DSGVO-INFO

DIE UMFASSENDE INFORMATIONSPLATTFORM

STIFTUNG DATENSCHUTZ

HINWEISE FÜR BLOGBETREIBER

Juni 2020

Prof. Dr. Anne Riechert

Seit Anwendbarkeit der DSGVO sind viele Blogbetreiber verunsichert, ob sie sich rechtskonform verhalten. Mancher Anbieter stellte seinen Blog aus Angst vor Bußgeldern sogar ein (http://web.archive.org/web/20180528171257/http://www.ennopark.de/2018/05/27/statt-links-der-woche-tote-links-der-woche/), auch wenn Constanze Kurz auf der Webseite netzpolitik.org (https://netzpolitik.org/2018/kommentar-zur-datenschutzgrundverordnung-das-war-erst-der-anfang/) darauf hinwies, dass viele der „Blog-Abschalter" die Schließung nur temporär planten oder „gerade keine Zeit oder kein Interesse am Umstellen" hätten.

Nachfolgend werden die datenschutzrechtlichen Anforderungen der DSGVO erörtert, die für das Betreiben eines Blogs relevant sein können. Technische Hinweise sind davon nicht umfasst.

A. Verzeichnis von Verarbeitungstätigkeiten

Nach der Datenschutzgrundverordnung gilt, dass Datenverarbeitungstätigkeiten dokumentiert werden müssen. Auch Blogbetreiber, die eine Kommentarfunktion zulassen, Newsletter versenden oder Plug-Ins verwenden, verarbeiten regelmäßig personenbezogene Daten und haben daher ein Verzeichnis von Verarbeitungstätigkeiten in einem schriftlichen oder elektronischen Format zu führen. Auf Anfrage muss dies der zuständigen Datenschutzaufsichtsbehörde zur Verfügung gestellt werden.

Von Seiten der Datenschutzaufsichtsbehörden wurde eine Mustervorlage für ein solches Verzeichnis von Verarbeitungstätigkeiten erstellt:https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf . Hinweise sind unter https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf abrufbar, ein Muster ist unter https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_verantwortliche.pdf veröffentlicht. Mit Blick auf die praktische Handhabbarkeit soll jedoch ergänzend auf das folgende Musterverzeichnis des Bayerischen Landesamtes für Datenschutzaufsicht hingewiesen werden. Dieses richtet sich zwar speziell an Vereine (https://www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf), enthält aber als Verarbeitungstätigkeiten unter anderem die Bereiche „Betrieb der Webseite" und „Veröffentlichung von Fotos". Dies kann eine gute erste Orientierung für Blogbetreiber darstellen, insbesondere da die Begriffe „betroffene Personen und personenbezogene Daten" mittels eines konkreten Beispiels beschrieben und darüber hinaus mögliche Löschfristen für die Daten dargestellt werden.

B. Informationspflichten

Dürfen Nutzer ihre Kommentare auf der Webseite einstellen oder werden personenbezogene Daten im Rahmen der Nutzung der Webseite (z.B. IP-Adresse) erhoben, muss eine Information über die damit zusammenhängende Datenverarbeitung erfolgen. Grundsätzlich ist für eine transparente Datenverarbeitung eine Information dahingehend erforderlich, wer welche personenbezogenen Daten zu welchem Zweck und für welche Dauer verarbeitet. In Artikel 13 DSGVO sind die umfassenden Informationspflich-

ten aufgelistet. Der Blogbetreiber muss daher entsprechende Datenschutzhinweise erstellen, die auf jeder Seite des Blogs mittels eines Links abrufbar sein sollten. Davon umfasst sind unter anderem Angaben zu seiner Identität, zu Auskunfts-, Berichtigungs-, Löschungs-, Widerspruchsrechte, zum Recht auf Datenübertragbarkeit, zum Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde oder zu Profilingmaßnahmen. Eine ausführliche Erläuterung der relevanten Informationspflichten der DSGVO findet sich beispielsweise in den Hinweisen der Industrie- und Handelskammer Mittlerer Niederrhein (https://www.ihk-krefeld.de/de/recht/internetrecht/datenschutzerklaerung-im-internet.html).. Bei Analysetools wie Google Analytics ist zu beachten, dass eine Einwilligung eingeholt werden **muss** (siehe hierzu die nachfolgenden Ausführungen).

Auf folgende Informationspflichten soll nochmals besonders hingewiesen werden:

Information über IP-Adressen

IP-Adressen werden als personenbezogene Daten eingestuft. Betrachtet man die Vorgehensweise der Datenschutzaufsichtsbehörden in Deutschland im Rahmen ihrer eigenen Webpräsenz, so gibt es dort Unterschiede in der Speicherpraxis: Teilweise werden IP-Adressen nur anonymisiert für statistische Zwecke gespeichert (https://datenschutz.hessen.de/datenschutzerkl%C3%A4rung), andere verweisen darauf, dass die IP-Adresse für den technischen Verbindungsaufbau notwendig ist, aber die IP-Adresse nicht dauerhaft gespeichert, ausgelesen oder anderweitig verwendet wird https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/03/Informationspflichten-02-2020.pdf). Teilweise wird die IP-Adresse auch vollständig für einen Zeitraum von sieben Tagen gespeichert und im Anschluss das letzte Oktett der IP-Adresse gelöscht, um eine anonymisierte Speicherung für statistische Zwecke vorzunehmen (https://www.lda.bayern.de/de/datenschutz.html). . Die vollständige Speicherung wird mit Zwecken der Datensicherheit begründet, also um unerlaubte Zugriffe aufklären oder Missbrauch der Internetseite verhindern zu können. Hintergrund ist eine gerichtliche Entscheidung, nach der die Speicherung erforderlich sein muss, „um die generelle Funktionsfähigkeit der Dienste zu gewährleisten“. Dabei muss allerdings stets eine Abwägung mit den Interessen der betroffenen Personen vorgenommen werden (siehe auch Pressemitteilung des Bundesgerichtshofs - http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2017&Sort=3&nr=78289&pos=1&anz=75). Blogbetreiber sollten daher prüfen, inwieweit Angriffe oder Missbrauch ihrer Webseite wahrscheinlich sind und daher eine Speicherung der IP-Adresse über das Verbindungsende hinaus überhaupt erforderlich ist.

Information über Cookies

In den Datenschutzhinweisen muss ein Blogbetreiber ebenso über die Nutzung von Cookies aufklären. Allerdings ist zu beachten, dass darüber hinaus eine Einwilligung eingeholt werden muss:

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) hat ein Positionspapier veröffentlicht (https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf). Danach wird nun für ein rechtskonformes Tracking eine vorherige informierte Einwilligung des Nutzers verlangt. Das bedeutet, dass eine **informierte Einwilligung** i. S. d. DSGVO eingeholt werden muss, d. h. z.B. **bevor Cookies platziert** werden bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.

Holt der Plattformbetreiber eine solche nicht ein, droht grundsätzlich ein Bußgeld oder eine Abmahnung. An dieser Auffassung wird vielfach Kritik geübt, so dass die zukünftige Rechtspraxis abzuwarten bleibt. Außerdem hat die Datenschutzkonferenz im März 2019 eine Orientierungshilfe für Anbieter von Telemedien veröffentlicht (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf).

Bekräftigt wird diese Rechtauffassung durch Urteile des Europäischen Gerichtshofs (EuGH) und des Bundesgerichtshofs (BGH). Der Bundesgerichtshof hat am 28.05.2020 entschieden, dass ein Diensteanbieter Cookies zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder Marktforschung nur mit Einwilligung des Nutzers einsetzen darf (http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=107623&pos=0&anz=1). Dieses Urteil basiert auf der Auffassung des EuGH, wonach keine wirksame Einwilligung vorliegt, wenn die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät des Nutzers einer Website gespeichert sind, mittels Cookies durch ein voreingestelltes Ankreuzkästchen erlaubt wird, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss (siehe Urteil vom 01.10.2019, abrufbar unter http://curia.europa.eu/juris/document/document.jsf;jsessionid=BD56B50E26B2706C0AFAAEB53CF30279?text=&docid=218462&pageIndex=0&doclang=de&mode=lst&dir=&occ=first&part=1&cid=10385480).

Information über Analysetools

Weiterhin besteht eine Informationspflicht über die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten sowie einer Verarbeitung in einem Drittland (d.h. wenn Daten in einem Land verarbeitet werden, welches kein EU-Mitgliedsstaat ist). Dies kann in Betracht kommen, wenn aufgrund der eingesetzten Plugins Daten in die Vereinigten Staaten übertragen werden (etwa Google Analytics). Siehe hierzu unter Punkt E. „Analysetools“. Auch an dieser Stelle soll vorab darauf hingewiesen werden, dass die Information nicht ausreichend ist, sondern eine Einwilligung eingeholt werden muss.

C. Vertrag zur Auftragsverarbeitung

Sofern Plattformbetreiber weitere Dienstleister im Rahmen der Datenverarbeitung einsetzen und diese Zugriff auf personenbezogene Daten erhalten, muss ein Vertrag zur Auftragsverarbeitung abgeschlossen werden. Dies betrifft etwa das Hosten der Plattform oder Dienstleister, die Newsletter im Auftrag des Plattformbetreibers versenden.

Die Landesbeauftragte für den Datenschutz Niedersachsen hat ein Vertragsmuster als Formulierungshilfe für die Auftragsverarbeitung veröffentlicht: https://www.lfd.niedersachsen.de/download/127630/Formulierungshilfe_zur_Auftragsverarbeitung_nach_Art._28_DS-GVO.pdf .

Ein Überblick ist unter folgendem Link zu finden: https://lfd.niedersachsen.de/startseite/themen/auftragsverarbeitung_nach_art_28_ds_gvo/auftragsverarbeitung-nach-art-28-ds-gvo-179673.html.

Die Datenschutzkonferenz hat ein Kurzpapier zu den Anforderungen einer Auftragsverarbeitung veröffentlicht (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf)

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz bietet außerdem in seinen FAQ - „Was ist neu bei der Auftrags(daten)verarbeitung?“ eine Hilfestellung an (https://www.datenschutz.rlp.de/de/themenfelder-themen/datenschutz-grundverordnung/faq/).

Nach Auffassung der Datenschutzkonferenz muss für einen IT-Wartungsvertrag ein Vertrag zur Auftragsverarbeitung abgeschlossen werden, für andere Dienstleistungen verneint sie dies (z.B. Steuerberater, Rechtsanwälte, Wirtschaftsprüfer, Postdienste für den Brieftransport). (https://www.datenschutz-konferenz-online.de/media/kp/dsk_kpnr_13.pdf)

Ergänzend ist auf folgendes hinzuweisen: In der Praxis besteht stets die Schwierigkeit, eine Auftragsverarbeitung von einer „gemeinsamen Verantwortlichkeit“ zu trennen.

Gemeinsame Verantwortlichkeit bedeutet, dass derjenige, der in der Praxis Einfluss auf die Zwecke und die Mittel der Verarbeitung hat, bei Rechtsverstößen zur Verantwortung gezogen werden kann. Relevanz hat dies etwa für Betreiber einer Website, in der der „Gefällt mir“-Button von Facebook eingebunden ist. Gemäß einer Entscheidung des Europäischen Gerichtshofs vom 29.07.2019 kann dieser für das Erheben und die Übermittlung der personenbezogenen Daten der Besucher seiner Website gemeinsam mit Facebook verantwortlich sein. Dagegen ist er grundsätzlich nicht für die spätere Verarbeitung dieser Daten allein durch Facebook verantwortlich (siehe unter http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=de&mode=req&dir=&occ=first&part=1&cid=10336163 sowie die Pressemitteilung unter https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-07/cp190099de.pdf).

D. Einwilligung

Eine informierte und freiwillige Einwilligung der Nutzer, die jederzeit widerrufbar ist, muss etwa bei Verwendung der Kommentarfunktion, bei Kontaktformularen oder Zusendung von Newslettern eingeholt werden. Über das jederzeitige Widerrufsrecht muss informiert werden.

Bei Verwendung von Web-Formularen sollte der Blogbetreiber darüber hinaus stets das Erforderlichkeitsprinzip beachten: Welche Angaben sind für die Nutzung des Angebots zwingend erforderlich? Nur diese Felder sollten als Pflichtfelder ausgestaltet sein. Alle übrigen Felder müssen transparent als freiwillige Angaben gekennzeichnet sein, und zwar auch unter der Information darüber, zu welchen Zwecken diese freiwilligen Angaben verwendet werden, welche Widerspruchs- und Widerrufsmöglichkeiten bestehen, wie lange die Daten gespeichert werden und wann eine (automatische) Löschung erfolgt. Im Übrigen ist zu berücksichtigen, dass in der Datenschutzgrundverordnung das Prinzip „Privacy by Design“ verankert ist. Daher sollten datenschutzfreundliche Voreinstellungen berücksichtigt werden, die die Erhebung und Speicherung von personenbezogenen Daten vermeiden. So kann beispielsweise anstatt eines Klarnamens des Nutzers ein frei gewählter Benutzername angegeben werden.

Insgesamt ist zudem die Sicherheit der Datenverarbeitung als eine Anforderung der Datenschutzgrundverordnung umzusetzen. Personenbezogene Daten oder auch Passwörter sollten verschlüsselt übertragen werden. Hier kann in der Praxis das https-Protokoll verwendet werden.

E. Analysetools

Wird das Analysetool Google Analytics auf der Webseite verwendet, haben die deutschen Aufsichtsbehörden in der Vergangenheit den Abschluss eines Auftragsdatenverarbeitungsvertrages (neuer Begriff unter der DSGVO: *Vertrag zur Auftragsverarbeitung*) zwischen dem Betreiber einer Webseite und Google Analytics verlangt. Hintergrund war, dass (wie oben bereits ausgeführt) die IP-Adresse der Nutzer seitens der Aufsichtsbehörden als personenbezogenes Datum eingestuft wird. Da Google außerdem durch Cookies Daten der Nutzer erfasst, musste in der Vergangenheit bislang in der Datenschutzerklärung der Webseite darüber hinaus ein Hinweis auf die Möglichkeit eines Widerspruchs gegen die Anfertigung von Nutzerprofilen eingeräumt werden. Hierzu konnte ein so genannter Browser-Add-On zur Verfügung gestellt werden, um insgesamt eine Datenerfassung durch Google zu vermeiden.

Da allerdings gemäß der Auffassung der Datenschutzkonferenz für ein rechtskonformes Tracking nun eine vorherige informierte Einwilligung des Nutzers erforderlich ist, ist diese Widerspruchsmöglichkeit bei Cookies nicht ausreichend. Bekräftigt wird diese Rechtauffassung durch die Urteile des Europäischen Gerichtshofs (EuGH) vom 01.10.2019 und des Bundesgerichtshofs (BGH) vom 28.05.2020: Ein Dienstanbieter darf Cookies zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder Marktforschung nur mit Einwilligung des Nutzers einsetzen (wie oben bereits dargestellt).

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit weist außerdem auf folgendes hin (https://datenschutz-hamburg.de/pressemitteilungen/2019/11/2019-11-14-google-analytics):

„Viele Website-Betreibende berufen sich bei der Einbindung von Google Analytics auf alte, längst überholte und zurückgezogene Veröffentlichungen wie die „Hinweise des HmbBfDI zum Einsatz von Google Analytics". Das Produkt Google Analytics wurde in den vergangenen Jahren so fortentwickelt, dass es in der aktuellen Gestaltung keine Auftragsverarbeitung mehr darstellt. Vielmehr räumt sich Google als Anbieter das Recht ein, die Daten auch zu eigenen Zwecken zu verwenden. Die Einbindung von Google Analytics erfordert daher eine Einwilligung, die den Anforderungen der Datenschutzgrundverordnung genügt. Die meisten der sogenannten Cookie-Banner erfüllen derzeit die gesetzlichen Anforderungen nicht."

F. In Kürze

Blogbetreiber sind regelmäßig verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten in einem schriftlichen oder elektronischen Format zu führen. Die Datenschutzaufsichtsbehörden haben eine Mustervorlage für ein solches Verzeichnis erstellt: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf. Auf der Webseite des Bayerischen Landesamtes für Datenschutzaufsicht sind darüber hinaus Musterverzeichnisse sowie Hinweise zu finden, die sich speziell an kleine Unternehmen und Vereine richten, aber aufgrund ihrer übersichtlichen Form auch für Blogbetreiber eine gute erste Orientierung darstellen können (https://www.lda.bayern.de/de/kleine-unternehmen.html).

Nach der Datenschutzgrundverordnung gelten außerdem umfassende Informationspflichten (Artikel 13 DSGVO), die in den Datenschutzhinweisen des Blogs umzusetzen sind. Diese Informationen müssen auch Ausführungen zur Erhebung und Löschung von IP-Adressen und Cookies enthalten. Zu beachten ist dabei, dass für ein rechtskonformes Tracking eine vorherige informierte Einwilligung des Nutzers verlangt wird. Das bedeutet, dass eine **informierte Einwilligung** i. S. d. DSGVO eingeholt werden muss, d. h. z.B. bevor Cookies platziert werden bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.

Eine ausführliche Erläuterung der relevanten Informationspflichten der DSGVO findet sich beispielsweise in den Hinweisen der Industrie- und Handelskammer Mittlerer Niederrhein (https://www.ihk-krefeld.de/de/recht/internetrecht/datenschutzerklaerung-im-internet.html) oder auf der Webseite der Landesbeauftragten für den Datenschutz Niedersachsen (https://lfd.niedersachsen.de/startseite/datenschutzreform/ds_gvo/faq/informationspflichten/informationspflichten-170998.html. Ebenso finden sich auf der Webseite des Bayerischen Landesamts für Datenschutzaufsicht Ausführungen zu den Informationspflichten mit weiterführenden Hinweisen (https://www.lda.bayern.de/de/thema_informationspflichten.html).

Ein Vertrag zur Auftragsverarbeitung ist beispielsweise abzuschließen, wenn Dienstleister mit der Verarbeitung von personenbezogenen Daten betraut werden, z.B. beim Hosten der Plattform, IT-Wartungsverträgen oder in Bezug auf Dienstleister, die Newsletter im Auftrag des Plattformbetreibers versenden. Kein Vertrag zur Auftragsverarbeitung ist etwa bei der Beauftragung von Steuerberatern oder Rechtsanwälten erforderlich

Blogbetreiber müssen außerdem an die Einholung einer Einwilligungserklärung denken, wenn sie die Kommentarfunktion zulassen, Kontaktformulare verwenden oder Newsletter zusenden. Bei einer Einwilligung ist stets ein jederzeitiges Widerrufsrecht sicherzustellen, über welches zusätzlich informiert werden muss. Personenbezogene Daten oder auch Passwörter sollten zudem verschlüsselt übertragen werden. Hier kann in der Praxis etwa das https-Protokoll verwendet werden.