pagemachine

DSGVO Checkliste

So machen Sie sich und Ihre Website fit für die neue DSGVO!

Mit dieser Checkliste können Sie sich auf die neuen Regelungen der Datenschutz-Grundverordnung vorbereiten, die ab 25. Mai 2018 gilt.

Sie erfahren, wie Sie Einwilligungen DSGVO-konform erhalten, wie Sie mit den neuen Rechten Ihrer Website-Nutzer umgehen und wie Sie Ihre Datenverarbeitung in Zukunft dokumentieren müssen.

Natürlich helfen wir Ihnen gerne bei Fragen weiter und unterstützen Sie bei der Umsetzung der neuen Vorschriften.*

* Dieses Dokument stellt keine Rechtsberatung dar und soll und kann keine juristische Rechtsberatung ersetzen. Die Checkliste soll zur Orientierung und Hilfestellung zur neuen DSGVO dienen. Deshalb verstehen sich alle folgenden Informationen ohne Gewähr auf Richtigkeit und Vollständigkeit. Außerdem übernehmen wir aus rechtlichen Gründen keine Rechtsberatung.

Wer ist betroffen?

Alle Website-Betreiber, die personenbezogene Daten verarbeiten (dazu zählt zum Beispiel der Versand von Newslettern oder Warenverkauf), müssen sich ab dem 25. Mai diesen Jahres auf die DGSVO einstellen:

Strengere Dokumentationspflichten, neue Betroffenenrechte und **hohe Strafen** fordern unter anderem neue Prozesse und Dokumente.
Wir geben Ihnen eine erste Übersicht, was nun zu tun ist.

Wie erhalten Sie rechtskonforme Einwilligungen?

Ab Mai müssen Sie als Website-Betreiber einige Dinge beachten, um personenbezogene Daten verarbeiten, d.h. erheben, speichern und nutzen zu dürfen. Dafür benötigen Sie meist eine Einwilligung der Personen, deren Daten Sie verarbeiten möchten.
Oder Sie dürfen dank **Ausnahmen** auf die Einwilligung bei der Datenverarbeitung verzichten.

So erhält man DSGVO-konforme Einwilligungen:

- ❏ Widerrufsrecht direkt bei der Datenerhebung einbauen
  - bspw. direkt im Bestell- oder Anmeldeformular
  - Hinweis bzw. **Verlinkung auf die AGB ist nicht ausreichend**
- ❏ Zweck der Daten ist klar erkennbar oder muss genannt werden
- ❏ Einwilligungen müssen nachweisbar sein
  - Dokumentation vom Abschicken des Formulars bis beispielsweise zum Klick auf die Bestätigung nach Double-Opt-In (dies ist bei vielen Newslettertools z.B. schon der Fall)
- ❏ Einwilligungen dürfen **nicht abhängig von anderen Einwilligungen** sein
  - Kopplungsverbot (eine Registrierung darf z.B. nicht von einer Newsletteranmeldung abhängig sein)

Ausnahmen zur Datenverarbeitung, die keine Einwilligungen erfordern:

- ❏ Wenn Daten zur Vertragserfüllung erforderlich sind
  - bspw. die Adresse für den Versand eines gekauften Artikels
- ❏ Wenn Daten zur Erfüllung einer rechtlichen Pflicht erforderlich sind
  - bspw. die Umsatzsteuer ID für das Finanzamt
- ❏ Wenn Daten im Zuge einer vorvertraglichen Maßnahme erhoben werden
  - bspw. bei einer Kontaktanfrage durch einen interessierten Website-Besucher
- ❏ Wenn Daten aufgrund eines berechtigten Interesses erhoben werden
  - bspw. bei Direktwerbung

  Voraussetzungen für die Direktwerbung:
  - die betroffene Person ist Stammkunde bzw. die Daten wurden im Zuge eines Verkaufs erhoben **UND**
  - es werden eigene ähnliche Leistungen beworben **UND**
  - ein Widerrufshinweis ist in der Mail enthalten

Wie müssen Sie nun mit den neuen Betroffenenrechten umgehen?

Recht auf „Vergessen-Werden“

Wenn eine Person ab Mai bei Ihnen einen Antrag auf Löschung stellt, muss diese innerhalb von einem Monat durchgeführt sein.

Um das sicherstellen zu können, ist Folgendes zu tun:

- ❏ Klären Sie, welche Daten im Fall eines Antrags gelöscht werden dürfen und welche nicht.
  - bspw. aus steuerrechtlichen Gründen
- ❏ Klären Sie außerdem, wo und wie man diese Daten findet und vollständig löschen kann.
  - werden beispielsweise mehrere CRM Systeme genutzt?
- ❏ Erstellen Sie einen Prozess zur fristgerechten Löschung oder zur Benachrichtigung, falls die Löschung der Daten nicht möglich ist.
- ❏ Bestimmen Sie eine Person oder Personengruppe, die die Löschungen vornehmen dürfen und unterweisen Sie diese.

Empfehlung:

Stellen Sie ein Formular zur Verfügung, mit dem betroffene Personen einen Antrag auf Auskunft über ihre Daten oder auf Löschung dieser abschicken können (z.B. auf der Datenschutzseite). So gehen die Anträge im Idealfall nur an einer Stelle ein und können von den zuständigen Mitarbeitern bearbeitet werden.

Recht auf Übertragbarkeit der Daten

Sie müssen Personen, deren Daten Sie verarbeiten, ab Mai nicht nur Auskunft über ihre Daten geben, sondern diese auch zur Übertragung an Dritte zur Verfügung stellen.

Das ist dabei zu beachten:

- ❏ Klären Sie, welche Daten im Fall eines Antrags übermittelt werden dürfen und welche nicht.
  - bspw. aufgrund des Betriebsgeheimnisses oder selbst errechneter Daten
- ❏ Prüfen Sie vorab, wo und wie man diese Daten findet und in welchem Datei-Format man sie zur Verfügung stellt.
  - bisher gibt es hier kein festgelegtes Standard Format
- ❏ Erarbeiten Sie einen Prozess, um die Daten kostenfrei zur Verfügung stellen zu können.

Wie müssen Sie ab Mai 2018 Ihre Datenverarbeitung dokumentieren?

Prüfen Sie Ihre Datenschutzerklärung.

Die Datenschutzerklärung muss dem Besucher bei der Datenerhebung zugänglich sein und kann von jeder weiteren Seite der Website erreicht werden. Ein **Link im Footer** ist weiterhin in Ordnung.

Das muss sie enthalten:

- ❏ Ihr Name und Ihre Kontaktdaten als Verantwortlicher
  - ggf. auch die Kontaktdaten Ihres Vertreters und/oder des Datenschutzbeauftragten
- ❏ Die Zwecke für die personenbezogenen Datenverarbeitung für jedes Tool, das auf Ihrer Seite Daten verarbeitet, sowie die Rechtsgrundlage für die Verarbeitung bzw. die berechtigten Interessen, wenn die Verarbeitung auf diesen beruht
  - Welche Daten werden z.B. bei einer Registrierung oder Newsletteranmeldung erhoben und weshalb?
- ❏ Dauer, für die die personenbezogenen Daten gespeichert werden
  - falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
- ❏ Informieren Sie über die Rechte, die eine betroffene Person laut DSGVO hat:
  Recht des Nutzers auf:
  - Auskunft (DSGVO Art. 15)
  - Berichtigung (DSGVO Art. 16)
  - Löschung (DSGVO Art. 17)
  - Einschränkung der Verarbeitung (DSGVO Art. 18)
  - Datenübertragbarkeit (DSGVO Art. 20)
  - Widerrufsrecht (DSGVO Art. 21)
- ❏ Hinweis auf das Recht des Nutzers auf Widerruf seiner Einwilligung
- ❏ Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- ❏ Umstände der Bereitstellung der Daten – gesetzliche oder vertragliche Vorschriften, ob sie für einen Vertragsabschluss erforderlich sind und ob die betroffene Person verpflichtet ist, die Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte
- ❏ Bestehen einer automatisierten Entscheidungsfindung
  - bspw. wenn Entscheidungen getroffen werden aufgrund von einer durch Scoring bewertete Kreditwürdigkeit einer Person
  - ggf. die Empfänger oder Kategorien von Empfängern der Daten (bei Weitergabe)

- ggf. die Absicht, die personenbezogenen Daten an ein Drittland weiterzugeben, sowie die Rechtsgrundlage

Neu: Das Verfahrensverzeichnis ist Pflicht

Ab Mai 2018 ist ebenfalls ein Verfahrensverzeichnis/Verzeichnis von Verarbeitungstätigkeiten Pflicht. Sie müssen es auf Anfrage bei der zuständigen Aufsichtsbehörde vorlegen. Deshalb **darf es elektronisch geführt werden, muss aber druckbar sein**. Das heißt es sind z.B. keine Hyperlinks auf Dokumente zulässig.

Das muss das Verfahrensverzeichnis beinhalten:

- ❏ Name/Firma und Kontaktdaten der verantwortlichen Stelle (beziehungsweise auch gesetzlicher Vertreter oder Datenschutzbeauftragter etc.), Leiter der Datenverarbeitung etc.
- ❏ Die Zwecke der Datenverarbeitung
  - z.B. Verarbeitung der Kundenverwaltung für die Abwicklung von Verträgen
- ❏ Eine Beschreibung der betroffenen Personengruppen oder -kategorien und der auf sie bezogene Daten oder Datenkategorien
  - z.B. Personengruppe “Kunden” mit Daten wie Namen, Adressen etc., aber auch Mitarbeiter oder Bewerber und die dazugehörigen Daten etc.
- ❏ Kategorien von Empfängern, welchen die Daten mitgeteilt werden können
  - bspw. Dienstleister, wie ein externes Kontaktcenter, an die z.B. Adressen von Kunden übermittelt werden
- ❏ Die vorgesehene Frist für die Löschung der Datenkategorien
  - z.B. die Dauer der Speicherung von Bewerberdaten nach Ablehnung
  - ggf. geplante Datenübermittlung an Drittstaaten
- ❏ Eine Beschreibung der technischen und organisatorischen Maßnahmen (auch TOM)
  - z.B. IT-Sicherheitskonzepte, die grundlegend für alle folgenden Datenverarbeitungstätigkeiten gelten, oder auch Datenschutz-Zertifizierungen

Weitere Punkte, die Sie beachten sollten:

- ❏ Sind Sie gewappnet für einen **Datenschutzverstoß**? Erstellen Sie eines Prozesses, um die betroffenen Personen und die zuständigen Behörden innerhalb von 72 Stunden zu informieren
- ❏ Benötigen Sie nach dem DSGVO einen **Datenschutzbeauftragten**? Das BDSG (Artikel 4f) wird in diesem Punkt wahrscheinlich weiterhin greifen. Prüfen Sie deshalb nach dieser Regelung, ob Sie einen DSB benennen müssen.
- ❏ Haben Sie **Dritte mit der Datenverarbeitung beauftragt**, wie z.B. externe Cloud-Lösungen oder Kundencenter? Schließen Sie mit Ihren Partnern einen **Auftragsverarbeitungsvertrag** (Art. 28 DSGVO). Prüfen Sie Verträge mit Partnern, die nicht mit der Datenverarbeitung betraut sind, auf Datenschutz- und Haftungsklauseln.
- ❏ Kann Ihre **Datenverarbeitung** für die betroffenen Personen ein **Risiko** darstellen? Informieren Sie sich ob Sie Voraussetzungen laut Artikel 35 DSGVO für eine **Datenschutz-Folgeabschätzung** erfüllen – wenn ja, sind Sie verpflichtet, eine Abschätzung durchzuführen.

Sie benötigen Unterstützung bei der Erhebung von Einwilligungen oder bei der Umsetzung eines Verfahrensverzeichnisses?

Wir helfen Ihnen bei diesen und weiteren Themen rund um die neue DSGVO, um Ihren Usern weiterhin eine datenschutzkonforme Website bieten zu können.*

Senden Sie uns einfach eine E-Mail oder rufen Sie uns an:

+49 69 260 99 70 30

info@pagemachine.de

* Dieses Dokument stellt keine Rechtsberatung dar und soll und kann keine juristische Rechtsberatung ersetzen. Die Checkliste soll zur Orientierung und Hilfestellung zur neuen DSGVO dienen. Deshalb verstehen sich alle folgenden Informationen ohne Gewähr auf Richtigkeit und Vollständigkeit. Außerdem übernehmen wir aus rechtlichen Gründen keine Rechtsberatung.