Datenschutz Checkliste

LOY INTERNETAGENTUR

Datum: gültig **ab 28.05.2018**

Datenschutzgrundsätze für Ihre Website

Ab dem **25.05.2018** gilt die neue **Datenschutzgrundverordnung** – kurz DSGVO.
Diese neue europäische Verordnung soll dem **Schutz** natürlicher Personen bei der Verarbeitung ihrer **personenbezogenen Daten** dienen. Dabei soll das Recht auf personenbezogene Daten kein uneingeschränktes Recht darstellen, sondern es soll im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden.
Auch bislang verfolgte die Bundesrepublik Deutschland mit dem Bundesdatenschutzgesetz (BDSG) diesen Zweck, so dass die neuen Regelungen als Fortschreibung des bisherigen Rechts angesehen werden können.
Damit Sie auch in Zukunft Ihre Webseite **datenschutzkonform betreiben** und **hohe Bußgelder** der Landesdatenschutzämter **vermeiden**, möchten wir Sie nachfolgend auf die Basics hinweisen, die für den Betrieb einer jede Webseite gelten.

Jede Website sollte eine Datenschutzerklärung bereithalten

Platzierung der Datenschutzerklärung:

- Diese sollte getrennt vom Impressum gehalten werden.
- Sie sollte von jeder Seite und Unterseite aus erreichbar sein, also im Header oder Footer einer Website platziert sein und der Link sollte mit „Datenschutz“ o.ä. eindeutig bezeichnet sein.
- Die Datenschutzerklärung muss leicht verständlich sein und die Rechtsgrundlagen für die jeweilige Verarbeitungen benennen.

Was muss alles in die Datenschutzerklärung?

Inhalt der Datenschutzerklärung:

- Name und Kontaktdaten des für die Verarbeitung Verantwortlichen sowie des betrieblichen Datenschutzbeauftragten
- Angaben zur Erhebung und Speicherung personenbezogener Daten sowie Art und Zweck von deren Verwendung
  - Bei Besuch der Website
  - Bei Vertragsschlüssen über die Webseiten, Vorhalten von Kunden-/Mitgliedskonten
  - Bei der Anmeldung für einen Newsletter
  - Bei der Verwendung eines Kontaktformulars

  Wichtig ist hierbei, dass Sie genau angeben, **welche Daten** erhoben und gespeichert werden und zu welchem Zweck, sowie die **Löschfristen**!

- Angabe zur Verwendung von **Cookies**

- Angabe zur Verwendung von **Analysetools**, bspw. Google Anlaytics, Trackingtools usw. und Social Media Plugins wie bspw. Facebook, Twitter, Instagram usw.

- Angabe von **weiteren Diensten** wie bspw. Google Maps oder Google Fonts

- Angabe der entsprechenden **Rechtsgrundlage** für die Verarbeitung der Daten, wobei hier überwiegend die beiden nachfolgend genannten Regelungen in Betracht kommen:

    - Art. 6 Abs. 1 Satz 1 lit. a) = Einwilligung der betroffenen Person
    - Art. 6 Abs. 1 Satz 1 lit. b) = Verarbeitung ist für die Erfüllung eines Vertrages oder Durchführung einer vertraglichen Maßnahme erforderlich

- Information zur Weitergabe der Daten **an Dritte**

- Aufklärung über Rechte der Betroffenen

    - Auskunftsrecht
    - Berichtigung
    - Löschung
    - Einwilligung widerrufen
    - Widerspruchsrecht

Weitere Anforderungen nach der DSGVO

Weitere Anforderungen der DSGVO:

Wichtig ist auch, dass die **Einwilligung der Kunden** bspw. bei dem Bestellen eines Newsletters, dem Ausfüllen eines Kontaktformulars und/oder dem Erstellen eines Kundenkontos zur Verarbeitung der Daten **eingeholt wird**.

Diese Einwilligung ist in einer Datenbank zu dokumentieren. Immer, wenn Sie die Einwilligung des Kunden für eine Verarbeitung seiner Daten einholen, sollten Sie noch einmal auf Ihre **Datenschutzerklärung verlinken**.
Daneben sollten Sie aber darauf achten, dass Sie häufig mit Dritten, denen Sie personenbezogene Daten übermitteln bzw. die Zugriff auf die personenbezogenen Daten von Kunden haben, einen **Vertrag zur Auftragsverarbeitung** abschließen. Zudem sollten Sie darauf achten, wo Ihre Server gehostet sind.

Am Besten ist es, wenn Ihre bzw. die von Ihnen genutzten Server in Deutschland bzw. Europa stehen.

LOY
INTERNETAGENTUR

Bei einer Übertragung von Daten ins außereuropäische Ausland müssen Sie darauf achten, dass hier besondere Vereinbarungen notwendig sind.

Nachfolgend möchten wir Sie noch auf die **4 wichtigsten Schritte** nach der DSGVO hinweisen, die auch jedes Unternehmen treffen:

- **Betrieblicher Datenschutzbeauftragter**
  10 Personen-Regel: sind min. 10 Personen mit der Datenverarbeitung beschäftigt, muss ein Datenschutzbeauftragter bestellt werden.

- **Erstellen eines Verzeichnisses aller Verarbeitungstätigkeiten**
  Im Rahmen eines Verzeichnisses müssen alle Verarbeitungstätigkeiten aufgelistet werden, bspw. Kundenkarteien, Urlaubslisten, Personallisten, Buchhaltungssoftware, andere Software mit Datenbezug, E-Mail-Programme, Webseiten, Social-Media-Acounts, betriebliches Intranet usw.

- **Gap-Analyse**
  Im Rahmen dieser Analyse sollen die oben benannten Verzeichnisse geprüft und auf Schwachstellen untersucht werden. Zu den Schwachstellen zählen:

  - Datensparsamkeit
  - Datenrichtigkeit
  - Rechtmäßigkeit
  - Löschfristen
  - Zugriffsrechte
  - Zugangskontrolle
  - Schutz gegen Hacker und Malware

- **Datensicherheit**
  Technische und organisatorische Maßnahmen – kurz TOMS- müssen ergriffen werden, dies schreibt die DSGVO vor. Hierzu zählen folgende Maßnahmen:

  - Verschlüsselung
  - Stabilität
  - Wiederherstelllbarkeit
  - Regelmäßige Überprüfung