Datenschutzgrundverordnung

Warum Kanzleien ein SSL-Zertifikat benötigen

von RA Heike Mareck, zertifizierte externe Datenschutzbeauftragte, Dortmund, www.kanzlei-mareck.de

| 12.500 EUR: DSGVO-Abmahnung für fehlendes SSL-Zertifikat. So lautete vor einigen Wochen die Meldung in der Presse. In der Tat: Wenn Sie auf Ihrer Kanzleiwebsite ein Kontaktformular hinterlegt haben, prüfen Sie bitte, ob Sie auch ein SSL-Zertifikat haben. Doch in Panik zu verfallen, wäre hier unangebracht. Die sieben wichtigsten Fragen zum SSL-Zertifikat für Ihre Website erhalten Sie hier. |

Was ist ein SSL- oder TLS-Zertifikat?

Ein SSL-Zertifikat stellt sicher, dass Daten zwischen dem Kunden und dem Webserver sicher übertragen werden. Die Daten zwischen Kunden und dem Webserver können bei SSL-Zertifikaten nicht abgehört oder ausgelesen werden. Demzufolge ist die Kommunikation online bei Webseiten, die ein SSL-Zertifikat nutzen, aus datenschutzrechtlicher und personenrechtlicher Sicht sichergestellt. Jetzt heißt das SSL-Zertifikat auch TLS-Zertifikat – im täglichen Verkehr ist das SSL-Zertifikat geläufiger.

Ist das Pflicht?

Für Kanzleien, die auf ihrer Website ein Kontaktformular, Bestell-, Online-Widerrufsformulare sowie Newsletter-Anmeldungen haben, ist das SSL-Zertifikat bereits seit Anfang 2016 Pflicht (§ 13 Abs. 7 TMG). Das haben allerdings viele versäumt. Auch die Agenturen wiesen darauf nicht immer hin. Spätestens seit dem 25.5.2018 sollte SSL für alle Formulare (z. B. Kontakt-, Bestell-, Online-Widerrufsformulare sowie Newsletter-Anmeldungen) auf der Website vorhanden sein.

Wozu dient das SSL-Zertifikat?

Bei der Nutzung eines Kontaktformulars werden personenbezogene Daten nach der Datenschutz-Grundverordnung (DSGVO) verarbeitet. Und jede Verarbeitung von personenbezogenen Daten braucht eine Rechtsgrundlage. Hier kommen „wirtschaftliche Interessen“ nach Art. 6 Abs. 1 lit. f DSGVO in

Betracht für die Erhebung von personenbezogenen Daten durch Kontaktformulare auf Ihrer Website.

Welche Vorteile bietet so ein Zertifikat?

Neben den Sicherheitsaspekten werden Sie von Suchmaschinen besser gerankt als Ihre Mitbewerber, die keine SSL-Verschlüsselung haben. Außerdem zeigen die Browser Warnungen an, wenn die SSL-Verschlüsselung fehlt. Gerade höher validierte SSL-Zertifikate werden bevorzugt angezeigt: EV-Zertifikate, also jene mit der höchsten Validierung, werden sogar mit grüner Adressleiste dargestellt. Sicherheit wird damit sichtbar.

Woran erkenne ich eine SSL-Verschlüsselung?

Ob die Verbindung eine gesicherte SSL-Verbindung ist, erkennen Sie an der Angabe am Browser. In der Adresszeile ist ein verschlüsselter Aufruf sichtbar an der Angabe https. Wenn nur http dort steht, dann ist meist kein SSL-Zertifikat vorhanden. Gibt man zur Überprüfung https in die Browserleiste ein und es gibt kein SSL-Zertifikat, erscheint danach eine Fehlermeldung. Zusammengefasst:

- Die URL in der Adressleiste Ihres Browsers beginnt mit „https://“. Eine Webseite, dessen Adresse mit „http://“ beginnt wird nicht durch SSL geschützt!
- Neben der Adressleiste des Webbrowsers erscheint ein „Schloss-Symbol“. Mit einem Klick darauf erhalten Sie detaillierte Informationen über das verwendete SSL-Zertifikat und den Betreiber der Webseite.
- Die Adressleiste des Webbrowsers färbt sich (teilweise) grün. Diese grüne Färbung signalisiert ein EV-Zertifikat; ein Zertifikat, das mit den höchsten Standards validiert wurde.

Auf der Webseite wird ein Site-Seal dargestellt, welches dem Besucher per Klick ebenfalls detaillierte Informationen zum Zertifikat, Inhaber und Aussteller ausgibt.

Wie erkenne ich eine sichere Verbindung?

Sie erkennen es am Schloss in der Adressleiste Ihres Webbrowsers. Anbei die gängigsten Beispiele:

= Firefox Browserleiste

= Explorer Browserleiste

= Chrome Browserleiste

Kein Kontaktformular auf der Website: Verschlüsseln?

Meist ist es aufwendiger, einzelne Unterseiten zu verschlüsseln als die komplette Website. Aus wirtschaftlichen Überlegungen ist eine Vollverschlüsselung in den meisten Fällen das Mittel der Wahl. Darüber hinaus werden Seiten ohne SSL-Verschlüsselung von Google sanktioniert. Bestimmte Browser zeigen mittlerweile eine fehlende Verschlüsselung offen an und weisen auf den fehlenden Schutz der Daten hin. Also: Verschlüsseln Sie!

PRAXISTIPP | Am einfachsten erhalten Sie ein SSL-Zertifikat über Ihren Provider (zum Beispiel 1&1, Vodafone, goneo, jimdo). Diese bieten entweder kostenlos oder -pflichtig ein SSL-Zertifikat an, je nach Ausführung, meist zwischen 1 und 10 EUR. Alternativ können Sie Ihre Agentur beauftragen, die Verschlüsselung für Ihre Website vorzunehmen.