DIGITALER ASSISTENT ZUR ERSTELLUNG VON DATENSCHUTZERKLÄRUNG UND VERFAHRENSVERZEICHNIS FÜR WEBSITES

Michael Weller / Ralph Hecksteden

Senior Berater IT-Compliance
Europaallee 10, 67657 Kaiserslautern, DE
m.weller@ebusiness-kompetenzzentrum.de

Geschäftsführer, jurmatix legal intelligence UG (haftungsbeschränkt),
Hauptstraße 28, 66453 Gersheim, DE
li@jurmatix.net; legalintelligence.jurmatix.net

Schlagworte: ***Datenschutzerklärung, Verarbeitungsverzeichnis, Assistenzsystem***

Abstract: *Das Erstellen einer korrekten Datenschutzerklärung für Websites stellt so manchen Website-Betreiber vor eine Herausforderung. Hinzu tritt, dass mit Blick auf die direkte Anwendbarkeit der Datenschutz-Grundverordnung auch dieses Verfahren in das gem. Art. 30 DS-GVO zu führende Verzeichnis der Verarbeitungstätigkeiten aufzunehmen ist. Sowohl die Erstellung der Datenschutzerklärung wie auch des Verfahrensverfahrensverzeichnisses lassen sich zumindest teilweise mit Hilfe eines «Datenschutz-Crawlers» automatisieren, so dass der digitale Datenschutz-Assistent Fehler vermeiden helfen kann.*

1. Problemaufriss

In Stichproben lässt sich feststellen, dass seit den im Jahr 2009 veröffentlichten Ergebnissen einer Untersuchung[1] zum Umgang mit Datenschutzerklärungen im Internet eine signifikante Qualitätsverbesserung ausgeblieben zu sein scheint. Dafür spricht auch ein zwischenzeitiges Datenschutz-Monitoring, nach dem die Zahl von Verstößen im Internet zugenommen hat.[2] Soweit in den betrachteten Webpräsenzen eine Datenschutzerklärung vorhanden war, war diese entweder nicht von jeder Unterseite aus erreichbar oder die Erklärung war unvollständig oder gar irreführend. Dies trifft nicht nur auf vom Anbieter selbst gebaute Websites zu, sondern auch auf solche, die von IT-Dienstleistern oder Agenturen erstellt wurden. Es muss davon ausgegangen werden, dass aufgrund dieser Mängel auch Verfahrensverzeichnisse gem. §§ 4g, 4e BDSG entweder nicht oder nicht richtig geführt werden. Die Vorbereitung auf die in Kürze unmittelbar anzuwendenden Bestimmungen der Datenschutz-Grundverordnung (DS-GVO)[3] bietet Gelegenheit, auch das Internetangebot einer Prüfung zu unterziehen. Diese Überprüfung ist insbesondere in Bezug auf die Pflicht zum Führen eines Verzeichnisses der Verarbeitungstätigkeiten gem. Art. 30 DS-GVO erforderlich und ein etwa noch nicht oder noch nicht den neuen Anforderungen genügendes Verzeichnis entsprechend zu erstellen bzw. zu modifizieren. Die Erstellung von Datenschutzerklärung und Verzeichnis lassen sich teilweise automatisieren, so dass digitale Assistenz bei der Herstellung von Compliance zielführend unterstützt.

---

1 Lepperhoff/Petersdorf, Umgang mit Datenschutzerklärungen im Internet – Ergebnisse einer empirischen Untersuchung, in: DuD 2009, 15 ff.

2 Lepperhoff/Petersdorf/Thursch, Datenschutzverstöße im Internet, DuD 2013, 301 ff.

3 Verordnung (EU) 2106/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

2. Rechtliche Anforderungen ab 25. Mai 2018

Die Einhaltung der Datenschutzrechtlichen Bestimmungen hat der gem. Art. 4 Nr. 7 DS-GVO Verantwortliche zu gewährleisten. Verantwortlicher in diesem Sinne ist derjenige, der über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Als personenbezogene Daten im hiesigen Kontext liegen jedenfalls die IP-Adressen vor, selbst wenn diese durch den Access-Provider dynamisch vergeben werden.[4] Dass künftig wegen Änderung der Definition des personenbezogenen Datums in Art. 4 Nr. 1 DS-GVO gegenüber der früheren Regelung in Art. 2 lit. a) der Datenschutz-Richtlinie[5] die IP-Adresse ausgenommen wird, steht nicht zu erwarten. Da der Anbieter der Internetseite über das «Ob» seines Internet-Auftritts entscheidet, fällt ihm die Entscheidung über das Erheben und Verarbeiten der IP-Adresse zu, womit er gem. Art. 4 Nr. 7 DS-GVO «Verantwortlicher» ist.

3. Pflichten des Website-Anbieters

Der Website-Anbieter ist nur dann berechtigt, personenbezogene Daten zu erheben und zu verarbeiten, wenn dies zu rechtmäßigen Zwecken in einer für die betroffenen Personen nachvollziehbaren Art und Weise geschieht, Art. 5 Abs. 1 lit. a) DS-GVO. Dies setzt voraus, dass zunächst überhaupt eine Berechtigung besteht, die IP-Adresse zu dem gem. Art. 5 Abs. 1 lit. b) DS-GVO festzulegenden Zweck zu erheben und die durch Art. 5 Abs. 1 lit. c) – f) DS-GVO gesetzten Grenzen nicht überschritten werden. Insoweit schreibt die DSGVO das bekannte Prinzip des Verbots mit Erlaubnisvorbehalt fort.

Der Anbieter der Website darf nach deutschem Recht gem. § 15 Abs. 1 TMG die IP-Adresse erheben und Verarbeiten, soweit und solange dies zur Inanspruchnahme seines Angebotes erforderlich ist. Darüber hinaus ist ihm gem. § 15 Abs. 3 TMG die Verarbeitung zu Werbezwecken, Zwecken der Marktforschung oder der bedarfsgerechten Gestaltung seines Angebotes mittels der Erstellung pseudonymer Nutzungsprofile dann erlaubt, wenn er den Nutzer auf sein Widerspruchsrecht gem. § 13 Abs. 1 TMG hingewiesen und der Nutzer von dieser Möglichkeit keinen Gebrauch gemacht hat.

Soweit hier die elektronische Kommunikation berührt ist, folgt die weitere Anwendbarkeit dieser nationalen Bestimmungen aus dem Umstand, dass die DS-GVO keine spezifischen Anordnungen trifft und auch die Datenschutzrichtlinie für elektronische Kommunikation[6] als lex specialis der DS-GVO vorgehen wird.[7] Insoweit ist durch die Bestimmung in Art. 95 DS-GVO klargestellt, dass die Verordnung gegenüber der RL 2002/58/EG keine besonderen, auf das gleiche Ziel gerichteten Anforderungen schafft.[8] Ein Inkrafttreten der ePrivacy-Verordnung zur Ablösung der Richtlinie ist zum Zeitpunkt der Manuskripterstellung noch nicht absehbar. Soweit die RL 2002/58/EG in nationales Recht umgesetzt wurde, bleibt dieses anwendbar.[9] Aufgrund der generellen Anforderung an die Zulässigkeit einer Verarbeitung personenbezogener Daten auf der Grundlage einer den Bedingungen aus Art. 7, 8 DS-GVO gerecht werdenden Einwilligung gem. Art. 6 Abs. 1 lit. a) DS-GVO ist auch die Frage der Erforderlichkeit des sog. «Cookie-Banner» beantwortet. Ohne die Zustimmung des Nutzers ist das Ablegen von Cookies nach dem Wortlaut der Norm unzulässig. Eine etwa anderslautende Regelung des nationalen Rechts wäre aufgrund des Anwendungsvorrangs der DS-GVO zwar nicht außer Kraft, jedoch nicht mehr anzuwenden.[10]

---

4 BGH, Urteil vom 16. Mai 2017 – VI ZR 135/13 – MMR, 2016, 605; EuGH, Urteil vom 19. Oktober 2016 – C-582/14 – MMR 2016, 842 – Breyer.

5 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

6 Richtline 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

7 Heckmann, in: Heckmann, jurisPK-Internetrecht, Kap. 9 Rn. 9.

8 Pauly, in: Paal/Pauly, Datenschutz-Grundverordnung, Art. 95 Rn. 2.

9 Pauly, in: Paal/Pauly, a.a.O., Rn. 3.

10 Vgl. EuGH, Urteil vom 15. Juli 1964 – C-6/64 – NJW 1964, 2371.

Das Website-Angebot stellt aufgrund der Erhebung und Verarbeitung der IP-Adresse ein datenschutzrechtlich relevantes Verfahren dar. Dieses ist gem. Art. 30 DS-GVO zu dokumentieren.[11] Die Befreiung von dieser Pflicht für Verantwortliche mit weniger als 250 Beschäftigten greift in Deutschland wegen der Gegenausnahme, nach der bei der Verarbeitung auch besonderer personenbezogener Daten gem. Art. 9 Abs. 1 DS-GVO die Pflicht nicht entfällt, nicht, wenn der Verantwortliche wenigstens einen Beschäftigten hat. Als Arbeitgeber verfügt der Verantwortliche mit dem für die Lohn- und Gehaltsabrechnung erforderlichen Kirchensteuermerkmal sowie aufgrund der Meldeobliegenheiten bei Krankheit über eben solche besondere Arten personenbezogener Daten.[12] Dies führt zu dem vom Verordnungsgeber möglicherweise gar nicht angestrebten Ergebnis, dass auch dann ein Verzeichnis zu führen ist, wenn es sich bei dem Verantwortlichen etwa um eine juristische Person mit einem einzigen Beschäftigten handelt.[13]

Der Dokumentation kann sich der Verantwortliche i.S. von § 4 Nr. 7 DS-GVO schon deshalb nicht entziehen, weil er aufgrund der ihm auferlegten Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO die Einhaltung der Anforderungen an die Rechtmäßigkeit der Verarbeitung nachweisen können muss.[14] Dies umfasst gem. Art. 24 Abs. 1 DS-GVO auch die gem. Art. 32 Abs. 1 DS-GVO zu treffenden technischen und organisatorischen Maßnahmen. Die gem. Art. 30 Abs. 1 lit. f) geforderten Angaben hat der Verantwortliche nach dem Wortlaut der Norm «wenn möglich» zu machen, was jedoch nicht als Entscheidung über das «Ob» solcher Informationen, sondern lediglich über das «Wieviel» verstanden werden darf.[15] Das Verzeichnis muss so ausführlich sein, dass es dem ggf. bestellten Datenschutzbeauftragten sowie der Aufsichtsbehörde eine Überprüfung der Angemessenheit des hergestellten Schutzniveaus ermöglicht.[16]

Gegenüber dem Betroffenen besteht die durch Art. 12 DS-GVO konkretisierte Transparenzpflicht gem. Art. 5 Abs. 1 lit. a) DS-GVO. Dies wird über die Fälle der technisch unvermeidbaren Erhebung der IP-Adresse während des Nutzungsvorganges besonders dann relevant, wenn die Nutzungsaktivitäten nachvollzogen werden sollen. Insoweit sind durch EG 24 DS-GVO vor allem Tracking-Services datenschutzrelevant, da diese dem dort erwähnten Nachvollzug der Internetaktivitäten der Nutzer dienen.[17] Der Website-Anbieter muss gem. Art. 12 DS-GVO die in Art. 13, 14 DS-GVO genannten Informationen zur Verfügung stellen und insbesondere auf die Einbeziehung von Diensten mit einem Sitz in einem Nicht-EU-Land hinweisen. Besondere Aufmerksamkeit verlangt die neue Regelung zur Wirksamkeit von Einwilligungen Minderjähriger bei ihnen direkt unterbreiteten Angeboten. Insoweit ist im Einzelfall zu erwägen, ob ein System zur Altersverifikation erforderlich sein kann.[18]

4. Prototypischer Entwurf eines digitalen Assistenten

Die in einer Datenschutzerklärung dem Nutzer zu gebenden Informationen lassen sich durch einen Blick darauf, welche Daten von dem Nutzer tatsächlich erhoben werden, ermitteln. Die für die Formulierung einer Datenschutzerklärung anzutreffenden Dienste im Internet sind in der Regel so gestaltet, dass der Ersteller Ele-

---

11 Licht, Das Verarbeitungsverzeichnis der DSGVO, in: ITRB 2017, 65; Wybitul, Welche Folgen hat die EU-Datenschutz-Grundverordnung für Compliance?, in: CCZ 2016, 194 (197); Martini, in: Paal/Pauly, Datenschutz-Grundverordnung Art. 30 Rn. 1.

12 Hartung, in: Kühling/Buchner, Datenschutz-Grundverordnung Art. 30 Rn. 38.

13 Martini, in: Paal/Pauly, Datenschutz-Grundverordnung Art. 30 Rn. 31.

14 Hamann, Europäische Datenschutz-Grundverordnung – neue Organisationspflichten für Unternehmen, in: BB 2017, 1090 (1092).

15 Spoerr, in: Wolff/Brink, Beck'scher Online-Kommentar Datenschutzrecht, Art. 30 DS-GVO Rn. 10; Martini, in: Paal/Pauly, Datenschutz-Grundverordnung Art. 30 Rn. 19.

16 Gossen/Schramm, Das Verarbeitungsverzeichnis der DS-GVO, in: ZD 2017, 7 (13); Martini, in: Paal/Pauly, Datenschutz-Grundverodnung a.a.O.

17 Ernst, in: Paal/Pauly, Datenschutz-Grundverordnung, Art. 3 Rn. 16.

18 Hierzu im Einzelnen: Krüger/Vogelgesang/Weller, Datenschutz für Minderjährige nach der Europäischen Datenschutz-Grundverordnung (DSGVO) vom 27. April 2016, in: Trends und Communities der Rechtsinformatik, Tagungsband des 20. Internationalen Rechtsinformatik-Symposions IRIS 2017, Österreichische Computer-Gesellschaft, Wien 2017, S. 493–500.

mente, die nach seiner Kenntnis relevant sind, anklickt und hieraus eine Datenschutzerklärung mittels Textbausteinen erstellt wird, die schließlich per Copy & Paste auf die Website übernommen werden kann. Kommt es zu Modifikationen der Homepage, insbesondere durch Abschalten, Hinzufügen oder Wechseln von Skripten oder Plugins, wird dies in der Datenschutzerklärung oft nicht nachgeführt. Hinzu tritt, dass eine ganze Reihe von Skripten eingesetzt werden können, für die die verschiedensten Angaben in die Datenschutzerklärung aufzunehmen sind und daher genau klar sein muss, welches Skript oder Plugin verwendet wird. Es lassen sich in der Praxis regelmäßig ein Auseinanderfallen von Angaben in der Datenschutzerklärung und tatsächlich verwendeten Skripten und Plugins feststellen.

Welche Daten beim Aufruf einer Website von dem Nutzer erhoben werden, lässt sich technisch mittels eines Crawlers automatisiert feststellen. Das Ausgabeergebnis des Crawlers lässt sich sodann weiter nutzen, um hieraus aus Textbausteinen die zutreffende Datenschutzerklärung zu generieren. Dadurch lassen sich Fehler infolge falscher manueller Anwahl von Textbausteinen vermeiden.

Da durch das Crawlen die datenschutzrelevanten Vorgänge geklärt werden können, lässt sich hierdurch auch das zu führende Verzeichnis der Verarbeitungstätigkeiten in Bezug auf das Website-Angebot zumindest insoweit automatisiert erstellen, als die Informationen zur Art der von dem Nutzer erhobenen und verarbeiteten Daten sowie etwaige Übermittlungsvorgänge etwa an die Anbieter von Skripten und Plugins erfasst und in Bezug zu den rechtlichen Grundlagen der Zulässigkeit der Datenverarbeitung gesetzt werden. Ergänzen muss der Website-Anbieter dann lediglich noch die Angaben, die nicht automatisiert feststellbar sind, wozu auch die getroffenen technischen und organisatorischen Maßnahmen zu rechnen sind. Insoweit kann jedenfalls die Notwendigkeit des Treffens solcher Maßnahmen aufgezeigt werden.

Der Prototyp des Datenschutz-Crawlers fokussiert die aus unserer Sicht typischen Problemlagen. Zu diesen zählen:

- Vorhandensein einer maschinenerkennbaren Datenschutzerklärung,
- Verwendung von Cookies,
- Verwendung von Reichweitenanalyse-Werkzeugen und deren datenschutzkonformer Einsatz,
- Verwendung von Bibliotheken, die ein Nachladen von Webseiten dritter Anbieter erfordern und damit Nutzungsdaten an den Dritten übermitteln,
- Standort des Rechenzentrums des Webhosting- und E-Mail-Providers und die damit verbundene Datenübertragung innerhalb/außerhalb des europäischen Wirtschaftsraumes.

Der Crawler ist als Webanwendung konzipiert. Die Clientoberfläche basiert auf dem HTML5-konformen Framework Bootstrap und den Javascript-Komponenten von jQuery. Serverseitig wird eine Sammlung von Programmen ausgeführt, die die zu bewertende Webseite herunterladen und die HTML-Baumstruktur (DOM) dieser Webseite nachbauen. Mittels XPath[19] wird daraufhin nach vordefinierten Mustern gesucht. Diese Muster sind als reguläre Ausdrücke in einer Konfigurationsdatei abstrahiert und können beliebig erweitert und angepasst werden.

Das Ergebnis des serverseitigen Crawl-Vorgangs wird an den Client mittels JavaScript Object Notation (JSON) übergeben. In dieser Weboberfläche werden dann die Bewertung der oben aufgezählten Problemlagen und die weiteren notwendigen Operationen zur Erstellung von Datenschutzerklärung und Verfahrensverzeichnis vorgenommen. Die zur Demonstration verwendete Version ist nicht auf Vollständigkeit, sondern auf das Aufzeigen der technischen Möglichkeiten ausgerichtet. Der Datenschutz-Crawler wird in der nächsten Zeit weiter ausgebaut.

[19] XML Path Language (XPath), https://www.w3.org/TR/1999/REC-xpath-19991116/.