DSGVO Checkliste

Disclaimer:

Ich bin kein Rechtsanwalt und das ist keine Rechtsberatung. Diese muss individuell beim entsprechenden Anwalt durchgeführt werden.

Diese Liste soll dir helfen einen Überblick über die verschiedenen ToDos zu behalten, damit du deine Seite möglichst konform nach den Richtlinien der Datenschutzgrundverordnung (DSGVO) erstellen, bzw. konfigurieren kannst. DSGVO ist ab 25.05.2018 vollständig wirksam.

DSGVO und Hosting

Hast du mit deinem Webhosting-Anbieter(n) einen Vertrag zur Auftragsdatenverarbeitung (ADV) abgeschlossen?	
Benutzt deine Seite einen Content Delivery Network (CDN)?	
Wenn ja, steht der Server in der EU?	
Wenn ja, hast du mit diesem Anbieter einen ADV geschlossen? (Falls die Daten nicht auf dem Webserver gespeichert werden, worauf deine Seite läuft)	
Wenn nein, erfüllt der Anbieter die Richtlinien der DSGVO und EU-US Privacy Shield? (Bestätigung geben lassen) (Siehe hierzu Kapitel 5, Art. 44 DSGVO)	

Verschlüsselung

Hast du auf deiner Webseite ein SSL Zertifikat installiert?	
Ist das SSL Zertifikat gültig?	
Hast du Maßnahmen gegen unbefugten Zugriff durch Hacker oder Dritte ergriffen? (sichere Dateirechte, sichere Passwörter, regelmäßige Updates, ggf. .htpasswd)	

DSGVO Trackingtools

Hats du ein Tracking Tool im Einsatz (Piwik (Matomo), Analytics, Wordpress.com-Stats, Yandex (beachte hierbei folgendes))? Wenn ja, welches hast du im Einsatz?	
Hast du die IP Adressen anonymisiert? (Google Analytics, Piwik / Matomo)	
Falls Google Analytics, wäre es denkbar auf Piwik, bzw., Matomo zu wechseln? Mit eigenem Server?	
Liegen die Daten auf deinem Server? Oder beim Drittanbieter?	
Falls Drittanbieter, befindet sich dieser in der EU?	
Falls ja, befindet sich dieser in Deutschland?	
Hast du eine ADV mit diesem abgeschlossen?	
Wenn außerhalb der EU, hast du eine Möglichkeit, diesen zu wechseln?	
Falls nicht, erfüllt der Anbieter die Richtlinien der DSGVO und EU-US Privacy Shield? (Bestätigung geben lassen) (Siehe hierzu Kapitel 5, Art. 44 DSGVO)	
Kann der Benutzer anhand eines Klicks der Erfassung widersprechen? (Link sollte in der Datenschutzerklärung sein)	

Formulare

Sind auf deiner Webseite Formulare eingebunden, die personenbezogene Daten übertragen? (ohne HTTPS darfst du keine Formulare einbinden)	
Falls ja, hats du einen Hinweis, bzgl. der Nutzung der Daten platziert? (unten, oben, daneben, in Kurzform)	
Ist ein Verweis auf deine Datenschutzerklärung vorhanden?	

Newsletter in der Datenschutzgrundverordnung

Wird ein Newsletter Plugin oder Dienst verwendet?	
Ist sichergestellt, dass bei der Verwendung des Newsletter Plugins oder Dienstes und somit der Eintragung des Benutzers in den Newsletter nach den Double-Opt-In-Verfahren erfolgt? (Double-Opt-In = Eintragung im Newsletter und anschließende Bestätigung der E-Mail-Adresse per E-Mail).	
Ist ein Hinweis bzgl. der Verwendung der Daten gegeben?	
Sammelst du alle E-Mail-Adressen auf deiner Seite zusammen in einem Topf?	
Wenn ja, hast du den Benutzer darauf aufmerksam gemacht, dass er auch andere Informationen und womöglich auch Angebote erhalten kann, wenn er sich in den Newsletter einträgt?	
Wenn du ein Plugin nutzt: werden die Daten auf deinem Server gespeichert?	
Wenn du einen Dienstleister nutzt: befindet sich dieser in der EU?	
Falls ja, hast du einen ADV mit diesem geschlossen?	
Falls nein, erfüllt der Anbieter die Richtlinien der DSGVO und EU-US Privacy Shield? (Bestätigung geben lassen) (Siehe hierzu Kapitel 5, Art. 44 DSGVO)	

Plugins, Widgets, Rechner, iFrames, etc.

Hast du auf deiner Webseite Plugins, Widgets, iframes, Scripte oder weitere Schnittstellen in Verwendung?	
Werden dadurch personenbezogene Daten gespeichert?	
Wenn ja, bei dir auf dem Server?	
Oder bei einem Drittanbieter?	
Zu welchem Zweck werden die Daten gespeichert?	
Werden nur die Daten gespeichert, die benötigt werden oder möglicherweise auch zu viele Daten?	

Membership

Benutzt du Membership Funktionen oder Dienste?	
Werden die Daten auf deinem Server gespeichert?	
Falls ja, steht dieser Server in der EU?	
Hast du mit diesem Hosting Anbieter einen ADV geschlossen?	
Wenn der Server außerhalb der EU steht: erfüllt der Anbieter die Richtlinien der DSGVO und EU-US Privacy Shield? (Bestätigung geben lassen) (Siehe hierzu Kapitel 5, Art. 44 DSGVO)	

Hinweis: Bei Membership-, Newsletter-, Social-Media, Formular-Plugins werden immer persönliche Daten gesammelt. Dasselbe kann auch für Finanzrechner gelten oder anderweitige Rechner und Tools, wo Name, Adresse oder E-Mail-Adresse eingegeben werden müssen.

Am besten ist es, wenn du in der jeweiligen Dokumentation des Anbieters oder Plugins nachliest, was alles gesendet wird und wohin. Es haben hoffentlich die meisten schon über das Thema GDPR / DSGVO gehört und ihre Dienste und Dokumentationen entsprechend angepasst. Allerdings wirst du auch auf solche stoßen, die es noch nicht gehört haben. Hier hilft nur eines, du musst selbst herausfinden, welche Tools Daten sammeln und verschicken. Dabei kannst du folgende Methoden verwenden:

- Chrome Developer Tools öffnen (rechte Maustaste -> Untersuchen -> Reiter „Sources“ gehen)
- Cookies findest du bei Chrome auch, wenn du in der Adresszeile auf das „i“ bzw. auf das Schlüssel-Symbol, links neben der Domain klickst:

- Es erscheint ein Fenster und zeigt dir die Anzahl der Cookies auf, dort kannst du auf diese Schaltfläche klicken und erhältst weitere Informationen, indem du dich entlang hangelst
- Bei Firefox ebenfalls, wenn du in der Adresszeile auf das „i“ bzw. auf das Schlüssel-Symbol, links neben der Domain klickst:

- Dann öffnet sich ein Fenster, wo du auf den Pfeil nach rechts klicken musst und schließlich ganz unten auf „weitere Informationen“ und dort auf „cookies anzeigen“.
- Du kannst aber auch die Seite „builtwith.com“ nutzen
- Oder du verwendest Ghostery (Browser Plugin)

Online Shops

Online Shops können unterschiedlich aufgebaut sein und daher ist es nur schwer darauf einzugehen, da dies sehr komplex sein kann. Gerade bei Kreditkarten und anderen Daten hinsichtlich Finanzen ist es sehr kritisch. Grundlegend und einige Themen können dennoch aufgegriffen werden:

Nutzt du hier einen Shop selbst gehostet?	
Wenn nein, befindet sich der Dienstleister in der EU?	
Wenn ja, hast du mit ihm eine ADV abgeschlossen?	
Wenn außerhalb der EU: erfüllt der Anbieter die Richtlinien der DSGVO und EU-US Privacy Shield? (Bestätigung geben lassen) (Siehe hierzu Kapitel 5, Art. 44 DSGVO)	
Nutzt du externe Bezahldienste?	
Wenn ja, hast in deiner Datenschutzerklärung detailliert darauf hingewiesen, welche Daten gesammelt und wohin geschickt werden?	
Beachte auch hier wieder, ADV Vereinbarung mit deinem Bezahldienstleister.	
Wenn außerhalb der EU: erfüllt der Anbieter die Richtlinien der DSGVO und EU-US Privacy Shield? (Bestätigung geben lassen) (Siehe hierzu Kapitel 5, Art. 44 DSGVO)	
Wird ein Paket-Trackingsystem verwendet?	
Werden dafür E-Mail oder Telefonnummer verwendet?	

Hast du in deiner Datenschutzerklärung darauf hingewiesen?	
Wenn ja, hast du eine ADV mit diesem Dienstleister geschlossen?	
Wenn außerhalb der EU: erfüllt der Anbieter die Richtlinien der DSGVO und EU-US Privacy Shield? (Bestätigung geben lassen) (Siehe hierzu Kapitel 5, Art. 44 DSGVO)	
Muss sich der Benutzer registrieren damit er die Bestellung durchführen kann?	
Wenn ja, ist dies entsprechend gekennzeichnet?	
Ist dies auch entsprechend in der Datenschutzvereinbarung aufgelistet?	
Hast du ein sicheres Passwort (mind. 10-stellig, klein- / Großschreibung, Zahlen, Sonderzeichen) für den Zugang zum Shop backend?	
Hast du ein sicheres Passwort für die Datenbank?	
Sind alle weiteren Passwörter die für das Shopsystem verwendet werden ebenfalls sicher?	
Ist die Verbindung verschlüsselt? (ohne SSL kein Shop)	
Ist die IT um den Shop (Webserver, Webseite, Netzwerk, Datenbank, Schnittstellen, etc.) gut abgesichert? Hier ist es notwendig, dass das von einem IT-Experten gründlich untersucht wird.	
Führe all deine Schnittstellen und externe Dienstleister auf und prüfe, ob du eine ADV mit diesen geschlossen hast (bei Kunden- und Mitarbeiterdaten notwendig).	
Prüfe außerdem, ob sich alle Dienstleister, die mit Kundendaten (aber auch Mitarbeiterdaten) in Berührung kommen, in der EU sind, sonst musst du prüfen, ob der Dienstleister außerhalb der EU alle Richtlinien nach der DSGVO erfüllt.	

Marketing

Das Thema Marketing ist ebenfalls sehr komplex aufgebaut. Das hat unter anderem den Grund, weil du teilweise nicht weißt, welche Schnittstellen und Systeme noch an der Plattform angeschlossen sind und was evtl. dahinter geschieht. Wichtig für die eigene Seite ist daher, dass du prüfst, welche Schnittstellen und Marketinginstrumente und -software angeschlossen ist, sowie was diese tut. Ein paar Punkte:

Nutzt du Google Analytics oder ähnliches?	
Wenn ja, hast du dies in deiner Datenschutzerklärung aufgeführt?	
Nutzt du Doubleclick?	
Wenn ja, hast du dies in deiner Datenschutzerklärung aufgeführt?	
Nutzt du Google Adsense oder ähnliches?	
Wenn ja, hast du dies in deiner Datenschutzerklärung aufgeführt?	
Nutzt du den Facebook Pixel oder ähnliches?	
Wenn ja, hast du dies in deiner Datenschutzerklärung aufgeführt?	
Hast du eine Möglichkeit eingebaut, dass der Nutzer dem Tracking widersprechen kann?	
Grundsätzlich ist dieses Thema „Tracking und Marketing“ sehr heikel. Daher wäre es – auch wenn es sehr unschön ist – besser, wenn du eine Opt-Out-Methode einbaust. Damit kann der Benutzer dem Tracking widersprechen.	
Gerade bei den Remarketing / Retargeting Möglichkeiten ist es besser, wenn du eine Opt-In Methode einbaust, damit der Benutzer explizit zustimmen muss, dass er getrackt werden möchte. Ebenfalls, dass er auf den Facebook Like-Button klickt und dann seine Daten entsprechend verwendet werden.	

Social Media (Plugins)

Benutzt du Social Media Plugins?	
Hast du darauf in deiner Datenschutzerklärung hingewiesen?	
Wenn du die Social Media Plugins verwendest, ist es sichergestellt, dass keine personenbezogenen Daten übertragen werden, bevor der Nutzer widersprechen kann? (Gilt für die Standard sharing Buttons).	
Verwende lieber alternative Plugins, wie z. B. das Shariff Plugin (bei WordPress)	
Verwendest du das Affiliatetheme.io? Dann sind die Social Media Plugins bereits DSGVO konform (es sind nur Links) zu affiliatetheme.io.*	
Hast du auf deinen Social Media Seiten ein Impressum oder verlinkst du zumindest auf dein Impressum?	

Was ist ein Auftragsdatenverarbeitung Vertrag (ADV-Vertrag)?

Jetzt wurde das Wort „Auftragsdatenverarbeitung“ ADV schon einige Male verwendet. Vollständigkeitshalber würde ich das hier nochmal kurz erklären, was das ist. Wenn du die Dienste von Webhostern oder anderen Dienstleistern nutzt, dann verarbeiten diese die personenbezogenen Daten deiner Kunden. Damit die Sicherheit und der Schutz der Daten dieser Nutzer und Kunden durch den externen Auftragnehmer gewährleistet werden kann. Für diese Verarbeitung von Daten durch einen externen Auftragnehmer, wird ein sogenannter Vertrag zur Auftragsdatenverarbeitung (ADV-Vertrag) notwendig und geschlossen.

Wer benötigt einen Auftragsdatenverarbeitung Vertrag?

Jeder, der personenbezogene Daten verarbeitet. Das bedeutet also, wenn du einen Dienstleister oder einen Dienst von einem externen Anbieter nutzt oder die personenbezogenen Daten deiner Benutzer auf einem Server gespeichert werden, der nicht dir gehört, dann ist ein ADV-Vertrag notwendig. In vielen Unternehmen werden zahlreiche Daten verarbeitet und an externe Anbieter übergeben, teilweise ohne, dass man sich damit auseinandergesetzt hat oder dem bewusst ist. Daher ist es notwendig, dies Datenübermittlung zu überprüfen und hinterfragen, ob die Daten überhaupt in diesem Detailgrad an den externen Dienstleister und Partner übermittelt werden müssen.

In jedem Fall benötigt man hier einen ADV-Vertrag. Wichtig ist vor allem, dass es für alle Dienstleister und Partner in der EU gilt. Dienstleister außerhalb der EU müssen die Datenschutzbestimmungen nach der Datenschutzgrundverordnung (DSGVO) erfüllen, da die personenbezogenen Daten ansonsten dort nicht verarbeitet werden dürfen.

Eine super Übersicht über die verschiedenen Dienstleister und deren Beitrag zum ADV-Vertrag wurde auf blogmojo erstellt[1]. Dort siehst du, welche Hoster und Dienstleister bereits ADV-Verträge erstellt haben. Diese kannst du dann herunterladen, ausfüllen und an den Dienstleister versenden.

Was ist eine Datenschutzerklärung?

[1] Vgl. https://www.blogmojo.de/adv-vertraege/

Auch dieser Begriff taucht öfter in der Checkliste auf. Eine Datenschutzerklärung beschreibt die Maßnahmen, die jemand tritt, um die Privatsphäre der Kunden, Mitarbeiter oder Benutzer zu wahren. Besonders beachtenswert sind hier die personenbezogenen Daten. Eine Datenschutzerklärung zu erstellen ist neben dem Impressum Pflicht. Diese kannst du über einen Anwalt erstellen lassen, was sehr kostspielig wird oder du nutzt die kostenlosen oder kostenpflichtigen Generatoren im Internet hierfür.

Du kannst zum Beispiel die folgenden Generatoren nutzen:

- Datenschutz-Generator der DGD (Deutsche Gesellschaft für Datenschutz, kostenlos)
- Datenschutz-Generator von eRecht24 (Wobei der Premium Account zu empfehlen ist*, aufgrund weiterer Tools und einer erweiterter Datenschutzerklärung.)
- Datenschutz-Generator von Dr. Schwenke (kostenlos)

Was sind personenbezogene Daten?

Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG[2] definiert es als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Das heißt, dass personenbezogene Daten Informationen sind, die irgendeinen persönlichen Bezug zu einer Person herstellen können[3]. Darunter fallen unter anderen:

- Name und Anschrift
- E-Mail-Adresse
- Telefonnummer
- Kreditkarten- und Kontodaten
- Mitarbeiternummer
- Kundennummer
- Foto
- Personenbeschreibung
- KFZ-Kennzeichen

Darüber hinaus gibt es noch die „besonderen personenbezogenen Daten“, was mit medizinischen Informationen zur Person gleichzusetzen ist.

Was ist ein Verfahrensverzeichnis?

Das Verfahrensverzeichnis wurde in den letzten Wochen und Monaten ständig im Gespräch. Immer wurde gefragt, was das überhaupt ist und was dort überhaupt hineinmüsste. Aber keine Angst, es ist oft gar nicht so schlimm. Beim Verfahrensverzeichnis handelt es sich um eine Übersicht aller eingesetzten Verfahren und Prozesse, die mit personenbezogenen Daten in Berührung kommen und diese verarbeiten. Also egal ob es Kollegen oder Mitarbeiter sind, die mit diesen Daten in Kontakt kommen, für diese Prozesse und Verfahren wird ein Verfahrensverzeichnis benötigt.

---

[2] Vgl. https://www.gesetze-im-internet.de/bdsg_1990/__3.html
[3] Vgl. https://www.datenschutzbeauftragter-info.de/personenbezogene-daten-definition-und-praktische-beispiele/

Dabei muss man beachten, dass es nicht nur um Kundendaten handelt, sondern auch um Benutzer- und Mitarbeiterdaten. So ist eine Lohnabrechnung und Mitarbeiterverwaltung sowie Einzelverbindungsnachweis und E-Mail-Liste für den Newsletter entsprechend einzustufen und es wird ein Verfahrensverzeichnis benötigt.

Wer braucht ein Verfahrensverzeichnis?

Kurz gesagt: **JEDER**! Im Artikel 30 der DSGVO „Verzeichnis von Verarbeitungstätigkeiten" steht drin, dass erst ab 250 Mitarbeiter ein solches Verzeichnis benötigt wird. Allerdings steht im gleichen Absatz drin, dass dies nur gilt, wenn die Verarbeitung nicht nur gelegentlich erfolgt. Wenn du nun also mit den eingesammelten E-Mail-Adressen der Newsletter-Abonnenten hantierst und diesen E-Mails zuschickst, dann ist dies nicht mehr gelegentlich. Auch mit den Mitarbeiterdaten und Kundendaten wird nicht nur gelegentlich hantiert, sondern regelmäßig. Fraglich ist hier, was man unter gelegentlich versteht.

Was gehört in ein Verfahrensverzeichnis?

Im Artikel 30 der DSGVO „Verzeichnis von Verarbeitungstätigkeiten" wird aufgelistet was alles in das Verfahrensverzeichnis gehört. Die nachfolgenden Informationen müssen in das Verfahrensverzeichnis aufgenommen werden:

- Name des Datenschutzbeauftragen (falls benötigt)
- Name und Kontakt des Verantwortlichen des Verfahrens
- WARUM (Zweck) der Verarbeitung der Daten
- Wer ist davon betroffen? (Personengruppen)
- Welche Daten werden von den Betroffenen erhoben?
- Wer hat Zugriff auf diese Daten (intern, extern, außerhalb der EU)
- Wie findet die Übermittlung an das Drittland (außerhalb der EU) statt?
- Ist diese Übermittlung rechtlich abgesichert?
- Welche Löschfristen sind für diese Daten vorgesehen (falls welche vorgesehen sind)
- Allgemeine technische Beschreibung der Datensicherheit (falls möglich) (=TOM => Technische und organisatorische Maßnahmen)

Bitkom hat hier ein Beispiel, bzw. ein Muster inkl. Leitfaden bereitgestellt, dass kostenlos heruntergeladen und angepasst werden kann[4].

Auch eine sehr gute Übersicht bietet Frau Regina Stoiber, inkl. Erklärung und Muster zum Download[5].

Informationspflicht in der DSGVO

Vieles ist in der Datenschutzgrundverordnung bereits seit dem BDSG vorhanden und somit nicht neu. Allerdings ist die Informationspflicht diesmal neu. Mit der Informationspflicht musst du deine Benutzer

[4] Vgl. https://www.bitkom.org/Bitkom/Publikationen/Das-Verarbeitungsverzeichnis.html
[5] Vgl. https://regina-stoiber.com/2018/03/11/datenschutz-verfahrensverzeichnis-nach-artikel-30-dsgvo-mit-muster/

VOR der Verarbeitung der Daten informieren, was du mit diesen Daten machst, sofern du diese bei ihm direkt erhebst. Solltest du diese **NICHT direkt** vom Betroffenen erhalten, sondern über andere Wege, dann ist das auf jeden Fall anzuzeigen, sprich, du musst den Betroffenen innerhalb von 4 Wochen darüber informieren.

Bei Webseiten und Blogs wird diese Informationspflicht in der Regel durch die Datenschutzerklärung getan. Sofern du außerhalb deiner Webseite Daten von Benutzern erhebst und verarbeitest, musst du diesen darüber informieren. Verschiedene und neue Änderungen in der DSGVO gegenüber dem BDSG hat die Datenschützerin Regina Stoiber in ihrem Blogbeitrag niedergeschrieben[6].

Datenschutzgrundverordnung für Mittelstand & Enterprise Unternehmen

Für größere Unternehmen und damit über die Bloggergröße hinaus, geht es für die meisten Unternehmen noch weiter. Daher hatte man auch ausreichend Zeit (2 Jahre), sich mit diesem Thema auseinanderzusetzen und die entdeckten Maßnahmen umzusetzen. Wie bereits erwähnt, ist vieles gleich geblieben und es gibt nur ein paar neue Änderungen. Das meiste ist bereits seit TMD oder BDSG vorhanden und wurde dennoch teilweise nicht umgesetzt.

Für viele Unternehmen geht es also weiter und es gilt zu prüfen, was alles gemacht werden muss. Da die Systeme und Verfahren teilweise historisch gewachsen sind, gilt zu prüfen, was alles geändert werden muss und was überhaupt geändert werden kann. Manchmal müssen gar neue Systeme und Verfahren etabliert werden. Hier sind die Analyse und die Dokumentation das A und O. Wer bereits alles gut und strukturiert dokumentiert hat, dürfte bei der Analyse deutlich weniger große Anstrengungen unternehmen müssen.

[6] Vgl. https://regina-stoiber.com/2018/03/03/informationspflicht-dsgvo-bdsg-neu/