicht es, dass dem Nutzer vor dem Setzen eines Cookies die erforderlichen Informationen (auch zur Möglichkeit der Deaktivierung von Cookies durch Browser-Einstellungen) erteilt werden (siehe Frage 48) und ihm zudem klargemacht wird, dass er durch die weitere Benützung der Website – also zB durch das Anklicken eines Links, eines Bildes oder eines sonstigen Inhalts –

die Setzung von Cookies akzeptiert. Dabei muss dem Nutzer transparent mitgeteilt werden, mit welcher Handlung seine Zustimmung erfolgt. Allein durch das Klicken auf den Link zur Information oder gar durch völlige Untätigkeit (dh bloßes Verbleiben auf der Website) wird keine Einwilligung erteilt und dürfen Cookies nicht gesetzt werden.

50. Was ist zu beachten, wenn ich Google Analytics verwende?

Auch bei der Verwendung von Google Analytics wird die IP-Adresse und damit ein personenbezogenes Datum verwendet. Die IP-Adresse wird dabei zusammen mit anderen Daten an Google übermittelt, die auf der Grundlage dieser Daten Zugriffsstatistiken erstellen.

Bei der Verwendung und Konfigurierung von Google Analytics sind deshalb die Regelungen der DSGVO und dabei vor allem die Grundsätze der Datenminimierung und des Privacy by Default sowie die Informationspflichten zu beachten (siehe Fragen 12, 68 und 104). Das bedeutet, dass

- die von Google angebotene Anonymisierungsfunktion verwendet werden muss (siehe dazu die Google-Analytics-Hilfe unter https://support.google.com/analytics/answer/2905384?hl=de),
- den Nutzern eine Opt-out-Möglichkeit geboten werden muss (dies kann durch ein Browser-Plugin oder ein Opt-out-Cookie erfolgen, siehe dazu https://tools.google.com/dlpage/gaoptout?hl=de und https://developers.google.com/analytics/devguides/collection/gajs/?hl=de#disable) und
- die Nutzer in der auf der Website bereitgestellten Datenschutzinformation detailliert über die Verwendung von Google Analytics informiert werden müssen.

51. Was ist bei der Verwendung von Social-Media-Plugins zu bedenken?

Auch Social-Media-Plugins (zB die „Teilen"-Buttons von Facebook oder Twitter) verarbeiten personenbezogene Daten, indem sie IP-Adressen an die Betreiber der zugehörigen Social-Media-Dienste übermitteln.

Da für eine solche Datenübermittlung keine Rechtsgrundlage – insbesondere auch kein berechtigtes Interesse – vorliegt, ist eine Einwilligung des Nutzers vonnöten. Social-Media-Plugins müssen also in einer Weise eingebunden werden, die sicherstellt, dass eine Datenverarbeitung erst dann stattfindet, wenn der Nutzer dafür seine ausdrückliche Einwilligung durch Klicken auf den jeweiligen Button erteilt hat. Bis der Nutzer das getan hat, müssen die Plugins deaktiviert bleiben und dürfen keine Daten übermittelt werden.

Die Literatur schlägt dafür eine „Zwei-Klick-Lösung" vor: Im ersten Schritt müssen die erst noch deaktivierten („ausgegrauten") Social-Media-Plugins durch einen Klick des Nutzers aktiviert werden; ab diesem Zeitpunkt kann eine Datenüber-

tragung an die Betreiber der Social-Media-Dienste erfolgen. Im zweiten Schritt kann der Nutzer das Plugin dann tatsächlich verwenden und zB einen auf der Website bereitgestellten Bericht teilen.

Über die Verwendung von Social-Media-Plugins und die damit in Zusammenhang stehenden Datenverarbeitungen sind Nutzer in der auf der Website bereitgestellten Datenschutzinformation zu informieren.

52. Was ist bei der Verwendung von Social-Media-Plattformen zu beachten?

Werden Social-Media-Plattformen wie Facebook, Instagram, Twitter, WhatsApp genutzt, ist darauf zu achten, dass dabei – meist unbedacht – Datenschutz- und andere Rechtsverstöße gesetzt werden können.

So birgt insbesondere das in vielen sozialen Netzwerken mögliche „Teilen" von Beiträgen anderer Nutzer Gefahren: Verstößt nämlich schon der ursprüngliche Post des anderen Nutzers gegen Rechtsvorschriften – zB weil ein Foto datenschutzwidrig aufgenommen wurde oder weil ein Text oder Video in das Recht des Urhebers eingreift –, ist auch das Teilen dieses Posts in der Regel rechtswidrig.

Dasselbe gilt, wenn Daten Dritter an Betreiber sozialer Netzwerke übermittelt werden. Dies ist insbesondere dann der Fall, wenn ganze Adressbücher mit dem sozialen Netzwerk „verbunden" bzw „synchronisiert" werden. Eine solche Übermittlung von Daten Dritter ist mangels Rechtsgrundlage in der Regel rechtswidrig. Bei der Verwendung solcher Plattformen und der von ihnen angebotenen Apps ist demnach unbedingt darauf zu achten, dass derartige Synchronisierungsfunktionen abgestellt werden. Ist dies nicht möglich, sollte der Dienst nicht verwendet werden, um Datenschutzverstöße zu vermeiden. In diesem Sinne geht die überwiegende Literatur davon aus, dass der Dienst WhatsApp in der derzeitigen Form nicht im beruflichen Kontext verwendet werden darf, weil er auf die Kontaktdaten sämtlicher Personen zugreift, die sich im Adressbuch des Nutzers befinden.

Infolgedessen sollte auch gängigen „Standard-Funktionen" etablierter Social-Media-Plattformen nicht unhinterfragt Vertrauen geschenkt werden. Vielmehr ist auch hier im Einzelfall danach zu fragen, ob ein „Teilen", „Synchronisieren" usw ein Risiko für einen Datenschutz- oder anderen Rechtsverstoß birgt.

53. Welche Vorkehrungen muss ich treffen, wenn ich eine Facebook-Fanpage betreibe?

Der Europäische Gerichtshof (EuGH) hat in seinem aufsehenerregenden Urteil C-210/16 *Wirtschaftsakademie Schleswig-Holstein* erkannt, dass der Betreiber einer Facebook-Fanpage für die damit einhergehende Verarbeitung personenbezogener Daten der Fanpage-Nutzer durch Facebook mitverantwortlich ist (gemeinsamer

Verantwortlicher iSd Art 26 DSGVO, siehe Frage 3). Im konkreten Fall ging es dabei um die Setzung von Cookies durch Facebook, die das Verhalten des Besuchers beobachten und die daraus gewonnenen Ergebnisse an Facebook übermitteln; der Fanpage-Betreiber erhält diese Ergebnisse in Form verschiedener Statistiken über das Nutzerverhalten auf seiner Fanpage. Die Mitverantwortlichkeit für diese Verarbeitung hat der EuGH damit begründet, dass der Fanpage-Betreiber mit der Einrichtung dieser Fanpage Facebook erst die Möglichkeit gibt, personenbezogene Daten der Besucher zu verarbeiten; zudem trage er durch die Einstellung seiner Fanpage zur Entscheidung bei, welche statistischen Daten erhoben werden, und er profitiere auch von den Ergebnissen dieser Datenanalysen.

Da der Fanpage-Betreiber also für die stattfindenden Verarbeitungen Verantwortlicher im Sinne der DSGVO ist, hat er sämtliche Regeln der Verordnung zu erfüllen. Insbesondere ist er also dafür verantwortlich, dass diese Datenverarbeitungen auf einer Rechtsgrundlage beruhen und dass die Nutzer umfassend informiert werden.

Dabei ergibt sich jedoch die Problematik, dass dem Betreiber einer Facebook-Fanpage gar kein rechtlicher oder tatsächlicher Einfluss auf die von Facebook durchgeführten Verarbeitungen zukommt. Er hat nämlich weder die Möglichkeit, Einwilligungen einzuholen (eine derartige Funktion gibt es bei Facebook nicht), noch weiß er überhaupt genau darüber Bescheid, welche Datenverarbeitungen Facebook konkret vornimmt, und kann daher seinen Informationspflichten nicht nachkommen. Darüber hinaus kann der Ausübung von Betroffenenrechten nicht vollumfänglich entsprochen werden, da für eine Auskunft, Berichtigung oder Löschung die Handhabe fehlt.

Bis Facebook sein Angebot so adaptiert, dass den datenschutzrechtlichen Regeln entsprochen werden kann, besteht eine erhebliche Rechtsunsicherheit für Fanpage-Betreiber.

Um sicherzugehen, keine Datenschutzverstöße zu begehen, können Facebook-Fanpages zurzeit also nur deaktiviert werden. Nimmt man dieses Risiko in Kauf – insbesondere mit dem Gedanken, dass diese Problematik Millionen von Fanpages betrifft –, sollte der DSGVO so weit nachgekommen werden, wie es dem Betreiber im Moment möglich ist.

Dafür ist es notwendig, die Nutzer so umfangreich wie möglich zu informieren. Ihnen ist demnach mitzuteilen,

- dass Facebook personenbezogene Daten für Marktforschungs- und Werbezwecke verarbeitet und dabei zB aus dem Nutzerverhalten und daraus abgeleiteten Interessen Nutzungsprofile erstellt werden, die für die Bereitstellung individuell angepasster Werbung verwendet werden,
- dass Facebook zu diesem Zweck Cookies auf dem Rechner der Nutzer setzt,

- dass Daten unabhängig davon verarbeitet werden können, ob der Nutzer der Fanpage auch Facebook-Mitglied ist (Fanpages sind auch für Nicht-Nutzer zugänglich),
- dass diese Datenverarbeitungen aufgrund der berechtigten Interessen gemäß Art 6 Abs 1 lit f DSGVO des Fanpage-Betreibers erfolgen, die durch eine Fanpage ermöglichte Nutzer-Information und -Kommunikation anbieten zu können,
- dass diese ihre Betroffenenrechte direkt gegenüber Facebook ausüben können, der Fanpage-Betreiber ihnen dabei jedoch behilflich ist,
- unter welchen Kontaktdaten Facebook erreichbar ist und unter welchem Link die Datenschutzerklärung von Facebook abrufbar ist.

54. Was muss ich beachten, wenn ich auf meiner Website Platz für Online-Behavioral-Advertising zur Verfügung stelle?

Aus dem in Frage 53 dargestellten EuGH-Urteil C-210/16 *Wirtschaftsakademie Schleswig-Holstein* ist zu folgern, dass auch der Betreiber einer Website datenschutzrechtlich mitverantwortlich ist, wenn er auf seiner Website Platz dafür bereitstellt, dass Dritte dort Behavioral Advertising anbieten können, und dabei Daten verarbeitet werden (zB durch das Setzen von Cookies). Die Argumentation, dass der Website-Betreiber selbst keine Kontrolle über die in seine Website eingebundenen Werbeformen und daher keine Verantwortung für dabei stattfindende Datenverarbeitungen hat, greift demnach zu kurz.

Auch in diesem Fall hat der Website-Betreiber also vor allem dafür zu sorgen, dass diese Verarbeitungen auf einer Rechtsgrundlage beruhen, wobei oft eine Einwilligung nötig sein wird. Zudem müssen umfangreiche Informationen über die Datenverarbeitungen erteilt werden. Diese Pflichten werden hier jedoch um ein Vielfaches leichter erfüllt werden können als im Falle des Betreibens einer Facebook-Fanpage (siehe Frage 53), da der Geschäftspartner, der primär über die vor sich gehenden Verarbeitungen bestimmt, leichter greifbar ist.