EU-Datenschutz-Grundverordnung: Auswirkungen auf Websites und Webshops

Übersichtsseite mit für Websites relevanten Themen und konkreten Anpassungsnotwendigkeiten

Die EU-Datenschutz-Grundverordnung (DSGVO) gilt seit 25. Mai 2018 unmittelbar. Der Text ist im Amtsblatt der EU bereits veröffentlicht.

Nähere Informationen finden Sie auf wko.at/datenschutz.

Die Verordnung enthält viele sogenannte "Öffnungsklauseln"; das sind Spielräume für Mitgliedsstaaten, nationale Regelungen vorzusehen. Die Nutzung dieser Öffnungsklauseln und Spielräume wurde in Österreich in Form von zwei Novellen zum Datenschutzgesetz (DSG 2018), nämlich dem Datenschutz-Anpassungsgesetz (DSG 2018) und dem Datenschutz-Deregulierungsgesetz 2018, beschlossen. Darin wurde das Alter für allenfalls notwendige Einwilligungen zu Datenverarbeitungen im Internet von 16 Jahren (DSGVO) auf 14 Jahre (DSG 2018) gesenkt.

Diese Übersichtsseite erläutert die wichtigsten für Websites relevanten Themen und zeigt konkrete Anpassungsnotwendigkeiten auf. In jedem Kapitel finden Sie zu wichtigen Begriffen im Text Links zu weiterführenden Inhalten sowie am Ende konkrete To Do–Vorschläge.

Für Cookies und Online-Direktwerbung (z.B. E-Mail-Newsletter) ist derzeit eine eigene europäische Datenschutz-Verordnung für elektronische Kommunikation (E-DSVO oder E-Privacy-VO) in Diskussion. Bis dahin gelten im Zusammenhang mit Cookies und Online-Direktwerbung die Bestimmungen des Telekommunikationsgesetzes (TKG). Informationen unter Berücksichtigung der DSGVO, bezüglich des TKG aber zur derzeitigen Rechtslage „Datenverarbeitung im Webshop/auf der Website: Einwilligungserklärung –Cookies – Datenschutzerklärung“ bzw „E-Mails versenden – aber richtig“.

Verarbeitung von Nutzerdaten – Grundsätze (Art 5 DSGVO)

Wenn Sie (auf Ihrer Website) personenbezogene Daten verarbeiten (insbesondere Erheben, Erfassen, Speichern, Auslesen, Abfragen, Verwenden, Ändern, Abgleichen, Übermitteln, Bereitstellen, Verknüpfen) haben Sie die geltenden Datenschutzbestimmungen einzuhalten. Die IP-Adresse gilt als personenbezogenes Datum.

Wenn Sie einen Webshop betreiben, verarbeiten Sie jedenfalls personenbezogene Daten und haben daher die jeweils geltenden Datenschutzbestimmungen einzuhalten. Jede Datenverarbeitung hat den in der DSGVO normierten Grundsätzen zu entsprechen. Dazu gehört neben einem gerechtfertigten Zweck und dem Grundsatz der Datenminimierung (auch im Hinblick auf Speicherdauer) unter anderem die Rechtmäßigkeit der Datenverarbeitung.

Wann ist eine Datenverarbeitung „rechtmäßig“ (Art 6 DSGVO)?

Wie schon nach der bisherigen Rechtslage dürfen personenbezogene Daten von Usern /Nutzern/Kunden/Website-Besuchern (die DSGVO spricht von „Betroffenen“) nur dann verarbeitet werden, wenn die Verarbeitung „rechtmäßig“ ist.

Eine Datenverarbeitung ist dann rechtmäßig, wenn einer der folgenden Punkte vorliegt:

- Verarbeitung ist zur Erfüllung des Vertrages unmittelbar notwendig (z.B. zur Abwicklung eines Online-Kaufes; Marketing nach dem Kauf ist aber bereits nicht mehr zur Vertragserfüllung notwendig). Es dürfen auch nicht mehr Daten als unbedingt erforderlich erhoben werden.

> **Beispiel:**
> Für die Zustellung der Bestellung im Webshop wird die Zusendeadresse erhoben. Diese muss für die Vertragserfüllung gespeichert und verarbeitet werden. Dies ist zulässig. Das bedeutet aber noch nicht automatisch, dass diese Adresse auch für die Zusendung von Werbematerial verwendet werden darf.

- Berechtigtes Interesse des Verantwortlichen (des Datenverarbeiters), sofern nicht die Interessen des Betroffenen überwiegen (vom Datenverarbeiter vorzunehmende Interessenabwägung). Nach Erwägungsgrund 47 kann Direktwerbung als ein berechtigtes Interesse betrachtet werden.

> **Beispiel:**
> Die Zusendung von Werbematerial per Post (per E-Mail bestehen Sondervorschriften; hier ist in der Regel eine vorherige Einwilligung notwendig) könnte als berechtigtes Interesse des Webshopbetreibers gesehen werden.

- Einwilligung des Betroffenen für einen oder mehrere genau bezeichnete und bestimmte Zwecke

> **Beispiel:**
> Der Besucher einer Website willigt ausdrücklich ein, vom Unternehmen X E-Mail-Newsletter zu erhalten.

- Erfüllung einer rechtlichen Verpflichtung des Datenverarbeiters

> **Beispiel:**
> Steuerrechtliche oder sozialversicherungsrechtliche Pflichten (Lohnverrechnung).

- Erfüllung einer Aufgabe im öffentlichen Interesse

Wenn in einem Webshop ausschließlich Daten verarbeitet werden, die zur Vertragsabwicklung notwendig sind und die Daten auch ausschließlich zur Vertragsabwicklung verwendet werden, kann eine Einwilligung entfallen. Informationspflichten (siehe unten) gibt es aber auch in diesem Fall.

Auf Grund des TKG dürfen allerdings nur Daten verarbeitet bzw. Cookies gesetzt werden, die zur Nutzung des jeweiligen Dienstes der Website (technisch oder zur Vertragserfüllung) erforderlich sind. Für alle anderen Cookies muss mit der Rechtsgrundlage der Einwilligung gearbeitet werden. Dies geschieht am besten durch Aufpoppen eines „Cookie-Fensters".

Bei sensiblen Daten (ethnische Herkunft; politische, religiöse oder weltanschauliche Überzeugung; Gewerkschaftszugehörigkeit; genetische Daten; biometrische Daten; sexuelle Ausrichtung) ist eine Datenverarbeitung auf Basis eines berechtigten Interesses nicht möglich. Die für Webseitenbetreiber wichtigste Rechtmäßigkeitsgrundlage für die Verarbeitung sensibler Daten ist eine ausdrückliche Einwilligung (aktives Ankreuzen einer Checkbox).

Wie sieht eine gültige Einwilligung aus (Art 7 DSGVO)?

Um gültig zu sein, muss eine Einwilligung folgende Kriterien erfüllen:

- freiwillig
- in informierter Weise und unmissverständlich (dies ergibt sich aus den Erläuterungen – „den sogenannten Erwägungsgründen" - der DSGVO)
- nachweisbar
- inhaltlich und optisch von anderen Erklärungen oder Texten abgegrenzt (nicht in AGB versteckt)
- nicht mit anderen Erklärungen gekoppelt; dieses sogenannte „Koppelungsverbot" bedeutet in der Praxis: im Zweifel für jede Datenanwendung eine eigene Checkbox, die aktiv angekreuzt werden muss)
- in verständlicher, leicht zugänglicher Form; in klarer und einfacher Sprache
- jederzeit widerrufbar

Aus dem Kriterium, dass die Einwilligung „in informierter Weise und unmissverständlich" erfolgen muss, kann abgeleitet werden, dass vor bzw. im Zuge der Einwilligungserklärung die Informationspflichten (Art 13, Art 14) zur Kenntnis gebracht werden müssen.

Das Koppelungsverbot bedeutet: Eine Einwilligung ist unzulässig, wenn die Erfüllung eines Vertrages, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung des Vertrages nicht erforderlich ist.

Beispiel:
Die Website/der Webshop muss auch ohne Datenauswertung, die für die Bestellung bzw die Dienste auf der Website nicht unmittelbar notwendig sind, funktionsfähig sein.

Die Einwilligung eines Kindes ist nur dann rechtmäßig, wenn das Kind das 16.Lebensjahr (DSGVO) vollendet hat. Österreich hat diese Grenze auf 14 Jahre herabgesetzt (§ 4 Abs 4 DSG 2018). Wie der Nachweis des Erreichens der relevanten Altersgrenze erfolgen soll, ist derzeit noch offen.

Dürfen Daten, deren Verwendung vom ursprünglichen Verwendungszweck nicht umfasst sind, für weitere Zwecke als den ursprünglichen Zweck verwendet werden (Art 6 Abs 4 DSGVO)?

Sie haben Daten rechtmäßig (z.B. auf Grund einer Einwilligung oder im Rahmen der Vertragserfüllung) erhoben und wollen diese Daten für einen weiteren Zweck (z.B. Geburtstagsgrüße), der von der ursprünglichen Rechtsgrundlage (z.B. Einwilligung oder Vertragserfüllung) nicht umfasst ist, verwenden. Dafür besteht eine „Erleichterung" im Vergleich zur bisherigen Rechtslage insofern, als dass künftig rechtmäßig erhobene Daten auch zu anderen als zu den ursprünglichen Zwecken verwendet werden dürfen, ohne dass dafür eine eigene Einwilligung erforderlich ist. Dies aber nur dann, wenn folgende Punkte eingehalten werden:

- Es besteht eine inhaltliche Verbindung bzw. ein Zusammenhang zwischen den ursprünglichen und den neuen Zwecken und der ursprünglichen Datenerhebung (z.B. Kundenbindung, Marketing für eigene Produkte)
- Vorhandensein angemessener Garantien gegen einen Missbrauch, wie insbesondere eine Pseudonymisierung oder Verschlüsselung der Daten. Bei der Frage, welche Maßnahmen als angemessen angesehen werden, sind die Art der Daten sowie mögliche Folgen der Weiterverarbeitung für betroffene Personen zu berücksichtigen.
- Der Betroffene ist von den weiteren Verwendungszwecken zu informieren.

Beispiel:
Im Zuge einer Bestellung wird auch das Geburtsdatum erhoben – entweder als freiwillige Angabe oder um das Alter des Bestellers überprüfen zu können oder um für den Fall einer erst nachträglichen Zahlung (bzw nicht-Zahlung) den Schuldner für einen Exekutionsantrag eindeutig identifizieren zu können. Ohne dass dafür eine ausdrückliche Einwilligung vorliegt, soll dieses Datum auch für einen zusätzlichen Zweck, nämlich die Zustellung von Geburtstagsgrüßen verwendet werden. Wenn der Betroffene z.B. in der Datenschutzerklärung über diese Verwendung informiert wird, kann diese Verwendung wohl als zulässig erachtet werden. Allerdings sollte dazu nicht eine offene Postkarte verwendet werden, aus der jedermann das Geburtsdatum oder gar das Alter ersehen kann.

Welche Informationspflichten gibt es bei der Datenerhebung (Art 13 DSGVO)?

Neu ist, dass die DSGVO anders als das bisherige Datenschutzgesetz losgelöst von einem aktiven Auskunftsbegehren eines Betroffenen umfangreiche Informationspflichten bereits im Zeitpunkt der Datenerhebung kennt. Da außerdem eine allenfalls zusätzlich erforderliche Einwilligungserklärung „in informierter Weise und unmissverständlich" erfolgen muss, setzt dies voraus, dass diesen Informationspflichten vor bzw. im Zuge der Einverständniserklärung nachgekommen wird. Aber auch wenn keine Einverständniserklärung notwendig ist, ist den Informationspflichten nachzukommen.

Bei den Informationspflichten handelt es sich um folgende Punkte (so diese im konkreten Einzelfall zutreffen):

- Name und Kontaktdaten des für die Datenverarbeitung Verantwortlichen
- Zweck sowie Rechtsgrundlage für die Verarbeitung
- Angabe der berechtigten Interessen zur Datenverarbeitung (wenn diese nicht auf einer Einwilligung, sondern auf einer Interessenabwägung beruht)

- Empfänger oder Kategorien von Empfängern
- Absicht, Daten an ein Drittland oder eine internationale Organisation zu übermitteln
- Speicherdauer, bzw. Kriterien für die Festlegung der Dauer (wenn eine konkrete Speicherdauer nicht angegeben werden kann; z.B. „bis zum Ablauf der Vertragsdauer“, „bis zum Verlassen der Website“, „bis zur Beendigung der Session“)
- Hinweis auf das Auskunftsrecht, Berichtigungsrecht und Löschungsrecht oder Einschränkung der Verarbeitung sowie auf das Widerspruchsrecht und das Recht auf Datenübertragbarkeit
- Hinweis auf das Widerrufsrecht, wenn die Daten durch Einwilligung erhoben wurden
- Hinweis auf ein allfälliges Beschwerderecht bei einer Aufsichtsbehörde
- Hinweis, wie weit die Datenbereitstellung gesetzlich oder vertraglich vorgeschrieben ist oder für den Vertragsabschluss erforderlich ist
- Hinweis, ob die betroffene Person verpflichtet ist, die Daten bereit zu stellen und welche möglichen Folgen die Nichtbereitstellung hätte
- Hinweis, ob die Daten zu einer automatisierten Entscheidungsfindung (einschließlich Profiling) verwendet werden und eine allgemein verständliche Darstellung der Entscheidungslogik sowie der Tragweite der Auswirkungen einer derartigen Verarbeitung
- Verwendung der Daten für einen anderen als den ursprünglichen Verwendungszweck

In diesen im Gegensatz zur bisherigen Rechtslage sehr umfassenden Informationspflichten besteht die für Webseiten wesentlichste inhaltliche Neuerung durch die DSGVO. Diese Informationspflichten entsprechen in etwa dem, was schon bisher als „Datenschutzerklärung“ auf vielen Websites zwar nicht in dieser Tiefe gesetzlich (TKG) vorgeschrieben, aber weitgehend best practice war.

Nach dem TKG bestehen folgende Informationspflichten, die aber weitgehend mit jenen der DSGVO übereinstimmen:

- Angabe, welche Daten verarbeitet oder an Dritte übermittelt werden
- Rechtsgrundlage (z.B. auf Grund eines Vertrages oder eines speziellen Gesetzes)
- Zweck der Verarbeitung
- Speicherdauer

Welche Informationspflichten gibt es, wenn Daten aus anderen Quellen verwendet werden (Art 14 DSGVO)?

Wenn Daten nicht direkt vom Betroffenen, sondern von Dritten erhoben werden, bestehen zusätzliche, d.h. zu den bereits oben angeführten Informationspflichten (Art 14 DSGVO) hinausgehende, insbesondere:

- Angabe der erhobenen Datenkategorien
- Angabe der Quellen aus denen allenfalls Daten eingespeist bzw. gesammelt werden

Welche Datensicherungsmaßnahmen sind bereits beim Webauftritt notwendig?

Datenanwendungen sind nach Möglichkeit so zu konfigurieren, dass bereits durch technische Voreinstellungen oder Konfigurationen der Website ein möglichst hohes Datenschutzniveau erreicht und erhalten wird (privacy by design/privacy by default).

Dazu gehört auch die möglichst weitgehende Pseudonymisierung der Daten.

To Do:

- Website nach Stand der Technik möglichst sicher und datenschutzfreundlich konfigurieren

Informationen zur technischen Umsetzung finden Sie auf der Website der European Union Agency for Network and Information Security (ENISA).

Wann muss ich eine Datenübertragbarkeit gewährleisten (Art 20 DSGVO)?

Datenverarbeiter haben die Übertragbarkeit von Daten, die der Betroffene bereitgestellt hat, in andere Portale oder Foren in einem strukturierten, gängigen und maschinenlesbaren Format zu gewährleisten (Datenportabilität).

Welche Dokumentationspflichten treffen mich?

Weil Sie mit Ihrer Website Nutzerdaten verarbeiten, trifft Sie eine betriebsinterne Dokumentationspflicht darüber, welche Daten zu welchem Zweck erhoben werden und was mit den erhobenen Daten geschieht (Verarbeitungsverzeichnis) sowie unter Umständen die Pflicht, das datenschutzrechtliche Risiko Ihrer Nutzer einzuschätzen (Datenschutz-Folgenabschätzung).

Da ein Webshop i.d.R. Kundenprofile erstellt, Webanalyse-Tools zur Auswertung des Nutzerverhaltens verwendet und/oder seine Kunden im Hinblick auf Kreditwürdigkeit überprüft, wird eine Datenschutz-Folgenabschätzung erforderlich sein.

Die Ausnahme für KMUs bis 250 Mitarbeiter von der Erstellung eines Verarbeitungsverzeichnisses greift gerade beim Webshop in der Regel nicht, weil die Datenverarbeitung nicht nur, wie in der Ausnahme gefordert, gelegentlich erfolgt und unter Umständen auch sensible Daten enthalten kann.

Nur durch Einhaltung der Dokumentationspflicht können Sie auch Ihren sonstigen

Verpflichtungen als „Verantwortlicher“
nachkommen.

Muss ich einen Datenschutz-Beauftragten bestellen (Art 37 DSGVO)?

Ein Datenschutz-Beauftragter ist nur zu bestellen, wenn die Kerntätigkeit des Betreibers einer Website in einer umfangreichen regelmäßigen oder systematischen Überwachung von betroffenen Personen oder in der umfangreichen Verarbeitung sensibler oder strafrechtsrelevanter Daten besteht. Wenn ein Webshop daher z.B. Profiling betreibt, wird dies idR nicht die Kerntätigkeit sein.

Benötige ich besondere Verträge mit externen Dienstleistern (Auftragsverarbeiter, Art 28 DSGVO)?

Auftragsverarbeiter ist, wer personenbezogene Daten weisungsgebunden im Auftrag eines Verantwortlichen und auf Basis eines Auftragsverarbeitervertrages (dieser muss bestimmte Mindestinhalte aufweisen) verarbeitet. Ein Auftragsverarbeiter hat keine Entscheidungsgewalt über den Verarbeitungszweck und über den wesentlichen, datenschutzrelevanten Mitteleinsatz (z.B. welche Daten wie lange verarbeitet werden). Entscheidungen in rein technisch-organisatorischer Hinsicht wird der Auftragsverarbeiter hingegen treffen können, ohne gleich in die Rolle des Verantwortlichen zu schlüpfen.

Werden Web-Analyse-Tools von Drittanbietern eingesetzt, wird es sich in der Regel um ein Auftragsverarbeiter-Verhältnis handeln, sofern der Betreiber des Web-Analyse-Tools die Daten lediglich im Rahmen des Auftrages und nur auf Weisung des Verantwortlichen (des Website-Betreibers) hin verarbeitet. Wenn er hingegen selbst Entscheidungen über eigene Verarbeitungszwecke oder über den wesentlichen Mitteleinsatz trifft, ist der Betreiber des Web-Analyse-Tools (auch) Verantwortlicher und benötigt die Übermittlung der (personenbezogenen) Daten an ihn daher eine eigene Rechtmäßigkeitsgrundlage.

Im Verhältnis zum Kunden müssen im Rahmen der Informationspflichten die Auftragsverarbeiter zumindest nach Kategorien (z.B. „Wir verwenden folgendes Web-Analyse-Tool: .... “) angegeben werden.

Wenn dabei Daten in einen Drittstaat (außerhalb der EU) übertragen werden, ist neben dem Empfänger auch der Drittstaat sowie der Umstand, ob ein sogenannter „Angemessenheitsbeschluss“ der EU-Kommission oder andere Grundlagen für den internationalen Datenverkehr (z.B. Standarddatenschutzklauseln, Binding Corporate Rules) vorliegen, anzugeben. Dabei sind die Bestimmungen zur Rechtmäßigkeit des internationalen Datenverkehrs zu berücksichtigen.

Muss ich etwas beachten, wenn ich eine bestehende Website oder einen bestehenden Webshop kaufen oder verkaufen möchte?

Wenn eine Website (z.B. an einen Unternehmensnachfolger) übertragen wird, werden damit unter Umständen auch personenbezogene Daten eines Betroffenen mit übertragen. Dies wird bei Webshops i.d.R. zutreffen. Dafür sind die Bestimmungen der DSGVO einzuhalten. Das bedeutet, dass ein Rechtsgrund (z.B. berechtigtes Interesse) für die Datenübertragung gefunden werden muss oder mit einer Einwilligung (Zustimmung) des Betroffenen gearbeitet werden muss. Der Erwerber hat außerdem den Informationspflichten des Art 14 DSGVO (Informationspflichten bezüglich nicht beim Betroffenen erhobener Daten) nachzukommen.

Zusammenfassung der TO DO-Liste:

- Evaluieren, welche Daten zu welchen Zwecken erhoben/verarbeitet/wie lange gespeichert werden
- Datenschutzerklärung anpassen oder erstellen
- Rechtsgrundlage überprüfen (Vertragserfüllung, technische Notwendigkeit/berechtigtes Interesse, Einwilligung)
- Erforderlichenfalls mit Einwilligungen arbeiten/Cookie-Fenster einrichten
- Evaluieren, ob die Einwilligung aller erhobenen Daten, Anwendungen und Zwecke (sowie gegebenenfalls ~~d~~die Übermittlung an Dritte) genau umfasst
- Keine vorangekreuzten Check-Boxen verwenden
- Altersgrenzen setzen
- Website nach Stand der Technik möglichst sicher und datenschutzfreundlich konfigurieren
- Website so erstellen, dass eine Datenübertragbarkeit möglich ist
- Betriebsinternes Daten-Dokumentationssystem aufbauen (Verarbeitungsverzeichnis, evtl. Datenschutz-Folgenabschätzung)
- Auftragsverarbeiter-Verträge schließen bzw. bestehende Verträge adaptieren

Tipp:

Überblicksweise Zusammenstellung zum Thema Cookies: Checkliste Cookies und Web-Analyse im WKO Webshop

Details:

Datenverarbeitung im Webshop und auf der Website - Einwilligungserklärung, Cookies, Datenschutzerklärung

Stand: 09.11.2021