KANZLEI-HOMEPAGE UND DATENSCHUTZ

Rechtsanwalt Dr. Ralph Wagner, Dresden, BRAK-Ausschuss Datenschutzrecht

Die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) gilt seit dem 25.5.2018 unmittelbar und zwingend in sämtlichen EU-Mitgliedstaaten, auch für Rechtsanwälte. Jede Anwaltskanzlei hat Änderungsbedarf zu prüfen und ggf. über neue, datenschutzfreundliche Gestaltungen zu entscheiden.

Die Kontrolle und Anpassung der eigenen Homepage besitzt dabei Priorität, schon allein deshalb, weil die Internetpräsenz als „Tor zur Welt" der öffentlichen Kanzleidarstellung dient, also von Jedermann – auch auf Datenschutzkonformität – geprüft werden kann. Gleichzeitig werden in vielen Fällen Daten von Besuchern der Homepage erhoben. (Nicht immer ist dies von den Betreibern der Homepage beabsichtigt oder ihnen überhaupt bekannt.)

Der vorliegende Beitrag soll bei diesen Arbeiten helfen. Allgemeine Fragen, wie z.B. die Impressumspflichten, bleiben außen vor – insoweit bringt die DSGVO keine Änderungen.

DIE EIGENE HOMEPAGE KENNENLERNEN

Datenschutzrechtlich bestehen im Wesentlichen zwei Anforderungen für unternehmerische Webpräsenzen: Der Verantwortliche hat (1) dafür zu sorgen, dass auf der Website keine unzulässigen Datenverarbeitungen stattfinden und er muss (2) die Besucher über die stattfindenden Datenverarbeitungen informieren.

Foto: grafikplusfoto/fotolia

In der Praxis besteht häufig ein Problem darin, dass die Kanzleiinhaber selbst technische Details der eigenen Homepage nicht oder nur teilweise kennen. Erstellung und Betrieb der Homepage werden meist externen Dienstleistern übertragen. Der Datenschutz zwingt nun dazu, insoweit nachzuforschen. Dies kann erneut durch Beauftragung eines Spezialisten geschehen. Zumindest ergänzend empfiehlt sich aber eigene Kontrolle.

Folgende Fragen sind datenschutzrelevant und sollten dem beauftragten Dienstleister gestellt werden:

- Überträgt die Kanzlei-Homepage Besucherdaten an Dritte, ggf. an wen und für welche Zwecke?
- Werden Cookies gesetzt, ggf. durch wen und für welche Zwecke?
- Ist die Übertragung der Webpräsenz gesichert, erfolgt also eine Datenübertragung im https-Protokoll?
- Ist die Erhebung personenbezogener Daten in Kontaktformularen auf das notwendige Maß beschränkt?

Eine gute Möglichkeit der Datenschutz-Diagnose (ggf. auch eine Möglichkeit, die Antworten des Dienstleisters auf die oben genannten Fragen zu prüfen) bietet z.B. die Seite https://webbkoll.dataskydd.net/en/. Nach Eingabe der eigenen Internetadresse wird ermittelt und angezeigt, welche technischen Datenschutzmängel bestehen. (Den Angaben des schwedischen Anbieters zufolge werden die Testergebnisse 48 Stunden lang auf dem dortigen Server gespeichert und dann gelöscht. Der Anbieter erzeugt weder Prüflisten, noch werden die eingegebenen Daten anderweitig genutzt.)

SICHER IST SICHER: VERSCHLÜSSELUNG

Internetverbindungen über das unverschlüsselte Protokoll http können (mit entsprechendem technischen Sachverstand) leicht überwacht und beeinflusst werden. Möglich sind z.B. sogenannte „Man-in-the-middle"-Attacken, bei denen Dritte in die Rolle der besuchten Homepage „schlüpfen". Konkret: Der Besucher Ihrer Kanzlei-Homepage nutzt das Kontaktformular – die Nachricht gelangt aber nicht zu Ihnen, sondern zu einem Unbefugten.

Foto: mbruxelle/fotolia

Eine deutliche Erhöhung der Kommunikationssicherheit ist durch Verwendung des verschlüssel-

ten Protokolls https erreichbar. Kurz gefasst: http-protokollierte Präsenzen sollten zügig auf https „umsteigen".

WENIGER IST MEHR: PROGRAMMIERUNG

Wenn die Kanzlei-Homepage Besucherdaten an Dritte übermittelt, muss dafür eine Rechtsgrundlage existieren. Nicht selten wurden solche Datenübermittlungen bei der Programmierung der Homepage gedankenlos (als Teil arbeitserleichternder Programmpakete) implementiert.

Foto: blende11.photo/fotolia

Musterbeispiel sind die viel diskutierten Analysetools. Wenn auf der Website z.B. Google Analytics (oder eine der vielen Alternativlösungen anderer Anbieter) eingesetzt wird, frage man sich zuerst: Haben wir das jemals genutzt? In zahlreichen Fällen ist den Verantwortlichen der Homepage die Einbindung der Tools gar nicht bekannt. Dann sollte nicht über Möglichkeiten anonymisierter Analyse nachgedacht, sondern das Tool gelöscht werden.

Für jede andere Datenübermittlung an Dritte gilt dasselbe Grundmuster: Benötigt wird eine Rechtsgrundlage, noch davor stelle man sich aber die Frage nach dem Sinn der Verarbeitung. Fehlt mindestens eines von beiden, ist technisch zu ändern (zu löschen).

Illustrativ sei darauf hingewiesen, dass z.B. die Einbindung von Google Maps (bei Anfahrtsskizzen), Google Captcha Codes (zur Absicherung von Kontaktformularen gegen Spam-Mails) und Google Fonts (zur Nutzung gestalteter Schrifttypen ohne urheberrechtliche Lizenzzahlungen) jeweils Datenübermittlungen generiert. Die Weitergabe von Besucherdaten an Dritte kann technisch unterbunden werden, indem der jeweilige Bereich ohne Rückgriff auf „datenfordernde" Drittanbieter programmiert wird.

Bei eigenen und fremden Cookies (also Übertragung von Dateien auf den Rechner des Homepage-Besuchers) stellt sich ebenso zuerst die Frage der Notwendigkeit. Ist kein sinnvoller Zweck erkennbar, soll und muss auf Cookies schlicht verzichtet werden.

Zu beachten ist für die Verarbeitung von Besucherdaten (Tracking) die Stellungnahme der Datenschutz-Konferenz vom 26.4.2018 (abrufbar z.B. unter ldi.nrw.de, Datenschutz>Technik>Technik und Organisation). Die Aufsichtsbehörden gehen davon aus, dass seit dem 25.5.2018 Internet-Tracking nur nach Art. 6 I DSGVO (insbesondere Buchstaben a, b und f) legitimiert werden kann. Daraus ergibt sich ein zusätzliches Argument für den Verzicht auf – häufig unnötig und historisch zufällig entstandene – Datenverarbeitungen.

TRANSPARENZ

Für diejenigen Verarbeitungsvorgänge, die nach den vorstehenden Schritten noch verbleiben, ist den Besuchern der Homepage mitzuteilen, welche Daten für welche Zwecke und welchen Zeitraum verarbeitet werden. Außerdem schreibt Art. 13 DSGVO Informationen über diverse Betroffenenrechte vor. Beides sollte auf der Homepage leicht auffindbar (also z.B. in einer Rubrik „Datenschutz" oder „Datenschutzerklärung") untergebracht werden.

Welche Informationspflichten im Einzelnen bestehen, ist Art. 13 DSGVO zu entnehmen; Formulierungsbeispiele finden sich im Internet (derjenige des DAV unter anwaltsblatt.anwaltverein.de/files/anwaltsblatt.de/dokumente/2018/s0196_1_t8938.html).

LAST BUT NOT LEAST: DIENSTLEISTERVERTRÄGE

Wie bereits mehrfach angesprochen, sind bei Erstellung und Betrieb der Homepage in fast allen Kanzleien externe Spezialisten (Programmierung, Hosting) beteiligt. Soweit mit ihren Tätigkeiten der Zugriff auf personenbezogene Daten einhergeht, sind sie im Datenschutz als Auftragsverarbeiter einzuordnen, mit denen Verträge gemäß Art. 28 DSGVO benötigt werden. Verwendbare Vertragsklauseln sind im Internet leicht zu finden (Formulierungsvorschlag aus Sicht der Aufsichtsbehörde z.B. unter lda.bayern.de/media/muster_adv.pdf).

Datenschutzrechtlich vorzugswürdig (weil leichter regelbar) sind Vertragspartner innerhalb des Europäischen Wirtschaftsraums (EWR). Werden Unternehmen außerhalb des EWR eingeschaltet, muss die Einhaltung eines angemessenen Datenschutzniveaus zusätzlich sichergestellt werden. In der Praxis empfiehlt sich dann die Verwendung der Standardvertragsklauseln der Europäischen Kommission für Auftragsverarbeitungen (abrufbar z.B. unter eur-lex.europa.eu/lexuriserv/lexuriserv.do?uri=OJ:L:2010:039:0005:0018:de:pdf).

Immer gilt: Fragen Sie zuerst den Dienstleister – für ihn ist die Auftragsverarbeitung Massengeschäft; er verwendet meist eigene Muster.