conzeptwerk

Das Schreckgespenst Datenschutzgrundverordnung (DSGVO)

Grundlagen der datenschutzkonformen Onlinekommunikation

Mit unseren Checklisten sind Sie auf der sicheren Seite:

- Datenschutzerklärung und Impressum
- Cookies
- Kontaktformular und SSL-Zertifikat
- Google Analytics/Trackingsoftware
- Auftragsverarbeitung und externe Dienstleister
- Facebook & Co.

eRecht24 AGENTUR PARTNER für rechtssichere Webseiten

TÜV SÜD

qualifiziert & zertifiziert

Datenschutzerklärung und Impressum

Jede Webseite benötigt eine DSGVO-konforme Datenschutzerklärung, bei der zwingend folgende Grundsätze Anwendung finden müssen:

- auf einfache und verständliche Sprache achten
- Nennung der Kontaktdaten des Seitenbetreibers
- falls vorhanden, Nennung des Datenschutzbeauftragten
- konkrete Nennung der jeweiligen Rechtsgrundlage zur Datenerhebung/ Verarbeitung (gesetzliche Regelung mit genauem Artikel oder Einwilligung durch den Kunden)
- Nennung aller Datenverarbeitungsvorgänge auf der Webseite
- Umgang mit Kunden- / Bestelldaten
- Tracking, Cookies, Social Media
- Newsletter, AV (z.B. mit Host)
- Dauer der Speicherung der personenbezogenen Daten, Löschungsfristen
- Betroffenenrechte wie: Auskunft, Berichtigung, Löschung, Widerspruch
- Recht auf Datenherausgabe und Übertragbarkeit

Eine **Einwilligung zur Verarbeitung der personenbezogenen Daten** darf **NICHT innerhalb der Datenschutzerklärung** gegeben werden und muss klar davon abgegrenzt sein!

Achtung! Löschpflicht Art. 17 DSGVO

Sie sind verpflichtet personenbezogene Daten zu löschen, wenn:

- der Erhebungszweck weggefallen ist
- die Einwilligung widerrufen wurde (Newsletter-Abmeldung)
- ein Widerspruch des Nutzers erfolgt („Löschen Sie meine Daten“) und keine gesetzlichen Speicherpflichten entgegenstehen (Steuern und Buchhaltung)

Wenn Ihr **Impressum** bisher rechtlich gesehen vollständig war, müssen Sie hier **keine weiteren Änderunge**n durchführen.

Cookies

Im Wesentlichen dienen Cookies dazu, um die Benutzerfreundlichkeit einer Website zur steigern. Besucht ein Benutzer erneut eine Website, sorgen Cookies dafür, diesen wiederzuerkennen und erleichtern die Handhabung der Website, indem Zugangsdaten hinterlegt werden und nicht nochmals eingegeben werden müssen oder es wird erkannt, dass der Benutzer bestimmte Produkte bereits angesehen oder gekauft hat. Diese Technik findet bei fast allen Websites Anwendung.

Der rechtliche Rahmen hierzu wird auf EU-Ebene geregelt, muss indes durch deutsches Recht umgesetzt werden, was bisher jedoch noch nicht erfolgte.

Das deutsche Recht kennt aktuell trotz der EU-Cookie-Richtlinie somit keine direkte Pflicht, die Nutzer in die Verwendung von Cookies einwilligen zu lassen.
Da die deutschen Regeln keine konkrete Einwilligung („Ja, ich stimme zu“), sondern nur einen Hinweis auf das Widerspruchsrecht vorsehen, bleibt trotz alledem ein gewisses Rest-Risiko, sollten Sie keinen Cookie-Hinweis auf Ihrer Website anbieten.

Unsere Empfehlung ist also ganz klar:

Binden Sie die Cookie-Richtlinie auf Ihrer Website ein!

Kontaktformular und SSL-Verschlüsselung

Die DSGVO verlangt zum einen angemessene technische Maßnahmen zum Schutz personenbezogener Daten, was faktisch eine Verschlüsselungspflicht von Kontaktformularen bedeutet, zum anderen gibt es ein Urteil des OLG Köln, das vom Seitenbetreiber fordert, eine Einwilligung/ Checkbox der Nutzer innerhalb von Kontaktformularen einzuholen.

Somit ergibt sich Handlungsbedarf:

- Seiten mit Anfrage- und Kontaktformularen mittels SSL-Zertifikat verschlüsseln
- Nutzereinwilligung mittels Checkbox innerhalb der Kontaktformulare einholen

WICHTIG: Checkbox darf nicht vorausgewählt sein! Implementierung eines Pflichtfeldes nötig!

Einwilligung mit Checkbox **muss** enthalten:

a) Welche Daten werden erhoben

b) Wofür werden diese Daten erhoben/verarbeitet

c) Wie lange werden diese gespeichert bzw. wann gelöscht

d) Hinweis auf jederzeitiges Widerrufsrecht, Link zur Datenschutzerklärung

Formulierungs-Muster für Kontaktformular (Pflichtfeld zum Anhaken):

Ich stimme zu, dass meine Angaben aus dem Kontaktformular zur Beantwortung meiner Anfrage erhoben und verarbeitet werde. Die Daten werden nach abgeschlossener Bearbeitung Ihrer Anfrage gelöscht. Hinweis: Sie können Ihre Einwilligung jederzeit für die Zukunft per E-Mail an info@mustermail.de widerrufen. Detaillierte Informationen zum Umgang mit Nutzerdaten finden Sie in unserer **Datenschutzerklärung**. *(Link zur Datenschutzerklärung)*

Nicht nur das Kontaktformular braucht eine Verschlüsselung! **Alle Seiten, auf denen der Nutzer personenbezogene Daten eingibt**, sollten verschlüsselt sein.

Das betrifft vor allem:

- Seiten mit Bestellmasken und -eingabefeldern
- Downloadseiten, auf denen der Nutzer seine E-Mail-Adresse angibt
- Newsletter-Anmeldungen
- Seiten mit Login-Feldern
- Seiten, auf denen Zahlungsprozesse ablaufen

Google Analytics/Trackingsoftware

Für den datenschutzkonformen Einsatz von Google Analytics gibt es klare Regelungen, die mit den Aufsichtsbehörden abgestimmt sind. Auch hier gibt es durch die Datenschutz-Grundverordnung (DSGVO) einige Neuerungen zu beachten:

- Vertrag zur Auftragsverarbeitung abschließen
- Tracking-Code anpassen
- Aufbewahrungsdauer der Daten festlegen (bei Google Analytics)
- Datenschutzerklärung anpassen

Eine datenschutzkonforme Nutzung von Google Analytics ist nur mit der **Code-Erweiterung „anonymizeIp"** möglich. Der von Google vorgegebene Tracking-Code erfüllt nicht die nötigen Anforderungen zum Datenschutz, deshalb muss der jeweilige Google Analytics Tracking-Code händisch angepasst werden.
Durch Nutzung der Code-Erweiterung werden **die letzten 8 Bit der IP-Adressen gelöscht** und somit **anonymisiert**. Dadurch ist zwar weiterhin eine grobe Lokalisierung möglich, dies ist jedoch von den deutschen Datenschutzbehörden anerkannt und akzeptiert.

Weiterführende Informationen: *https://www.datenschutzbeauftragter-info.de*

Auftragsverarbeitung und externe Dienstleister

Viele Betreiber von Webseiten nutzen Dienste externer Anbieter, an die personenbezogene Nutzerdaten vom Seitenbetreiber übertragen werden. Beispiele hierfür sind etwa:

- externe Newsletter-Anbieter
- Ticket-Systeme
- Hoster
- Agenturen
- externe Callcenter
- externe Rechnungsbearbeitung/Buchhaltung

Auf der anderen Seite haben Agenturen und Webdesigner häufig auch Zugriff auf die Endkundendaten ihrer Kunden. Diese Daten dürfen eigentlich nur mit Zustimmung der jeweils betroffenen Personen an andere Unternehmen und Dienstleister übertragen werden.
Da dies praktisch aber oft kaum möglich ist, hilft die **Konstruktion der Auftrags(daten)verarbeitung (AV-Vertrag)**, um die Zustimmung jedes einzelnen Kunden zu umgehen.

Prüfen Sie als Seitenbetreiber, mit welchem externen Dienstleister Sie einen AV-Vertrag abschließen müssen. Fragen Sie im Zweifel bei dem jeweiligen Anbieter nach einem AV-Vertrag und schließen diesen mit dem Anbieter ab.
Bei **US-amerikanischen Anbietern** heißt das Dokument in der Regeln **„data processing agreement"**. Achten Sie zusätzlich darauf, dass der Anbieter Privacy-Shield-zertifiziert ist.
Dies können Sie unter folgendem Link prüfen: *https://www.privacyshield.gov/list*
Prüfen Sie als Webdesigner oder Agentur, ob Sie Zugriff auf personenbezogene Daten Ihrer Unternehmenskunden (etwa über Google Analytics), direkten Zugriff auf Kundenanfragen oder Bestellungen usw. haben.

Schließen Sie mit Ihren Kunden einen AV-Vertrag ab.

Als Seitenbetreiber sollten Sie mit den jeweiligen Dienstleistern einen AV-Vertrag nach DSGVO abschließen – als Agentur mit Ihren Kunden.

Facebook und Co.

Auf Facebook sind monatlich **über 2 Milliarden Nutzer aktiv***, da ergibt es sich von selbst, dass Facebook aufgrund der immensen Anzahl an Nutzern eine ideale Plattform ist, um das eigene Unternehmen zu präsentieren, Waren, Leistungen und Services anzubieten, mit den eigenen Kunden in Kontakt zu treten oder schnell auf Kundenanfragen oder Kritik zu reagieren.

Daher gibt es **einige Punkte**, die Sie unbedingt in Ihrem täglichen Umgang mit Facebook als Unternehmen **beachten müssen**:

- wettbewerbsrechtliche Vorgaben im Bereich Werbung und Marketing
- Datenschutzfragen bei der Kundenkommunikation
- Markenrechtsverletzungen
- die Frage der Haftung für Fanbeiträge auf der eigenen Facebook-Seite

Wenn **mehrere Mitarbeiter** über Ihre Unternehmensseite bei Facebook kommunizieren dürfen, stellen sich ebenfalls die Frage, wie Sie die Kommunikation regeln wollen. Dabei kann die Erstellung von **Social Media Guidelines** sinnvoll sein.

Beachten Sie jedoch:

Jede Social-Media-Plattform benötigt eine eigens dafür angepasste Datenschutzerklärung und ein eigenes Impressum.

**Quelle: https://de.newsroom.fb.com/company-info/*