Inhalt

WICHTIG:
Dieser Artikel stellt keine Rechtsberatung dar und kann auch keine Rechtsberatung ersetzen. Es wird keine Gewähr für die Richtigkeit, Vollständigkeit oder Aktualität der bereitgestellten Informationen übernommen.

Der Hintergrund:

Ab dem 25.05.2018 gilt die neue Datenschutzgrundverordnung der EU, kurz DSGVO
Sie betrifft alle, die personenbezogene Daten innerhalb der EU erheben.
Trotzdem gibt es auch wenige Wochen vor Inkrafttreten noch viel Unwissen und vor allem sehr viel Verwirrung bei den Betroffenen.
Dieser Artikel soll speziell kleinen Unternehmen und Solopreneuren konkrete Tipps und Handlungsempfehlungen geben. Dabei haben wir uns primär auf die Anforderungen im Bereich der Firmenwebseite konzentriert.

1. Worum geht es bei der DSGVO überhaupt?

Das Ziel ist ein besserer, umfassenderer Datenschutz: Denn personenbezogene Daten werden in großen Mengen und an vielen Stellen eingesammelt; nicht immer sinnvoll und nicht immer gut gegen Missbrauch geschützt.
Eine ganz durchschnittliche Firmenwebseite beispielsweise sammelt oft schon mittels Cookies oder Besucherstatistiken Daten und serverseitige Logfiles ein. Hinzu kommen Daten beispielsweise auch aus Kontaktformularen, Newsletter-Bestellungen, Onlinekäufen und vielem mehr. Auch „nur“ eine Email-Adresse oder sogar nur eine IP-Adresse gehört bereits zu den personenbezogenen Daten!

Das heißt: Jeder, der eine Webseite betreibt, sammelt personenbezogene Daten – deshalb hat der Betreiber die Pflicht, genau darzustellen, was mit den Daten passiert.
Also beispielsweise wo sie aufgenommen werden, für was sie genutzt werden und auch wie lange sie gespeichert werden.

Die EU-Verordnung soll – sehr verkürzt gesagt - dafür sorgen, dass weniger unnötige Daten gesammelt werden, dass die betroffenen Personen besser vorab informiert werden und dass sie der Erhebung ihrer Daten besser widersprechen können.

Der Grundsatzartikel auf https://blog.elopage.com/dsgvo-das-aendert-sich-fuer-online-unternehmer/ gibt einen sehr guten Überblick über die Hintergründe der DSGVO und die Bereiche, auf die Webseitenbetreiber achten müssen.

- **Tipp 1:** Lesen Sie den Artikel – dann sind Sie schon ganz gut im Bilde.
  Natürlich können Sie auch direkt hier nachlesen
  - Bundesbeauftragte für den Datenschutz:
    https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf?__blob=publicationFile&v=44
  - Haufe (generelle Infos)
    https://www.haufe.de/compliance/recht-politik/eu-datenschutz-grundverordnung-die-10-wichtigsten-regeln_230132_402196.html
  - Haufe (speziell für Webseitenbetreiber)
    https://www.haufe.de/compliance/recht-politik/auswirkung-der-datenschutzgrundverordnung-auf-website-pflichten_230132_440812.html
- **Tipp 2:** Prüfen Sie zunächst schnellstens, ob Sie vielleicht sowieso einen Datenschutzbeauftragen benötigen: Falls ja, kann dieser sie gleich bei allen weiteren Schritten begleiten.

2. Betroffene Bereiche (in Bezug auf die Webseite)

Wie oben schon erwähnt werden viele Daten automatisch gesammelt, ohne dass Sie als Webseitenbetreiber das mitbekommen. Durch das Setzen von Cookies und Plugins werden Daten gesammelt, ebenso durch Analysetools wie beispielsweise Google Analytics.
Andere Daten erheben Sie bewusst selbst, beispielsweise in (Kontakt-) Formularen oder auch für den Versand eines Newsletters.

Hier einmal einige Beispiele von Orten, an denen typischerweise auf der Webseite Daten erfasst werden (wobei die Liste nur ein kleiner Ausschnitt ist):

Durch Eingabe des Nutzers:

- Kontaktformulare
- Newsletter-Anmeldung
- Shop Bestellprozess
- Kommentare (z.B. im Blog)
- Benutzer-Registrierung /Kundenkonten

Im Hintergrund:

- Cookies
- Besucher-Statistiken
- Erfassung von Zugriffsdaten durch das CMS (Aufrufe, IP-Adresse…)
- Erfassung von Zugriffsdaten durch den Provider (Aufrufe, IP-Adresse…)

Widgets und Funktionen:

- Facebook Like-Button
- Facebook Posts eingebunden auf Webseite
- Google Maps eingebettet
- Soundcloud Player

Externe und sonstige Anbieter:

- Google Analytics
- Piwik Statistiken
- Google Adwords
- Facebook Pixel
- Wordpress JetPack

Die Einbettung bzw. Nutzung externer Dienste/Plugins soll durch die sogenannte e-Privacy-Verordnung genauer geregelt werden; diese ist allerdings noch nicht in Kraft.
Der Bundesverband Digitale Wirtschaft liefert dazu regelmäßig aktuelle News, siehe https://www.bvdw.org/themen/recht/eprivacy-verordnung/.
Auf https://www.blogmojo.de/dsgvo-checkliste/ gibt es eine Checkliste für typische Datensammelstellen bzw. auch für weitere mögliche Schwachstellen (Stichwort: SSL-Verschlüsselung).

Mithilfe von Ghostery bzw. Privacy Badger können Sie feststellen, welche Cookies/Services auf Ihrer Webseite laufen/erfasst werden – und ggf. Besucher verfolgen.

- Zusatztipp für JIMDO-Nutzer:
  Verfolgen Sie den Stand der Dinge, speziell in Bezug auf die notwendigen technischen Anpassungen auf https://jimdo-legal.zendesk.com/hc/de/articles/360000189886-DSGVO bzw. auch im Magazin https://de.jimdo.com/magazin/

- Zusatztipp für Wordpress-Nutzer:
  Interessante Infos haben wir hier gefunden:
  https://www.annetteschwindt.de/2018/03/24/umstellungen-wegen-der-dsgvo/ und

https://www.socialmedia-betreuung.de/dsgvo/.
Auch für nicht WP-Nutzer interessant, aber schon teilweise sehr speziell auf Wordpress-Plugins bezogen, die nützlich oder schädlich in Bezug auf die Umsetzung der DSGVO-Vorschriften sein könnten.

3. Generelle Anforderungen

Wir beziehen uns hier im Artikel primär auf den Bereich Webseiten und können deshalb nicht näher auf alle anderen Aspekte eingehen.

Trotzdem kommt an dieser Stelle noch einmal ausdrücklich der Hinweis, dass die Anforderungen aus der DSGVO sich nicht nur auf die Daten beziehen, die auf der Webseite erhoben werden – sondern es geht dabei um alle möglichen Bereiche, in denen Daten gesammelt und verarbeitet werden:
Hier ist also auch allgemein der Umgang mit beispielsweise Mitarbeiterdaten, Bewerberdaten, Kundendaten etc. gemeint. Alle diese Daten werden ja auch irgendwo erhoben, verarbeitet und eventuell auch an Dritte transferiert – beispielsweise an einen Dienstleister für Rechnungserstellung.

Auf der Seite des Bayerischen Landesamtes für Datenschutzaufsicht https://www.lda.bayern.de/de/kleine-unternehmen.html findet man einige Kurzbeispiele für die wesentlichen Anforderungen an kleine Unternehmen wie beispielsweise Handwerksbetriebe, Steuerberater und Ähnliches. Das Beispiel des Steuerberaters, siehe https://www.lda.bayern.de/media/muster_4_steuerberater.pdf ist vermutlich am typischsten dafür, was die meisten kleinen Unternehmen – hauptsächlich – beachten müssen.
Hier noch ein Beispiel für Onlineshops:
https://www.lda.bayern.de/media/muster_9_online-shop.pdf

4. Die Grundsätze zur Gewährleistung der DSGVO im Überblick

Der Hintergrund:
Grundsätzlich ist es verboten, personenbezogene Daten zu verarbeiten, siehe https://www.datenschutz.org/verbot-mit-erlaubnisvorbehalt/. Dieses Verbot wird ausgesetzt, falls man eine Erlaubnis dafür hat oder wenn es gesetzliche Regelungen für die Verarbeitung gibt (die richtig angewendet werden).

Die zentralen Prinzipien (siehe https://www.haufe.de/compliance/recht-politik/eu-dsgvo_230132_441242.html**)**

- Rechtmäßigkeit und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit von Daten
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

5. Was müssen bzw. können Sie jetzt tun

a. **Für SSL-Verschlüsselung der Webseite sorgen, falls nicht schon geschehen.**
Hinweis: Alle Jimdo-Webseiten sind standardmäßig SSL-verschlüsselt.

Erklärung: HTTPS steht für Hypertext Transfer Protocol Secure. Der Datenaustausch findet verschlüsselt über eine SSL-Verbindung statt. Die Identität einer Webseite wird durch ein entsprechendes Zertifikat ausgewiesen.
Achtung: Normalerweise sollte die Browserzeile für eine Webseite mit SSL-Verschlüsselung, also https://-Adresse so aussehen

Sollten Sie statt des grünen Schlüsselsymbols nur das graue mit Ausrufezeichen

sehen, dann gibt es nicht verschlüsselte Inhalte auf der Webseite. Diese sollten überprüft und entfernt werden.

Übrigens spielt die SSL-Verschlüsselung auch eine sehr große Rolle für die Suchmaschinenoptimierung einer Webseite, da Google nicht verschlüsselte Websites als unsicher einstuft.

b. **Datenschutzerklärung für die Webseite DSGVO-konform gestalten (lassen)**
Entweder idealerweise mit einem spezialisierten Rechtsanwalt oder als zweitbeste Lösung mit einem Datenschutzgenerator:

Beispielsweise von

a. https://www.e-recht24.de/muster-datenschutzerklaerung.html
b. https://dsgvo-muster-datenschutzerklaerung.dg-datenschutz.de/
c. https://datenschutz-generator.de/
d. https://www.mein-datenschutzbeauftragter.de/datenschutzerklaerung-konfigurator/

ACHTUNG: Unbedingt auch noch einmal das **Impressum** dahingehend überprüfen, ob es rechtssicher ist! Tipps finden Sie unter anderem hier: https://www.fuer-gruender.de/wissen/unternehmen-gruenden/unternehmensstart/aussenauftritt/website-impressum/

c. **Cookie-Hinweis auf der Webseite aktvieren**
ACHTUNG: Der Hinweis darf auf keinen Fall den Link zur Datenschutzerklärung oder den Link zum Impressum überdecken!

d. **Google Analytics – falls verwendet – rechtssicher einbinden**
Wenn Sie ein Google Analytics-Konto für Ihr Unternehmen eingerichtet haben, müssen Sie sich um diesen Punkt unbedingt kümmern!

(Übrigens: Für jedes Konto, d.h. jeden Google Account muss ein eigener Vertrag mit Google geschlossen werden. Wenn Sie mehrere Webseiten auf nur einem Account verwalten, reicht ein Vertrag)

Hinweis:
Falls Sie eine Jimdo-Webseite betreiben und die Seitenstatistiken dort aktiviert haben, dann trackt Ihre Webseite trotzdem die Besucher, auch wenn Sie keinen eigenen, persönlichen Analytics Account bei Google haben! Deshalb ist in der allgemeinen Datenschutzerklärung bei Jimdo auch ein Hinweis auf Analytics, der erst einmal gar nichts mit Ihrem evtl. auch vorhandenen persönlichen Konto zu tun hat.

Diesen sollten Sie unbedingt in der Datenschutzerklärung lassen, es sei denn, Sie schalten auch diese Jimdo-eigenen Seitenstatistiken ab.

Bitte lesen Sie zu Google Analytics auf jeden Fall den Beitrag von RA Dr. Schwenke https://drschwenke.de/google-analytics-datenschutz-muster-faq/

Drei Schritte sind unbedingt notwendig:

a. **IP-Anonymisierung**
b. **Vertrag mit Google zur Auftragsdatenverarbeitung abschließen**
   ACHTUNG: Falls Sie bereits einen Vertrag mit Google geschlossen haben, jedoch vor dem 23.09.2016, sollten Sie einen neuen abschließen!
   Alternative zum Papierversand zu Google nach Irland:
   Es ist jetzt auch möglich, die Vereinbarung mit Google online abzuschließen, siehe https://support.google.com/analytics/answer/3379636
   WICHTIG: Daten, die Sie vor Zustandekommen der Vereinbarung über die Datenverarbeitung erhoben haben, sind nicht datenschutzkonform erhoben. Dementsprechend wäre in einem solchen Fall die Neuerstellung des Google-Kontos der sicherste Weg.
c. **Datenschutzerklärung ergänzen**

e. **Aufträge mit Daten-Verarbeitern abschließen**

Je nach Art Ihres Unternehmens sind diverse Drittanbieter beteiligt, die von Ihnen Daten zur Verarbeitung weitergereicht bekommen.

Dazu gehören beispielsweise Ihre Email- und Webseiten-Provider, das Webseiten-CMS das Sie nutzen, ggf. CRM-Software, Newsletter-Dienste, Google-Dienste, Apps wie Billbee oder Dropbox (und auch z.B. DATEV), etc., etc.
Hinweis: Auch deshalb sollten Sie ein Verzeichnis von Verarbeitungstätigkeiten erstellen (siehe Punkt h)

All diese Firmen verarbeiten Daten, die Sie Ihnen durch die Nutzung dieser Dienste weitergereicht haben – und Sie sind dafür mitverantwortlich, ob mit diesen Daten dort datenschutzkonform umgegangen wird.

Damit Sie rechtlich abgesichert sind, sollten Sie unbedingt mit diesen genutzten Daten-Verarbeitern Verträge zur Auftragsdatenverarbeitung abschließen.
Eine gute Übersicht über den Stand der Dinge (wer bietet Verträge ab wann oder überhaupt) finden Sie hier: https://www.blogmojo.de/adv-vertraege/

f. **Alle kritischen Stellen auf der Webseite mit Einwilligungserklärungen nachrüsten**
Hier finden Sie Informationen zum Thema Einwilligung im Internet https://t3n.de/news/dsgvo-einwilligungen-843918/ und hier https://www.datenschutz.org/einwilligungserklaerung/ einige grundsätzliche Informationen zum Thema Einwilligung bzw. Einwilligungserklärung.

g. **Newsletter-Versand bzw. -Anmeldeprozess datenschutzkonform machen**
Kurz gesagt müssen Sie nachweisen können, dass alle Empfänger in Ihrem Email-Verteiler sich in einem Double-Opt-In-Verfahren für diesen Verteiler (freiwillig) angemeldet haben. Ausnahmen gibt es so gut wie keine.
Bitte lesen Sie dazu den Artikel von – mal wieder – Dr. Schwenke: Dieser bezieht sich zwar auch in Teilen auf Besonderheiten für die Nutzung von Mailchimp, aber er enthält auch die ganzen wichtigen allgemeinen Infos dazu:
https://drschwenke.de/mailchimp-newsletter-datenschutz-muster-checkliste/

h. **Verzeichnis von Verfahrenstätigkeiten erstellen**
Eigentlich würde dieses Verzeichnis an den Anfang aller Ihrer Aktivitäten gehören, denn es hilft Ihnen einerseits, sich selbst klarzumachen, welche Daten Sie überhaupt wie erheben und andererseits sind Sie auch dazu eigentlich datenschutzrechtlich verpflichtet. Mehr Infos dazu hier https://www.datenschutz-guru.de/verzeichnis-von-verarbeitungstaetigkeiten/.

Allerdings gehen wir davon aus, dass am 26.05. eher keine Behörde bei Ihnen vor der Tür stehen wird, um die Vorlage Ihrer Verfahrensverzeichnisse zu verlangen.
Wesentlich wahrscheinlicher ist es, dass ab dem 26.05. Abmahnvereine und Abmahnanwälte ausschwärmen werden, um leichte Beute zu machen:
Und das wird vermutlich am ehesten aufgrund von nicht datenschutz-konformen Datenschutzerklärungen auf der Webseite oder Erhebung von Daten ohne Einwilligung oder dem Versäumen von Informationspflichten passieren.

6. Was müssen Sie jetzt weiter beobachten

Bestimmte notwendige Maßnahmen können durch Webseitenbetreiber unter Umständen zurzeit noch gar nicht umgesetzt werden, weil einfach die (technischen) Voraussetzungen fehlen.
So bietet ja beispielsweise auch noch nicht jeder Daten-Verarbeiter einen entsprechenden Vertrag an, aber es gibt auch noch beispielsweise bei Jimdo diverse technische Faktoren, die erst einmal umgesetzt werden müssen, bevor der Webseitenbetreiber überhaupt seinen Pflichten nachkommen kann.

Zwar gäbe es zumindest teilweise auch individuell umsetzbare Lösungen, doch diese sind unter Umständen kompliziert und teuer – weshalb es häufig vermutlich sinnvoll ist, generelle Lösungen durch die Anbieter abzuwarten.

- **Weitergabe von Daten an externe Dienste über Plugins, Widgets etc.**
  Wer Plugins beispielsweise zu Facebook (Like-Button, Page Box, Posts eingebunden auf Webseite), Instagram (Feed), Youtube (eingebettete Videos) oder Twitter (Feed) auf seiner Webseite implementiert, macht diesen Netzwerken das Besuchertracking einfach. Falls User während des Besuchs der Website auch in ihrem jeweiligen Profil des sozialen Netzwerks eingeloggt sind, werden diese Informationen zusätzlich teilweise mit den persönlichen Daten aus den Profilen verknüpft.

  Deshalb wäre es hier besonders notwendig, Daten erst dann zu übermitteln, wenn der Nutzer ausdrücklich sein Einverständnis erteilt hat (Opt-In):
  Der Webseitenbetreiber kann zwar theoretisch selbst schon einmal eine solche Opt-In-Checkbox an der entsprechenden Stelle neben das Video oder neben den Like-Button einbauen … aber die technische Umsetzung fehlt dann erst einmal immer noch: Nämlich, dass die Datenübertragung unterbunden wird, wenn keine Einwilligung vorliegt.
  Dieses Problem besteht grundsätzlich erst einmal für alle Systeme, egal ob Wordpress, Jimdo, Drupal oder andere: Und der Webseitenbetreiber ist in der Pflicht, dafür zu sorgen, dass seine Webseite die Aktionen, die der Besucher nicht erlaubt hat, auch nicht ausführt.

- **Einsatz von Cookies:**
  In den meisten Fällen werden von Webseiten die unterschiedlichsten Cookies gesetzt (Was ist ein Cookie; https://support.mozilla.org/de/kb/cookies-informationen-websites-auf-ihrem-computer), um z.B. personenbezogene Daten zwischen zu speichern oder sich Benutzereinstellungen zu merken – aber auch beispielsweise um Besucherverhalten zu messen.
  Um es kurz zu sagen: Hier wird es dann wirklich kompliziert.

  Wer sich damit beschäftigen möchte, kann beispielsweise diesen Artikel lesen https://brands-consulting.eu/cookies-und-ds-gvo-welche-änderungen-die-datenschutz-grundverordnung-ds-gvo-zum-einsatz-von-cookies-bringt oder nach „Cookies E-Privacy DSGVO“ o.ä. googlen.
  Es dürfte für den normalen Webseitenbetreiber aber quasi unmöglich sein, den rechtlichen Anforderungen an seine Webseite in Bezug auf das Setzen von Cookies im Alleingang nachzukommen.

  Hier sollte es dringend generelle, datenschutzkonforme Einstellungen der jeweiligen CMS, beispielsweise Jimdo, geben. Das Problem dabei ist, dass hier juristisch noch große Unklarheit darüber herrscht, was eigentlich zu tun ist … und vielleicht auch nicht alles Wünschenswerte technisch ohne Weiteres umgesetzt werden kann.

- **Google Adwords Re-Marketing und Facebook Pixel**
  Hier ist die rechtliche Lage noch so unsicher, dass man eigentlich zurzeit nur von der Nutzung dieser Dienste abraten kann.

- **Laden von weiteren Daten, Diensten, Scripts**
  Es gibt noch eine Menge Dinge mehr, die auf Webseiten automatisch geladen werden und für die – theoretisch – jeweils Einwilligungen der Besucher abgefragt werden müssten, beispielsweise die Google-Schriften (Google WebFonts), falls sie direkt von Google hineingeladen werden.
  In Bezug auf die Google WebFonts scheint es bei Jimdo demnächst eine generelle Lösung zu geben.

7. Fazit

Diese Informationssammlung ist alles andere als vollständig; beispielsweise auf die Themen Speicherdauer, Kopplungsverbot, weitere Besonderheiten für Online-Shops und noch Einiges mehr sowie auf generelle unternehmensinterne Datensicherheit (Server, Virenscanner, Passwortverwendung, Kundenverwaltung, Rechnungserstellung etc.) konnten wir hier gar nicht eingehen.

Im ersten Schritt ist es vermutlich am wichtigsten, sich vor möglichen Abmahnungen aufgrund von – offensichtlich – nicht datenschutzkonformen Website-Einstellungen zu schützen.
Für die entsprechenden Maßnahmen konnten wir Ihnen hoffentlich mit unserer Info-Sammlung ein paar konkrete Hinweise geben.

Viel Erfolg!

Stefanie Engel, webhonesty.de
Tobias Groß, hn-worx.de