Anhang a zu Schritt 6:
Anleitung – wie Sie Ihre Website auf die DSGVO vorbereiten

Diese Anleitung soll Ihnen dabei helfen, Ihre Website und Ihr Online-Marketing (Google Analytics, Facebook, Newsletter etc.) auf die DSGVO vorzubereiten.

Inhalt

In 5 Schritten zur DSGVO-„sicheren“ Website

Schritt 1: Datenschutzerklärung erstellen und richtig veröffentlichen

Die **Datenschutzerklärung** ist das Erste, was für die Öffentlichkeit sichtbar ist – daher sollten Sie großen Wert darauf legen, diesen Schritt ordentlich umzusetzen.

Wenn Sie eine schlechte (oder gar keine) Datenschutzerklärung auf Ihrer Website haben, sind Sie ab 25. Mai 2018 stark **für Abmahnungen gefährdet**. Denn es gibt viele Anwälte, die davon leben, Websites auf Datenschutz-Verstöße zu durchsuchen und Abmahnungen auszuschicken (sogenannte „Abmahn-Anwälte“).

Als erstes sehen sich die **Abmahn-Anwälte** die Datenschutzerklärung auf den Websites an – und wenn Ihre Datenschutzerklärung professionell erscheint, sind Sie schon auf der sicheren Seite.

Außerdem setzen Anwälte häufig auch **Tools** ein, mit denen Sie Websites automatisch auf Datenschutzlücken durchsuchen. Diese Tools erkennen, ob Codes von Facebook, Google etc. (z. B. Facebook Like-Button oder Pixel, Google Analytics) auf Ihrer Website eingebaut sind. Daher wäre es sinnvoll, wenn Sie selbst auch ein solches Tool nutzen (wie die Abmahn-Anwälte es machen), um Ihre Website auf DSGVO-Verstöße zu prüfen.

Ihre Aufgaben:

- **Ihre Website auf Erweiterungen prüfen**: Fragen Sie Ihre Internet-Agentur oder nutzen Sie ein Tool (wie z. B. *Ghostery* – *https://www.ghostery.com/de/*). Ein solches Tool zeigt Ihnen, welche Erweiterungen auf Ihrer Website installiert sind. Diese Erweiterungen schreiben Sie alle auf, um sie im nächsten Schritt in Ihrer Datenschutzerklärung einzubauen.

- **Datenschutzerklärung erstellen**
  - Tipp: Verwenden Sie einen **Generator**: Damit haben Sie natürlich keine 100%ige Rechtssicherheit – das geht nur mit einem Anwalt. Doch Abmahn-Anwälte suchen sich „leichte Opfer“. Zumindest 99 % Rechtssicherheit erreichen Sie in der Regel auch mit Hilfe von Generatoren und Vorlagen.

- **Beispiele** für Datenschutzerklärungs-Generatoren:
  - Datenschutz-Generator von eRecht24-Premium: *https://www.e-recht24.de/muster-datenschutzerklaerung.html* (derzeit um € 14,90 erstellbar – Abo kann sofort wieder gekündigt werden)
  - Oder *https://datenschutz-generator.de*
- In einem guten Generator sollten Sie die meisten typischen Website-Erweiterungen (wie Google Adwords, Facebook-Plugins …) auswählen können. Dann wird automatisch ein Text mit Hinweisen für die Datenschutzerklärung erstellt.

➤ **Datenschutzerklärung veröffentlichen**

- Veröffentlichen Sie Ihre Datenschutzerklärung **als eigene Seite** (nicht unter dem Impressum oder den AGB). Außerdem sollte man von jeder Seite aus Zugriff auf die Datenschutzerklärung haben
- Der **Link** zur Datenschutzerklärung kann z. B. so aussehen: „www.ihrewebsite.de/datenschutz“
- **Tipp**: Weisen Sie in Ihren Dokumenten (z. B. Auftragsformulare und Einwilligungserklärungen) sowie in Ihren E-Mails (als Signatur) mit einem Link auf Ihre Datenschutzerklärung hin.

Schritt 2: Cookie-Hinweis einbauen

Cookies sind kleine Textdateien, die auf Ihrem PC gespeichert werden, wenn Sie Websites besuchen. Beispiel: Sie bleiben eingeloggt, solange der „Login-Cookie“ gespeichert wird. Ein anderes Beispiel ist der „Analyse-Cookie“, die Webanalyse-Tools (wie Google Analytics) verwenden, um Auswertungen über die Website zu erstellen. Rechtlich ist es notwendig **Ihre Website-Besucher auf die Nutzung von Cookies hinzuweisen** (Informationspflicht).[1]

Ihre Aufgabe:

➤ **Cookie-Hinweis erstellen und auf Ihrer Website integrieren**

- Hinweis auf die Verwendung von Cookies
  (z. B.: „*Um unsere Webseite für Sie optimal zu gestalten und fortlaufend verbessern zu können, verwenden wir Cookies. Durch die weitere Nutzung der Webseite stimmen Sie der Verwendung von Cookies zu.*“)
- Verlinkung auf die Datenschutzerklärung
  (z. B.: „*Weitere Informationen: Datenschutzerklärung*“)

[1] Vgl. https://www.e-recht24.de/artikel/datenschutz/8451-hinweispflicht-fuer-cookies.html

Schritt 3: Website verschlüsseln

Die meisten Browser sowie Google stufen **unverschlüsselte Websites** (erkennbar am „http“ in der URL) inzwischen als „unsicher“ ein. Die Folgen: Unverschlüsselte Websites werden **in Google nach hinten gereiht**. Besucher misstrauen Ihrem Unternehmen, weil Ihre unsichere Website **nicht vertrauenswürdig** wirkt.[2]

Wenn Sie außerdem ein **Formular** auf Ihrer Website haben (z. B. Kontaktformular oder Bestellmöglichkeit), in dem Personen ihre Daten eingeben können, ist eine SSL-Verschlüsselung (erkennbar am „https“ in der URL) dringend zu empfehlen. Denn nur so können Sie sicherstellen, dass Sie die Personen-Daten gemäß der DSGVO schützen.[3]

Ihre Aufgaben:

- **Bei Ihrem Webhoster ein SSL-Zertifikat bestellen**
- **Ihre Website auf „https“ umstellen lassen**:
  Dies kann Ihr Webmaster machen (Wir würden empfehlen, dass dies ein Website-Spezialist macht, da die Website nicht mehr aufrufbar sein kann, wenn man einen Fehler macht).

Schritt 4: Facebook, Google & Co. „sicher“ einsetzen

Nutzen Sie auf Ihrer Website **Webanalyse-Tools** (Google Analytics, Mouseflow etc.) oder **Social-Media-Integrationen** (Facebook, Youtube usw.)? Wenn ja, dann müssen Sie bestimmte Maßnahmen setzen – denn sonst ist das Risiko groß, dass Sie abgemahnt werden.

Da *Facebook* und *Google Analytics* sehr häufig eingesetzte Website-Erweiterungen sind, zeigen wir Ihnen, welche Schritte Sie umsetzen sollten, wenn Sie diese nutzen:

Ihre Aufgaben, wenn Sie Google Analytics einsetzen:

- **Neue DSGVO-gerechte Nutzungsbedingungen von Google Analytics akzeptieren** und dort die erforderlichen Daten eingeben (wie z. B. Speicherdauer, Kontaktdaten)
- **Google Pixel anonymisieren** (nicht mehr die volle IP-Adresse des Besuchers speichern)
- **In der Datenschutzerklärung auf die Nutzung von Google Analytics hinweisen:**
  Verwenden Sie hierzu ein Muster oder den Text aus einem Datenschutzerklärungs-Generator.

[2] Vgl. https://www.heise.de/newsticker/meldung/Chrome-markiert-bald-alle-HTTP-Webseiten-als-unsicher-3963924.html, Feb. 2018.

[3] Vgl. https://www.datenschutzbeauftragter-info.de/dsgvo-muessen-kontaktformulare-jetzt-verschluesselt-werden/, Stand: April 2018.

Ihre Aufgaben, wenn Sie Facebook in Ihrer Website integriert haben:

- Neue DSGVO-gerechte Nutzungsbedingungen von Facebook akzeptieren
- In der Datenschutzerklärung auf die Nutzung von Facebook hinweisen: Verwenden Sie hierzu ein Muster oder den Text aus einem Datenschutzerklärungs-Generator.

Weitere Empfehlungen:

- Abmeldemöglichkeit auf der Website einbauen (Widerspruch der Nutzer gegen die Verwendung von Cookies und die Weitergabe von Daten an Google, Facebook usw.). Um Ihren Website-Besuchern einen Widerspruch zu ermöglichen, haben Sie drei Möglichkeiten:
  - *a) Minimal-Lösung:* Hinweise in Datenschutzerklärung
    Mit der Datenschutzerklärung sollten Sie bereits Anleitungen eingebaut haben, wie Nutzer gegen die Datenerfassung widersprechen können. Dies ist allerdings laut der Ansicht vieler Juristen und Experten nicht ausreichend.
  - *b) Praktisch empfohlene Lösung*: Opt-Out
    Deutlich besser wäre es, wenn Sie den Nutzern ermöglichen, diesen Widerspruch mit nur 1 Klick zu ermöglichen (durch ein „Opt-Out“)
    Tipp: Wenn Sie Wordpress nutzen, können Sie dafür ein Plugin einsetzen (z. B. *https://soulsites.de/facebook-pixel-plugin-wordpress-opt-out-dsgvo/*)
  - *c) Sicherste Lösung*: Opt-In
    Am sichersten wäre es aus Datenschutz-Sicht, wenn Daten von Website-Besuchern nur erfasst werden, wenn sie ausdrücklich zustimmen (durch ein „Opt-in“). Doch diese Lösung würde jegliche Webanalyse ziemlich nutzlos machen, weil das die Auswertungen extrem verfälschen würde – weshalb wir diese Lösung kritisch sehen.
- Alte Daten löschen in Bezug auf Google Analytics, Facebook & Co.
  Aus Datenschutz-Sicht wäre optimal, die alte Datenbank zu löschen (z. B. Google Analytics Daten löschen, wenn Sie vorher keine Anonymisierung eingesetzt hatten). Wir würden dies jedoch nicht als wichtigste Maßnahme sehen, solange Sie sich mit 25. Mai 2018 an die strengeren Vorgaben halten.
- Auf unnötige Webanalyse-Tools und Social-Plugins verzichten:
  Der sicherste Weg ist aus Datenschutz-Sicht immer noch der Verzicht auf solche Website-Tools, die Daten Ihrer Website-Besucher verwenden. Überlegen Sie sich also, welche Tools Sie wirklich benötigen und treffen Sie eine Entscheidung, wie viel Risiko Sie auf sich nehmen wollen. Doch denken Sie daran: 100%ige Sicherheit gibt es nicht.

Schritt 5: Einwilligungen für den E-Mail Versand sicherstellen

Versenden Sie Newsletter oder andere automatische E-Mails? Wenn ja, dann müssen Sie einige Vorkehrungen treffen. [4]

Ihre Aufgaben:

- **Austragen-Möglichkeit bei jedem E-Mail:** (jederzeitiger Widerruf)
  Die E-Mail-Empfänger sollen bei jedem E-Mail die Möglichkeit haben, sich einfach aus dem Newsletter auszutragen und keine weiteren E-Mails mehr zu erhalten. Daher sollten Sie am Ende jedes E-Mails einen Austragen-Link einfügen.

- **Link auf Datenschutzerklärung beim Anmeldeformular einbauen:**
  Es ist zu beachten, dass Sie direkt beim Formular auf Ihre Datenschutzerklärung hinweisen

- **Auf unnötige Pflichtangaben verzichten:**
  Um die DSGVO-Grundregel der Datenminimierung zu erfüllen, sollten Sie nur so viele Daten erheben (zumindest als Pflichtfeld), wie Sie benötigen. Freiwillige Zusatzangaben sind unproblematisch.

- **Auftragsverarbeitungs-Vertrag mit Ihrem E-Mail-Marketing Anbieter abschließen:**
  Fragen Sie bei Ihrem E-Mail Marketing Anbieter nach, ob er Ihnen einen Mustertext für Ihre Datenschutzerklärung bereitstellt und weisen Sie in Ihrer Datenschutzerklärung auf Ihren E-Mail-Marketing-Anbieter hin *(Details zur Auftragsverarbeitung – siehe Schritt 3)*.

- **Kopplungsverbot beachten und transparent aufklären**:
  Laut DSGVO gibt es eine Zweckbindung mit einem Kopplungsverbot. Das bedeutet, dass Sie Personen-Daten nur für einen bestimmten Zweck (und für keine anderen Zwecke) verwenden dürfen. Daher ist es wichtig, dass Sie bereits beim Formular die Person aufklären, für welche Zwecke Sie ihre Daten verwenden und sie kontaktieren usw.

[4] In Anlehnung an Solmecke/Kocatepe: Recht im Online-Marketing, 2. Auflage, 2018, S. 63-118.

Weitere Empfehlungen:

- **Regelmäßig E-Mails versenden:**
  Wenn Sie Ihre E-Mail Kontakte für eine längere Zeit nicht kontaktieren, ist davon auszugehen, dass die Einwilligung ungültig wird. Daher ist zu empfehlen, dass Sie regelmäßig E-Mails versenden (mind. vierteljährlich). Vor allem sollten Sie nicht zu lange warten, bis Sie Ihre neuen Kontakte das erste Mal kontaktieren.

- **Ausdrückliche Einwilligung sicherstellen:** („Double-Opt-In“)
  Das „Double Opt-In Verfahren“ ist die rechtssicherste Lösung für den Versand von Newslettern. Dabei muss die Person ihre Anmeldung durch einen Klick in einer „Willkommens-Mail“ bestätigen. Damit stellen Sie sicher, dass die Person, die sich einträgt, auch tatsächlich diejenige ist. Dieses „Double Opt-In“ sollte jeder seriöse E-Mail-Marketing Anbieter DSGVO-konform erfüllen. Sie können das Double-Opt-In Verfahren in der Regel in den Einstellungen aktivieren und relativ einfach einrichten. Durch dieses Verfahren können Sie die ausdrückliche Einwilligung sicherstellen – wie es die DSGVO verlangt.

- **Sollten Sie keine ausdrückliche Einwilligung** (per „Double Opt-in“**) haben**, prüfen Sie, ob Sie ALLE folgenden 4 Voraussetzungen erfüllen *(Spätestens bei neuen Kontakten, die sich nach dem 25. Mai 2018 eintragen)* :[5]

  1. **Bestellung**: Die E-Mail-Adresse des Kunden wird bei einer Bestellung erhoben (z. B. Verkauf einer Ware oder einer Dienstleistung).

  2. **Zusammenhang**: Die E-Mail Zusendung erfolgt (zur Direktwerbung) für eigene, ähnliche Produkte (oder Informationen in diesem Zusammenhang).

  3. **Jederzeitiger Widerspruch**: Der Kunde wird bei Erhebung der E-Mail-Adresse und bei jeder Zusendung klar und deutlich darauf hingewiesen, die Verwendung jederzeit kostenfrei und problemlos abzulehnen.

  4. **Nicht widersprochen**: Der Kunde hat der Verwendung nicht widersprochen.

[5] Vgl. https://www.it-recht-kanzlei.de/newsletter-datenschutzgrundverordnung-dsgvo.html, Stand: 28.08.2017: *„In § 7 Abs. 3 UWG wird jedoch eine Ausnahme vom Einwilligungserfordernis des Adressaten in die Zusendung elektronischer Post gemacht. Danach soll es dem Händler im Rahmen bestehender Kundenbeziehungen möglich sein, für den Absatz ähnlicher Waren und Dienstleistungen per E-Mail zu werben, ohne die Einwilligung des Kunden eingeholt zu haben. Hintergrund dieser Regelung ist, dass der Durchschnittskunde die Werbung eines Händlers für ähnliche Produkte in der Regel nicht als Belästigung auffasst.“*;
https://www.gesetze-im-internet.de/uwg_2004/__7.html: *„(3) Abweichend von Absatz 2 Nummer 3 ist eine unzumutbare Belästigung bei einer Werbung unter Verwendung elektronischer Post nicht anzunehmen, wenn 1. ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat, 2. der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet, 3. der Kunde der Verwendung nicht widersprochen hat und 4. der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.“*

Tipps, wie Sie mit bestehenden E-Mail Kontakten umgehen können

Was machen Sie nun mit Ihren **bestehenden Newsletter-Empfängern**? Hier gibt es keine eindeutige Antwort – denn selbst Juristen sind sich bei dieser Frage uneinig.

Teilweise ist man der Meinung, dass neue Einwilligungen für alle alten Kontakte einzuholen sind. Dies ist jedoch aus Marketing-Sicht eine Katastrophe, weil so in der Regel ein Großteil der Newsletter-Kontakte verloren geht.[6]

Als praktische Lösung sollte es unproblematisch sein, **bestehende Kontakte** einfach zu behalten,

- wenn Sie damals eine **gültige Einwilligung** erhalten haben oder
- wenn Sie eine **bestehende Geschäftsbeziehung** haben (z. B. Kunden) – hier können Sie „berechtigtes Interesse“ als Rechtsgrundlage angeben (im Verarbeitungsverzeichnis).[7]

Wichtig ist dabei jedoch, dass Sie alle **neuen E-Mail Kontakte** (die sich nach dem 25. Mai 2018 eintragen bzw. eingetragen haben) alle strengeren Voraussetzungen der DSGVO erfüllen (wie oben bei Ihren Aufgaben und den Empfehlungen genannt).

Außerdem ist es notwendig, dass Sie (alte) **Daten löschen**, die Sie nicht mehr (für einen bestimmten Zweck laut Verarbeitungsverzeichnis) benötigen.

[6] Kontakte, die den Newsletter zwar lesen, aber nicht bereits sind, Links darin anzuklicken, würden verloren gehen. Dieser Anteil kann in der Praxis weit mehr als die Hälfte (!) aller Kontakte ausmachen.

[7] Vgl. https://www.ipcl-rieck.com/news/3640.html, Stand: Jan. 2018. “*Beispiele für berechtigtes Interesse: In den Erwägungsgründen (Nr. 47 zu Art. 6 DSGVO) wird beispielsweise aufgeführt, dass eine **Vertragsbeziehung** ein solches berechtigtes Interesse begründen kann. Auch eine dienstliche Abhängigkeit kann zu einem berechtigten Interesse führen. Wichtig ist, dass der **Betroffene** zum Zeitpunkt der Erhebung der personenbezogenen Daten vernünftigerweise **abschätzen konnte**, dass seine Daten für die jeweiligen Zwecke des Unternehmers verarbeitet werden würden. […] dürfte auch mit der DSGVO das Versenden eines Newsletters im Rahmen **bestehender Kundenbeziehungen** auch ohne Einwilligung möglich bleiben. Auch hier gilt aber ausdrücklich, dass der Betroffene jederzeit widersprechen kann und hiervon auch durch den Unternehmer in Kenntnis gesetzt werden muss. Dies kann, wie bereits üblich, am Ende der jeweiligen Email, bestenfalls mit einem diesbezüglichen Link, erfolgen.“*

Impressum

DI Rico Kogleck (geprüfter Datenschutzexperte und Unternehmensberater)
Feldweg 29, A-9400 Wolfsberg
E-Mail: rico@digitalerfolgreich.com

Im Auftrag des VDN – Verband Deutscher Naturparke e.V.
Holbeinstr. 12, D-53175 Bonn
E-Mail: info@naturparke.de

Hinweis

Dieses Dokument basiert auf den Erfahrungen beim
Verband der Naturparke Österreichs (VNÖ) und wurde auf die deutschen Naturparke angepasst.

Disclaimer