DSGVO:

CHECKLISTE

holzweg
strategie.design.technologie

EINLEITUNG

Die DSGVO (Verordnung (EU) 2016/679) trat bereits im Mai 2016 in Kraft mit einer 2-jährigen Übergangsfrist **(gültig ab dem 25.05.2018)** und löst damit die DSRL von 1995 ab. Wesentliche Eckpfeiler sind Stärkung der Betroffenenrechte mit neuem Fokus auf Datensicherheit.

WARUM DIESE CHECKLISTE?

holzweg möchte Sie fit für das Thema DSGVO und Website machen.
Die Checkliste soll Ihnen einen Überblick geben und Hintergrundwissen vermitteln.

Achtung: Wir haben diese Checkliste und Erklärungen nach ausgiebiger Recherche, bestem Wissen und Gewissen und in Abstimmungen mit Spezialisten zusammengestellt. Da wir keine Rechtsanwälte sind, können wir dafür keine Haftung übernehmen. Für rechtssichere Informationen zum Thema DSGVO, ePrivacy und weiteren datenschutzrechtlichen Fragen raten wir auf alle Fälle, einen Rechtsexperten zu kontaktieren.

holzweg GmbH. Adamgasse 11 | 6020 Innsbruck | www.holzweg.com
Ingrid Eppensteiner : +43 699 174074 02 | ingrid.eppensteiner@holzweg.com

CHECKLISTE

1. SSL-VERSCHLÜSSELUNG

- ☐ von http auf https umstellen

2. DATENSCHUTZERKLÄRUNG

- ☐ Datenschutzrichtlinien aktualisieren (eigener Navigationspunkt)
- ☐ Verlinkungen auf der Website zu dieser Seite erstellen (Newsletter, Kontaktformulare, etc.)

3. NEWSLETTER-ANMELDUNG

- ☐ Double Opt-in ermöglichen
- ☐ Abmeldungsmöglichkeit geben
- ☐ Info/Checkbox für Opt-in-Formular erstellen
- ☐ Link zur Datenschutzerklärung erstellen
- ☐ Hinweistext „Zweck der Daten“ einfügen

4. KONTAKTFORMULAR

- ☐ nur relevante Daten abfragen
- ☐ Hinweis & Checkbox zu Datenschutz hinterlegen

5. CLOUDDIENSTLEISTUNGEN

- ☐ Verträge zur Auftragsdatenverarbeitung abschließen

6. COOKIES

- ☐ in der Datenschutzerklärung auf Cookies hinweisen
- ☐ Opt-out Möglichkeit geben
- ☐ Cookie-Banner erstellen (nur notwendig bei AdSense oder DoubleClick)

7. AUFTRAGSDATEN-VERARBEITUNGSVERTRAG

- ☐ Vertrag abschließen mit allen Sub-Unternehmen, mit denen personenbezogenen Daten ausgetauscht werden

8. IP-ADRESSE

- ☐ Vertrag zur Auftragsverarbeitung mit Google abschließen Datenschutzerklärung dahingehend anpassen
- ☐ IP-Adressen der Website-Besucher anonymisieren
- ☐ Opt-out-Verfahren einbinden
- ☐ Altdaten löschen und neue Properties anlegen

9. E-MAILSYSTEME

- ☐ Widerrufsrecht einbauen
- ☐ Einwilligung einholen & nachweisbar ablegen
- ☐ Widerrufsrecht einbauen
- ☐ Subunternehmer in Verarbeitungsverzeichnis aufnehmen

10. SOCIAL MEDIA

- ☐ 2-Klick-Lösung für die Like- und Teilen-Funktion z.B. für Facebook

11. CRM- & KUNDENDATENSYSTEME

- ☐ Kundenrechte beachten

12. VERARBEITUNGSVERZEICHNIS

- ☐ alle Prozesse dokumentieren, in denen personenbezogene Daten verarbeitet werden

DSGVO-ANGEBOTE

WEBSITE-CHECK

Wir führen einen Website-Check für Sie durch.	**Ab € 300,-**
Ergebnis: • Aktueller Stand Ihrer Website • Strukturiertes Prüfungsergebnis als PDF • Liste noch notwendiger Maßnahmen, um DSGVO konform zu sein • Standardformulierungen zu Cookies, Google Analytics, usw.	*je nach Umfang*

NEWSLETTER – CRM-SYSTEME UND DSGVO

Durch unsere zertifizierten Berater erhalten Sie bei speziellen Beratungen bis zu 50 % der Kosten gefördert!

• **Workshops** und **Strategieberatungen** zu E-Mail-, Newsletter-, CRM- und Adressdatenverwaltungssystemen (gerne auch mit Blick auf DSGVO) sowie Erarbeiten eines Maßnahmenplans und möglicher Prozessverbesserungen im Zusammenspiel zwischen den Tools. Auf Wunsch Evaluierung neue Tools.	**Ab € 2.000,-** *je nach Umfang und Inhalte*
• **Förderungsberatung**: Überblick über die Förderlandschaft in Tirol von der Idee über das Konzept, externer Beratung, Investitionen bis hin zu geförderten Weiterbildungen für Sie und ihre MitarbeiterInnen.	**Ab € 400,-**
• Erstellung einer kostenlosen **Potentialanalyse** für Ihr Unternehmen mit Blick auf digitale Trends und Innovationen und deren Chancen und Risiken für Ihr Unternehmen. Diese Analyse in Kombination mit einem anschließenden Strategieworkshop zum Thema Digitalisierung kann wertvollen Input für Ihre jährliche Strategieplanung liefern.	**100% gefördert**

ERKLÄRUNGEN ZUR CHECKLISTE

Hintergrundinformationen zu den einzelnen Punkten der Checkliste:

SSL steht für “Secure Sockets Layer”: Ohne diese Verschlüsselung können die Daten von Dritten gelesen werden, daher ist dieser Schritt notwendig. Außerdem hat Google bereits im August 2014 damit begonnen, Websites mit HTTPS-Verschlüsselung in ihrem Algorithmus höher zu ranken.

Die Datenschutzerklärung sollte DSGVO-konform in einem eigenen Navigationspunkt aktualisiert werden. Muster dafür bietet z.B. die WKO.

a) Double Opt-in: Der neue Newsletter-Abonnent erhält zusätzlich einen Bestätigungslink. Diese ausdrückliche Einwilligung ist notwendig, um Werbe-E-Mails versenden zu dürfen.

b) Abmeldelink: Dieser muss in jedes E-Mail direkt eingebaut werden. Zusätzlich sollten Sie eine Abmeldemöglichkeit auf der Website einbinden. Diese kann auch in der Datenschutzerklärung zusammen mit dem Hinweis auf das Recht der Auskunft, Berichtigung, Löschung und des Widerspruchs der Datenerfassung allgemein enthalten sein.

c) Pflicht-Checkbox: Integrieren Sie diese Checkbox auf der Anmeldeseite zum Newsletter und beachten Sie, dass die Box direkt durch den Besucher selbst aktiviert werden muss, um die Anmeldung erfolgreich abschließen zu können. Vorausgewählte Boxen sind nicht gültig.

d) Zweck der Datenerhebung: Wenn Sie ein Newsletter-Formular oder einen Anmelde-Button auf der Website haben, dann ist es ratsam, darunter einen Hinweis zu schreiben, für welchen Zweck die Daten erhoben werden und was mit diesen Daten passiert.

Hier gilt das Prinzip der Sparsamkeit: Erheben Sie so wenig personenbezogenen Daten wie möglich. Personenbezogen sind z.B. Nachname, Vorname, E-Mailadresse und Telefonnummer. Erlaubt ist die Erhebung dieser Daten, wenn der Betroffene freiwillig, bewusst und eindeutig in die Datenverarbeitung einwilligt. Außerdem muss er die Möglichkeit bekommen, jederzeit die erteilte Zustimmung wieder löschen oder ändern zu können.

Lösung: Eigene Checkbox. Hier ist kein Double-Opt-in notwendig. Es wäre aber ratsam, einen Link zur Datenschutzerklärung zu setzen und nachzufragen, ob der Websitebesucher die Datenschutzerklärung gelesen hat. Bestellungsdaten berechtigen nicht automatisch zum Versand von Werbe-E-Mails. Diese dürfen nicht damit verknüpft werden und müssen separat eingeholt werden (=Koppelungsverbot).

Wenn Ihre Website nicht auf Ihrem eigenen Server im eigenen Rechenzentrum liegt, oder wenn Sie *Office 365* in der *Cloud*, *Trello*, *Dropbox*, usw. nützen und auf diesen Plattformen Kundendaten ablegen, dann müssen Sie Auftragsverarbeitungsverträge abschließen. Sie sind ab sofort in der Pflicht, dass die Drittanbieter DSGVO-konform mit den Daten umgehen. *Dropbox* zum Beispiel, welches bei vielen Unternehmen im Einsatz ist, hat laut aktueller Recherche (Anfang Mai 2018) noch keinen gültigen Vertrag. *Dropbox* verspricht jedoch, bis 25.05.2018 DSGVO-konform zu sein.

Fast alle Webseiten haben Cookies im Einsatz. Diese erleichtern das Surfen und erkennen den User wieder (z.B. müssen so Zugangsdaten nicht neu eingeben werden). Das ist in den so genannten „Cookie-Richtlinien" in der EU geregelt und sieht eine ausdrückliche Einwilligung des Nutzers in solchen Fällen vor. Deutschland hat das jedoch z.B. nicht umgesetzt und daher gilt diese dort eigentlich nicht.

In Österreich wird dieses Thema in der derzeit heiß diskutierte ePrivacy-VO geregelt werden (diese kommt wahrscheinlich erst 2019). Der momentane Stand in Österreich ist, dass Cookies nur noch dann gesetzt werden dürfen, wenn User ausdrücklich dazu einwilligen. Bei Session-Cookies, bei denen Cookies technisch notwendig sind, dürfen sie ohne die Einwilligung gesetzt werden.

In der Datenschutzerklärung muss auf Cookies hingewiesen und die Opt-Out Möglichkeit gegeben werden. Einen Cookie-Banner braucht es laut DSGVO nicht, aber Google schreibt dieses Cookie-Banner vor, wenn Sie AdSense oder DoubleClick einsetzen.

Fertigen Sie eine Liste an, mit welchen Subunternehmer, Social Media-, und Werbeagenturen für E-Mail-Marketing-Aktionen, E-Mail-Marketing-Software, Tracking-Software, Hoster, Buchhalter, Steuerberater, usw. Sie **personenbezogene Daten austauschen.** Schließen Sie mit allen einen Vertrag zur Auftragsverarbeitung ab.

Mithilfe der **IP-Adresse** ist es möglich, Personen eindeutig zu identifizieren – diese wird daher als personenbezogen angesehen. Folgende Schritte sind für die DSGVO notwendig:

a) Vertrag mit Google zur Auftragsverarbeitung abschließen: Den Vertrag ausdrucken und an Google nach Irland senden. Eine Anleitung zum genauen Vorgehen finden Sie auf der ersten Seite des ADV-Vertrages von Google. Ab 25. Mai 2018 wird es voraussichtlich eine Online-Variante geben.

b) Datenschutzerklärung mit Hinweis, dass Google Analytics verwendet wird, **anpassen**: Dafür gibt es Standard-Formulierungen.

c) Anonymisierung der IP-Adressen: Google Analytics bietet anonymizeIP für die Anonymisierung an, dadurch werden die letzten drei Ziffern der IP-Adresse (das ist die Hostkennung) gelöscht. Eine grobe Standort-Identifizierung ist dadurch trotzdem weiterhin möglich, aber es lässt auf kein Gerät Ihrer Besucher schließen. Es gibt Unterschiede in der Code-Einbindung, je nachdem, ob das Universal Analytics, das klassische Google-Analytics oder der Google Tag Manager genutzt wird.

d) Widerrufsmöglichkeit der Einwilligung zur Verarbeitung personenbezogener Daten – die Einbindung der Opt-out Möglichkeit. Dafür gibt es ein Browser-Add-on, welches aber auf mobilen Geräten nicht funktioniert. Deshalb ist es zusätzlich notwendig, auf ein Opt-out-Cookie zu verlinken.

e) Altdaten löschen und neue GA-Property anlegen: Wenn die Besucher der Website bisher nicht anonymisiert wurden, sind alle Besuche mit der vollständigen IP-Adresse aufgezeichnet worden. Da dies laut neuer DSGVO verboten ist, müssen alle Daten gelöscht werden. Das funktioniert, indem eine neue Property in Google Analytics angelegt wird – am besten mit einem neuen Namen. Danach die alte Property aufrufen und in den Papierkorb legen.

Mit 12. April launchte Google eine Steueroption zur Datenaufbewahrung (Data Retention Control). Damit kann man als Webmaster festlegen, nach welcher Zeit Nutzerdaten automatisch von den Google Servern gelöscht werden sollen. Per Default scheint dieser Wert auf 26 Monate gesetzt zu sein. Außerdem wurde ein Tool angekündigt, um in Zukunft alle Daten, die einem einzelnen User zugeordnet werden können, aus Analytics zu löschen.

a) Wo sind die personenbezogenen Daten?

- ✓ Im eigenen Unternehmen
- ✓ In einem EU-Land
- ✓ In einem sicheren Drittland (z.B. Schweiz)
- ✓ In einem Land mit speziellem Abkommen (z.B. USA)
- ✓ Im Unternehmen: im Auftragsverarbeitungsverzeichnis erfassen

In einem EU-Land ist die Verwendung von E-Mailsystemen problemlos. Einfach den angebotenen Vertrag zur Datenverarbeitung von den Softwareanbietern unterzeichnen und in der Datenschutzerklärung auf der Website die notwendigen Hinweise angeben.

In einem sicheren Drittland bzw. Land mit speziellem Abkommen: Hier liegt die Verantwortung bei Ihnen, immer wieder zu prüfen, ob das Newsletter-Tool noch DSGVO-konform ist. Mit der USA (betrifft vor allem *Mailchimp*) wurde eine sogenannte Privacy Shield Abkommen getroffen – dieses ist seit 2016 gültig und löst damit das vorherige Safe-Harbor ab, welches im Dezember 2015 laut EUGH als europarechtswidrig erklärt wurde. Darin wird ausgedrückt geregelt, dass Unternehmen aus den USA Daten speichern und verarbeiten dürfen, wenn sie sich vertraglich dazu verpflichten, gewisse Richtlinien einzuhalten. *Mailchimp* hat sich laut Recherche dazu verpflichtet. Siehe Privacy Shield Abkommen Mailchimp: Inwiefern das neue Abkommen dann tatsächlich einer gerichtlichen Überprüfung durch den EUGH standhalten wird, wissen wir nicht. Eher geht unsere Empfehlung dahin, einen Anbieter aus der EU zu nutzen. Es bleibt eine Unsicherheit bestehen, wie lange Unternehmen wie *Mailchimp* als sicher im Sinne der DSGVO gelten.

b) Gibt es eine gesetzliche Erlaubnis oder Einwilligung auch für bereits bestehende Newsletter Abonnenten? Diese müssen nachgewiesen werden können. Wissen Sie, woher ihre Kontaktdaten kommen? (Bestehender Kunde und Vertrag, kein Kunde, usw.) Können Sie den Nachweis der Einwilligung (E-Mail-Adresse, Datum, Uhrzeit) zum Newsletter von allen Newsletter-Empfängern erbringen? (Durch Double opt-in)

c) Verwendungsgrund der Daten: laut Art.13 der DSGVO muss eine entsprechende Datenschutzerklärung formuliert und über die Datenverarbeitungsvorgänge informiert werden.

d) Widerrrufsrecht einbauen

e) Subunternehmer im Verarbeitungsverzeichnis aufnehmen: Unternehmen, mit denen Sie z.B. E-Mail-Kampagnen umsetzen, müssen mit Ihnen einen Vertrag zur Auftragsverarbeitung abschließen.

Durch das Einbinden von Facebook, Twitter & Co wurden bisher personenbezogene Daten wie die IP-Adresse ohne Einwilligung der Besucher übertragen, ganz unabhängig davon, ob der Besucher mit dem Button in irgendeiner Weise agiert. Beim Facebook „Like"-Button kommt hinzu, dass Facebook beim Aufrufen einer Seite über Cookies, die auf dem Rechner des Nutzers hinterlegt sind, prüft, ob der Nutzer bei Facebook angemeldet ist. Wenn nun ein Nutzer bei Facebook eingeloggt ist, und auf einer Seite mit eingebundenen „Gefällt mir"-Plugin surft, werden personenbezogene Daten übertragen, die Facebook dem Nutzer zuordnet. Laut DSGVO ist das nun nicht mehr erlaubt. Reine Verlinkungen auf ihre Social-Media-Profile sind jedoch kein Problem.

Lösung: Bei Einbindung von Like- und Teilen-Funktionen muss vorher eine Einwilligung der Besucher erfolgen. Das funktioniert z.B. mit einer 2-Klick-Lösung: mit dem ersten Klick werden die Social-Media-Funktionen aktiviert, mit dem zweiten Klick kann der Inhalt geteilt/geliked werden. Oder Sie binden **Shariff-Buttons** ein: Hier werden die Besucherdaten nur dann übertragen, wenn auf einen Social-Media-Button geklickt wird – vorher werden keine Besucherdaten weitergeleitet.

Es müssen folgende Rechte der Kunden berücksichtigt werden:

- ✓ Auskunftsrecht
- ✓ Recht auf Löschung des Datensatzes
- ✓ Recht auf eingeschränkte Verarbeitung
- ✓ Prinzip der Richtigkeit

Daher sollten sich folgende Dinge wiederfinden:

- ✓ Rechtsgrund der Datenverarbeitung
- ✓ Einwilligung der Person
- ✓ Verarbeitungszweck
- ✓ Ablaufdatum der personenbezogenen Daten
- ✓ Datenquelle
- ✓ Datenprüfung
- ✓ Security und Zugriffsrechte
- ✓ Prozesse im CRM und Dokumentation im Verarbeitungsverzeichnis

Das Verarbeitungsverzeichnis löst in Österreich das DVR Register, in Deutschland das Bundesdatenschutzgesetz und in Italien den italienischen Datenschutzkodex ab. Das Verarbeitungsverzeichnis in Österreich beinhaltet die Verarbeitungstätigkeiten (Prozesse) des Verantwortlichen, in denen personenbezogene Daten verarbeitet werden. Hier müssen unter anderem auch der Zweck und die TOMs (technische und organisatorische Maßnahmen) dargestellt werden.

DSGVO ANSPRECHPARTNER

Ansprechpartner zum Thema DSGVO bei holzweg sind:

INGRID EPPENSTEINER

Marketing/Sales & Digital Consultant
ingrid.eppensteiner@holzweg.com

Da wir aber keine DSGVO-Experten sind, hier für Sie ein Ansprechpartner für darüber hinausgehende Fragen:

MARKUS REITSHAMMER
info@re-systems.com

Zertifizierter Datenschutzbeauftragter

Sie möchten Details in der DSGVO nachlesen?

https://www.dsb.gv.at/datenschutz-grundverordnung

Viele weiterführende Informationen bietet die WKO

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Informationen-zur-EU-Datenschutz-Grundverordnung.html