

Die neue EU Datenschutzverordnung - DSGVO

Ab dem 25. Mai 2018 tritt die neue Datenschutzgrundverordnung (DSGVO) in den EU Mitgliedstaaten in Kraft. Die neue Datenschutzerklärung muss bis zu diesem Datum im Internet verfügbar sein. Was ändert sich?

Löschungspflicht

Unternehmen haben die Pflicht, Daten auf Verlangen zu löschen. Hat ein Nutzer einem Unternehmen seine Daten anvertraut, kann er die Löschung einfordern. Das gilt, solange es keine juristischen Gründe gibt, die es erfordern, dass die Daten erhalten bleiben.

Opt-in

Bislang mussten Nutzer der Verarbeitung ihrer Daten aktiv widersprechen. Diese so genannte Opt-out-Regelung ändert sich. An ihrer Stelle führt die neue EU-Verordnung das Opt-in-Verfahren ein. Damit müssen Nutzer aktiv der Verarbeitung ihrer Daten zustimmen.

Transparenz

Betreiber von Internetshops müssen dem Nutzer offen legen, welche Daten sie sammeln und wie sie diese verarbeiten. Wenn ein Internetshop Informationen an Dritte weiterleitet, dann erhalten Nutzer einen Zugriff auf ihre Daten.

Portabilität

Internetshops müssen jetzt sicherstellen, dass Daten eines Nutzers einfach auf einen anderen Anbieter übertragen werden können.

Meldepflicht

Wenn Daten verloren gehen, muss das Unternehmen diese Information innerhalb von 24 Stunden bei der Behörde melden.

Zentrale Aufsichtsbehörde

Die Verordnung sieht die Einrichtung von zentralen Aufsichtsbehörden vor, so dass Unternehmen in Zukunft eine zentrale Anlaufstelle haben.

Internationale Kontrolle

Unternehmen können den Missbrauch ihrer Daten bei der nationalen Aufsichtsbehörde melden die den Missbrauch auch grenzüberschreitend verfolgt.

Geltungsrecht

Der Geltungsbereich der Verordnung geht über die EU hinaus. Unternehmen, die ihren Sitz außerhalb der EU haben, aber in der EU tätig sind, sind der Verordnung verpflichtet.

Bußgeld

Die EU-Verordnung setzt als Bußgeld für Verstöße bis zu vier Prozent des Jahresumsatzes eines Unternehmens fest.

Administration

Um die Bürokratie für Unternehmen abzubauen, entfallen Pflichten in der Administration, wie zum Beispiel die Meldepflicht.

Jugendschutz

Jugendliche können sich erst ab 16 Jahren oder mit Einwilligung eines Erziehungs-berechtigten in sozialen Medien anmelden. Damit soll ihnen die Anmeldung bei Internetdiensten wie Facebook und Instagram künftig deutlich erschwert werden.

Betrieblicher Datenschutzbeauftragter

In Unternehmen muss ein Datenschutzbeauftragter bestellt werden, wenn sich mindestens zehn oder mehr Personen laufend mit der Datenerhebung und -verarbeitung beschäftigen.

Datenschutzerklärung auf der Website

Sobald man Daten von den Besuchern der Website abfragt ist eine Datenschutzerklärung notwendig. Das betrifft z.B. Versand von Newsletter, Downloads oder die Bestellung einer Broschüre, Gewinnspiele oder Registrierung auf der Website, Statistik-Programme oder Plugins die Besucher der Website zählen etc. Zu den Informationen die die Datenschutzerklärung enthalten muss gehören Name und Adresse des Betreibers, die Kontaktdaten des Datenschutzbeauftragten, Zweck der Datennutzung und die Weitergabe an Dritte mit deren Namensnennung. Darüber hinaus muss die Datenschutzerklärung die Dauer der Datenspeicherung angeben und über die Rechtslage des Datenschutzes, wie das Recht auf Beschwerde, Widerruf oder Auskunft aufklären.

Wo muss der Datenschutzhinweis stehen

Der Nutzer sollte maximal zwei Klicks tätigen müssen, um die Datenschutzhinweise zu sehen. Das kann sicherlich bei einer Prüfung positiv ausgelegt werden.

Zugriffsdaten und Server-Logfiles

Der Anbieter (oder sein Webspaces-Provider) erhebt Daten über jeden Zugriff auf das Angebot (so genannte Serverlogfiles). Zu den Zugriffsdaten gehören: Name der abgerufenen Webseite, Datei, Datum und Uhrzeit des Abrufs, übertragene Datenmenge, Meldung über erfolgreichen Abruf, Browsertyp nebst Version, das Betriebssystem des Nutzers, Referrer URL (die zuvor besuchte Seite), IP-Adresse und der anfragende Provider. Der Anbieter verwendet die Protokolldaten nur für statistische Auswertungen zum Zweck des Betriebs, der Sicherheit und der Optimierung des Angebotes. Der Anbieter behält sich jedoch vor, die Protokolldaten nachträglich zu überprüfen, wenn aufgrund konkreter Anhaltspunkte der berechnigte Verdacht einer rechtswidrigen Nutzung besteht.

Personenbezogene Daten

Personenbezogene Daten sind Informationen, mit deren Hilfe eine Person bestimmbar ist. Dazu gehören der Name, die Emailadresse oder die Telefonnummer, aber auch Daten über Vorlieben, Hobbies, Mitgliedschaften oder welche Webseiten von jemandem angesehen wurden. Personenbezogene Daten werden vom Anbieter nur dann erhoben, genutzt und weiter gegeben, wenn dies gesetzlich erlaubt ist oder die Nutzer einwilligen.

Cookie Hinweis

Sofern Cookies auf der Webseite, dem Blog oder einem Shop zu Marketingzwecken Verwendung finden, ist ein Hinweis darauf angeraten. Viele Content Management Systeme (WordPress, TYPO3, Drupal) nutzen Cookies, um den Nutzer zu „identifizieren“. Daher ist der Einsatz eines Cookie-Banners angeraten der beim Aufruf der Webseite zu sehen ist.

Kontaktaufnahme

Bei der Kontaktaufnahme mit dem Anbieter (zum Beispiel per Kontaktformular oder E-Mail) werden die Angaben des Nutzers zwecks Bearbeitung der Anfrage sowie für den Fall, dass Anschlussfragen entstehen, gespeichert.

Generator für eine Datenschutzerklärung: <https://datenschutz-generator.de/>

Das Datenschutzgesetz <https://dsgvo-gesetz.de/>

Beispiel für eine einfache Datenschutzerklärung

Inhaltlich Verantwortlicher gemäß § 10 Absatz 3 MDStV: Max Mustermann
Haftungshinweis: Trotz sorgfältiger inhaltlicher Kontrolle übernehmen wir keine Haftung für die Inhalte externer Links. Für den Inhalt der verlinkten Seiten sind ausschließlich deren Betreiber verantwortlich.

Geltungsbereich

Diese Datenschutzerklärung informiert über die Art, den Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten durch den verantwortlichen Anbieter Max Mustermann Musterstr 3 PLZ Musterstadt Mail Adresse Telefon auf dieser Website (im folgenden "Angebot") auf. Die rechtlichen Grundlagen des Datenschutzes finden sich im Bundesdatenschutzgesetz (BDSG) und dem Telemediengesetz (TMG).

Zugriffsdaten/ Server-Logfiles

Der Anbieter (beziehungsweise sein Webpace-Provider) erhebt Daten über jeden Zugriff auf das Angebot (so genannte Serverlogfiles). Zu den Zugriffsdaten gehören: Name der abgerufenen Webseite, Datei, Datum und Uhrzeit des Abrufs, übertragene Datenmenge, Meldung über erfolgreichen Abruf, Browsertyp nebst Version, das Betriebssystem des Nutzers, Referrer URL (die zuvor besuchte Seite), IP-Adresse und der anfragende Provider. Der Anbieter verwendet die Protokolldaten nur für statistische Auswertungen zum Zweck des Betriebs, der Sicherheit und der Optimierung des Angebotes. Der Anbieter behält sich jedoch vor, die Protokolldaten nachträglich zu überprüfen, wenn aufgrund konkreter Anhaltspunkte der berechnete Verdacht einer rechtswidrigen Nutzung besteht.

Umgang mit personenbezogenen Daten

Personenbezogene Daten sind Informationen, mit deren Hilfe eine Person bestimmbar ist, also Angaben, die zurück zu einer Person verfolgt werden können. Dazu gehören der Name, die Emailadresse oder die Telefonnummer. Aber auch Daten über Vorlieben, Hobbies, Mitgliedschaften oder welche Webseiten von jemandem angesehen wurden zählen zu personenbezogenen Daten. Personenbezogene Daten werden von dem Anbieter nur dann erhoben, genutzt und weiter gegeben, wenn dies gesetzlich erlaubt ist oder die Nutzer in die Datenerhebung einwilligen.

Kontaktaufnahme

Bei der Kontaktaufnahme mit dem Anbieter (zum Beispiel per Kontaktformular oder E-Mail) werden die Angaben des Nutzers zwecks Bearbeitung der Anfrage sowie für den Fall, dass Anschlussfragen entstehen, gespeichert.

Widerruf, Änderungen, Berichtigungen und Aktualisierungen

Der Nutzer hat das Recht, auf Antrag unentgeltlich Auskunft zu erhalten über die personenbezogenen Daten, die über ihn gespeichert wurden. Zusätzlich hat der Nutzer das Recht auf Berichtigung unrichtiger Daten, Sperrung und Löschung seiner personenbezogenen Daten, soweit dem keine gesetzliche Aufbewahrungspflicht entgegensteht.

Impressum

Nach wie vor müssen Angaben zum Betreiber der Website in einem Impressum aufgeführt werden. Dazu gehört die Postadresse, Kontaktdaten und Name des Schulbesitzers.

Hier eine Checkliste für eine „sichere“ Image-Website.

SSL Verschlüsselung

Sollte aktuell JEDE Website haben, egal ob mit oder ohne Online-Formular. Grund ist nicht nur der Datenschutz, die Browser warnen vermehrt auch bei Seiten ohne Formulare vor unverschlüsselten Websites.

Google Analytics

Die Snippets die im Quellcode eingesetzt werden, müssen das anonymize_ip enthalten und das Google OptOut muss eingesetzt sein. Dazu gehört ein Quellcode Snippet welches über dem GA-Code eingesetzt wird, sowie ein OptOut-Link im Datenschutz-Hinweis.

Cookie Toolbar

Die Toolbar ist anzuraten, wenn die Website Cookies setzt. Das ist bei vielen Content Management Systemen heute standardmäßig der Fall z.B. TYPO3, Wordpress etc.

Datenschutz-Checkbox in Formularen

In Formularen muss eine Pflichtfeld-Checkbox enthalten sein, mit der der User bestätigt die Datenschutz-Hinweis zur Kenntnis genommen zu haben. Natürlich sollte in unmittelbarer Nähe auch ein Link zum Datenschutz-Hinweis zu finden sind.

Datenschutz-Hinweis in Newsletter-Anmeldung

Sollte hier wenn möglich ebenso gemacht werden, falls der Newsletter-Anbieter das nicht ermöglicht, reicht ggf. auch ein Texthinweis auf den Datenschutz.

Social Media Einbindung

Gefällt mir und Teilen Buttons sollten über die Datenschutz-Lösung von Heise verbaut sein:
<https://www.heise.de/ct/artikel/Shariff-Social-Media-Buttons-mit-Datenschutz-2467514.html>

Video-Einbindung Youtube Datenschutz aktiv und ggf. Hinweis / 2-Click

Wenn man den Embed-Code bei Youtube generiert, sollte dort die Datenschutz-Checkbox aktiv sein. Es ändert sich dann die Domain, von der das Video eingebunden wird. Es werden dann erst Userdaten an Youtube übermittelt, wenn das Video angeschaut wird. Um auf Nummer sicher zu gehen sollte vor dem Start des Videos ein Datenschutz-Hinweis erscheinen, der erst weggeblickt werden muss (ähnlich 2-Click Social Media Lösung von Heise).

Datenschutzhinweis Text aktualisieren / vervollständigen

Der Datenschutz-Hinweis muss mit maximal 2 Klicks über den bei erstem Aufruf sichtbaren Bereich zu erreichen sein. Der Text sollte aktuell sein und je nach eingesetzter Technik passende Textbausteine haben (Newsletter, Cookies, Google Analytics, Facebook etc.).

Kontaktformular-Daten

Wenn z.B. Kontaktformular-Daten in der Datenbank oder auch Bewerbungen mit Datei-Anhängen in FTP-Verzeichnissen gespeichert werden, müssen diese regelmäßig nach einem bestimmten Zeitraum gelöscht werden, um das unnötige Vorhalten von persönlichen Daten zu vermeiden. Mit Hilfe von Cronjobs kann das löschen alle 3 Monate automatisch erfolgen.

Diese Hinweise wurden vom VDWS zusammengestellt mit freundlicher Unterstützung der Webagentur Ideenwerft GmbH Claudia Höhne in Kiel www.ideenwerft.com

Um sich vor teuren Abmahnungen von freundlichen Mitbewerbern zu schützen, empfehlen wir die Überprüfung der eigenen (evt. selbstgestrickten) Datenschutzerklärung durch einen Fachanwalt.