EU-Datenschutz-Grundverordnung: Auswirkungen auf Websites und Webshops

Seit 25. Mai 2018 gilt sie, die Datenschutz-Grundverordnung (DSGVO). Wir fassen in diesem Beitrag zusammen, welche Anpassungen für Websites und Webshops durchzuführen sind, und geben zahlreiche praktische Beispiele.

Wenn Sie auf Ihrer Website personenbezogene Daten verarbeiten – dazu zählen das Erheben, Erfassen, Speichern, Auslesen, Abfragen, Verwenden, Ändern, Abgleichen, Übermitteln, Bereitstellen und Verknüpfen –, müssen die Datenschutzbestimmungen eingehalten werden. Die IP-Adresse gilt als personenbezogenes Datum. In Webshops verarbeiten Sie ebenso personenbezogene Daten. Jede Datenverarbeitung hat den in der DSGVO normierten Grundsätzen zu entsprechen. Dazu gehört neben einem gerechtfertigten Zweck und dem Grundsatz der Datenminimierung (ebenso im Hinblick auf Speicherdauer) unter anderem die Rechtmäßigkeit der Datenverarbeitung. Für Cookies und Online-Direktwerbung (z. B. E-Mail-Newsletter) wird es eine eigene Verordnung geben: die Datenschutzverordnung elektronische Kommunikation – E-DSVO. Bis dahin gelten die Bestimmungen des Telekommunikationsgesetzes (TKG).

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

Sowohl nach der derzeitigen Rechtslage als auch künftig dürfen personenbezogene Daten von Kunden (die DSGVO spricht von „Betroffenen“) nur dann verarbeitet werden, wenn die Verarbeitung „rechtmäßig“ ist. Dafür müssen folgende Punkte vorliegen:

Die Verarbeitung ist zur Erfüllung des Vertrages unmittelbar notwendig, z. B. bei der Abwicklung eines Onlinekaufs. Achtung: Marketing nach dem Kauf ist nicht mehr zur Vertragserfüllung notwendig. Es dürfen auch nicht mehr Daten als unbedingt erforderlich erhoben werden.
Beispiel: Für die Zustellung einer im Webshop bestellten Ware wird die Lieferadresse erhoben. Diese muss für die Vertragserfüllung gespeichert und verarbeitet werden. Das ist zulässig. Das bedeutet aber nicht automatisch, dass an diese Adresse nun auch Werbematerial versendet werden darf.

Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen (des Datenverarbeiters) erforderlich, 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. Hier ist in der Regel eine vorherige Einwilligung notwendig. Dies könnte als berechtigtes Interesse des Webshop-Betreibers gesehen werden.

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

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

Erfüllung einer rechtlichen Verpflichtung des Datenverarbeiters.
Beispiel: Steuerrechtliche oder sozialversicherungsrechtliche Pflichten (Lohnverrechnung).

Erfüllung einer Aufgabe im öffentlichen Interesse.
In Zweifelsfällen muss in der Praxis im Bereich des „berechtigten Interesses" oft mit einer Einwilligung (z. B. via Checkbox) gearbeitet werden. Wenn in einem Webshop ausschließlich Daten verarbeitet werden, die zur Vertragsabwicklung notwendig sind und diese Daten auch ausschließlich zur Vertragsabwicklung verwendet werden, kann eine Einwilligung entfallen. Informationspflichten (siehe unten) gibt es aber auch in diesem Fall.

To-dos:

Evaluieren, welche Daten zu welchen Zwecken erhoben/verarbeitet/wie lange gespeichert werden.
Erforderlichenfalls mit Einwilligungen arbeiten.
Bei sensiblen Daten (ethnische Herkunft; politische, religiöse oder weltanschauliche Überzeugung; Gewerkschaftszugehörigkeit; genetische Daten; biometrische Daten; sexuelle Ausrichtung) ist eine ausdrückliche Erklärung (aktives Ankreuzen einer Checkbox) notwendig.

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

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 den allgemeinen Geschäftsbedingungen versteckt und nicht mit anderen Erklärungen gekoppelt. Dieses sogenannte Koppelungsverbot bedeutet in der Praxis: Im Zweifel für jede Datenanwendung eine eigene Checkbox anbieten, die aktiv angekreuzt werden muss.
verständliche, leicht zugängliche Form; klare und einfache Sprache
jederzeit widerrufbar
Das Koppelungsverbot bedeutet: Eine Einwilligung ist unzulässig, wenn die Erfüllung eines Vertrages, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese 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.

To-dos:

Evaluieren, ob die Einwilligung alle erhobenen Daten, Anwendungen und Zwecke genau umfasst.
Keine vorangekreuzten Check-Boxen.
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 (Art. 4, Abs. 4 DSG 2018). Wie der Nachweis des Erreichens der relevanten Altersgrenze erfolgen soll, ist derzeit noch offen.

To-do: Altersgrenzen setzen.

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

Neu ist, dass die DSGVO, anders als das bisherige Datenschutzgesetz (ähnlich wie das bisherige Telekommunikationsgesetz; Art. 96), losgelöst von einem aktiven Auskunftsbegehren eines Betroffenen umfangreiche Informationspflichten bereits zum 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:

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
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 oder für den Vertragsabschluss erforderlich ist
Hinweis, ob die betroffene Person verpflichtet ist, die Daten bereitzustellen 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

Diese (im Gegensatz zur bisherigen Rechtslage) sehr umfassenden Informationspflichten sind die wesentlichste inhaltliche Neuerung für Websites durch die DSGVO. Sie 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.

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 Informationspflichten (Art. 14 DSGVO), insbesondere:

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

To-do: Datenschutzerklärung anpassen oder erstellen.

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.

Wann muss eine Datenübertragbarkeit gewährleistet werden (Art. 20 DSGVO)?

Datenverarbeiter haben die Übertragbarkeit von Daten in andere Portale oder Foren zu gewährleisten (Datenportabilität).

To-do: Website so erstellen, dass eine Datenübertragbarkeit möglich ist.

Welche Dokumentationspflichten treffen Sie?

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

Da ein Webshop zumeist 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 KMU 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.

To-do: Datenverarbeitungen auf der Website in das Verarbeitungsverzeichnis aufnehmen.

Was gilt es zu beachten, wenn eine bestehende Website oder ein bestehender Webshop gekauft oder verkauft werden 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 in der Regel 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.

To-dos:

Evaluieren, welche Daten zu welchen Zwecken erhoben/verarbeitet/wie lange gespeichert werden.
Datenschutzerklärung anpassen oder erstellen.
Erforderlichenfalls mit Einwilligungen arbeiten.
Evaluieren, ob die Einwilligung alle erhobenen Daten, Anwendungen und Zwecke 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, eventuell Datenschutz-Folgenabschätzung).
Auftragsverarbeiter-Verträge schließen bzw. bestehende Verträge adaptieren.
Foto: iStock.com/mikkelwilliam