DSGVO Checkliste

Für ihre Kanzleihomepage

1 HOSTING & DATENSICHERHEIT

- ☑ Hat ihre Website ein SSL-Zertifikat?
- ☑ Haben Sie Maßnahmen ergriffen, um ihren Blog oder ihre Website gegen Hacker oder unbefugte Dritte zu schützen (sichere Dateirechte, sichere Passwörter, regelmäßiges Installieren von Sicherheitsupdates etc.)?
- ☑ Haben Sie einen Vertrag zur Auftragsdatenverarbeitung mit ihrem Hosting-Anbieter abgeschlossen?

2 ANALYSETOOLS

- ☑ Haben Sie ein Analyse-Tool im Einsatz?
  - ☑ Falls ja, welches (z. B. Google Analytics, Piwik oder WordPress.com-Stats)?
- ☑ Sind die IP-Adressen anonymisiert?
- ☑ Liegen die Daten auf ihrem Server oder bei einem Drittanbieter?

- [ ] Falls Drittanbieter, sind die Daten adäquat geschützt? Haben Sie einen Vertrag zur Auftragsdatenverarbeitung (ADV-Vertrag) mit dem Drittanbieter abgeschlossen?

- [ ] Haben Sie sichergestellt, dass Nutzer anhand eines Klicks der Erfassung widersprechen können (der Link dazu sollte in der Datenschutzerklärung sein)?

FORMULARE

- [ ] Haben Sie Formulare auf ihrer Webseite eingebunden, die personenbezogene Daten übertragen?
  - [ ] Wenn ja, haben Sie unterhalb, oberhalb oder neben dem Formular darauf hingewiesen (in Kurzform), was mit den Daten passiert, wenn sie gesendet werden und auf ihre Datenschutzerklärung hingewiesen, in der Sie das ganze ausführlich beschreiben?
- [ ] **Wichtig**: kein Formular ohne HTTPS!

NEWSLETTER

- [ ] Nutzen Sie einen Newsletter-Dienst oder -Plugin?

- [ ] Erfolgt der Eintrag nur nach einem Double-Opt-In-Verfahren (also Eintrag der E-Mail-Adresse im Anmeldeformular und anschließende Bestätigung per Adresse per E-Mail-Link)?

- [ ] Haben Sie mit ihrem Eintragungsformular darauf hingewiesen, was der Interessent von Ihnen erhält, wenn er sich einträgt? Sind Sie transparent und haben offen geschrieben, wenn Sie neben Informationen und Artikeln auch Angebote versenden?

- [ ] Haben Sie mit ihrem Newsletter-Dienstleister einen ADV-Vertrag geschlossen?

- [ ] **Vorsicht bei Dienstleistern außerhalb der EU:** In dem Fall reicht ein einfacher Vertrag zur ADV nicht aus. Bei nicht-europäischen Anbietern müssen Sie sich zusätzliche Informationen des Datenimporteurs bezüglich Datenschutz (am besten vertraglich) nachweisen lassen. Bei US-amerikanischen Dienstleistern wie Mailchimp ist es zudem nötig, dass das Unternehmen nach dem **EU-US Privacy Shield** zertifiziert ist (wobei es immer noch nicht eindeutig geklärt ist, ob das tatsächlich ausreicht).

PLUGINS, WIDGETS ETC.

- Nutzen Sie auf ihrer Website Plugins, Widgets, iFrames, zusätzlichen Scripte oder Schnittstellen?
- Werden dadurch personenbezogene Daten auf ihrer Website oder bei Drittanbietern gespeichert? Wenn ja, zu welchem Zweck? Fließen nur die benötigten Daten, damit der Dienstleister seinen Job machen kann oder wird zu viel übertragen?

- Persönliche Daten werden z. B. gesammelt bei Membership-, Formular-Plugins, Social- oder Newsletter-Plugins.
- Am einfachsten ist in der Dokumentation oder auf der Website des Entwicklers zu lesen, ob ein Plugin, Widget etc. DSGVO-konform nutzbar ist. Leider ist nicht jeder Entwickler so transparent (oder hat überhaupt ein Bewusstsein für die Anforderungen der DSGVO), daher muss man oft selbst den Dienst durchleuchten.
- Falls Daten übertragen werden, brauchen Sie eine ADV mit dem Dienstleister. Das sollte einfach sein, wenn der Partner in der EU sitzt. Ist er allerdings in einem Drittland, was gerade bei Plugins häufiger der Fall ist, wird es schwieriger. Sie brauchen einen Vertrag und auf jeden Fall den Zusatz, wie die Daten bei der Übertragung und beim Dienstleister geschützt sind.

6 MARKETING & WERBUNG

- Nutzen Sie Dienste wie Facebook Pixel, DoubleClick, Google AdSense oder ähnliches? Dann müssen Sie ausführlich darüber in der Daten-schutzerklärung schreiben!
- Der Einsatz von Werbe-Trackern ist nicht ganz unumstritten. Stellen Sie daher sicher, dass Sie Nutzern, soweit Sie einen “erweiterten Abgleich ihrer Daten” machen, eine Opt-Out-Möglichkeit bereitstellen.
- Vor allem beim **Retargeting** (auch Remarketing genannt) wäre es sogar noch besser, wenn der Nutzer per Opt-In dem Tracking zustimmen muss.

7 SOZIALE MEDIEN

- Nutzen Sie Plugins oder Widget von sozialen Netzwerken wie Facebook, Twitter, Pinterest und Co.?
  - Wenn ja, stellen Sie sicher, dass diese keine personenbezogenen Daten übertragen, bevor Nutzer widersprechen können! Das gilt z. B. für die Standard-Sharing-Buttons oder das Seiten-Plugin von Facebook.

- Alternativ können Sie mit einfachen Links auf ihre sozialen Plattformen verweisen und für die Sharing-Buttons das Plugin Shariff nutzen (falls Sie WordPress verwenden).

- Sind die sozialen Netzwerke und deren Umgang mit personenbezogenen Daten in ihrer Datenschutzerklärung zu finden? Ergänzen Sie in der Datenschutz-erklärung auch, ob und wie Sie die Daten aus Facebook für ihr Unternehmen verwenden!

- Haben Sie auf ihren Social-Media-Seiten ein Impressum und eine Daten-schutzerklärung angegeben oder von dort aus auf die entsprechenden Seiten auf ihrer Website verlinkt?

- Haben Sie in ihrer Datenschutzerklärung erwähnt, dass diese auch für Facebook, Instagram und Co. gilt?

DATENSCHUTZERKLÄRUNG

- Stellen Sie sicher, dass zu allen oben genannten Wegen, auf denen die personenbezogene Daten verarbeitet werden, eine Passage in der Datenschutzerklärung zu finden ist!

Achten Sie aber darauf, dass sie DSGVO-konform sind, da z. T. noch zusätzliche Informationen nötig sind, die bisher nicht in der Datenschutzerklärung enthalten waren.

QUELLE

HTTPS://WWW.BLOGMOJO.DE/DSGVO-CHECKLISTE/

Ansprechpartner: Georg Kassuhn
www.kanzleimarketing-gkwebsolution.de
info@gk-websolution.de