Das müssen Sie als Webseitenbetreiber zur neuen DSGVO wirklich wissen

Die zahlreichen Änderungen, die die DSGVO ab dem 25. Mai 2018 mit sich bringt, treffen jeden Unternehmer und Webseitenbetreiber. Es gibt in fast allen Bereichen des Datenschutzrechts umfangreiche Neuregelungen. Einige sind relativ einfach umzusetzen, andere sind sehr komplex.

Unser DSGVO-Special – das wir als eRecht24 Agenturpartner in Zusammenarbeit mit eRecht24 Premium für Sie zur Verfügung stellen – hilft Ihnen dabei, einen Überblick über die Anforderungen der DSGVO zu erhalten und zeigt Ihnen, wie Sie diese einfach und schnell für Ihre Webseite umzusetzen.
Gern unterstützen wir Sie in der DSGVOkonformen Umsetzung Ihrer Webseite. Sprechen Sie uns an.

1. Einführung

Die DSGVO regelt ab dem 25. Mai 2018 den Umgang von Unternehmen mit personenbezogenen Daten – einheitlich europaweit. Viele der aktuellen Vorschriften des deutschen Bundesdatenschutzgesetzes (BDSG) gelten dann nicht mehr bzw. das BDSG wird zeitgleich neu gefasst.

Die Datenschutzgrundverordnung vereinheitlicht das Datenschutzrecht innerhalb der EU, da bisher überall verschiedene Datenschutzgesetze und damit unterschiedliche Standards gelten. Unternehmer können also zukünftig darauf vertrauen, dass innerhalb der EU ein (überwiegend) einheitliches Datenschutzrecht gilt.

Die Verordnung gilt aber auch für Unternehmen mit Sitz außerhalb der EU, wenn diese Daten von Personen aus der EU verarbeiten. So soll sichergestellt werden, dass sich auch Cloud-Dienste oder soziale Netzwerke (etwa aus den USA) an die Regeln halten müssen.

Die DSGVO betrifft dabei wirklich JEDES Unternehmen, das im Internet aktiv ist: Nutzer-Tracking, Kundendaten, Newsletter oder Werbemails, Werbung auf Facebook, die eigene Datenschutzerklärung, vieles ändert sich durch die Neuregelungen. Im Einzelnen:

2. Datenschutzerklärung und Impressum

Zunächst benötigt jede Webseite eine neue Datenschutzerklärung, die den Vorgaben der DSGVO entspricht. Grundsätze einer DSGVO-konformen Datenschutzerklärung:

- Einfache und verständliche Sprache
- ggf. eine vorgeschaltete, allgemein-zusammenfassende Erklärung
- Kontaktdaten des Seitenbetreibers
- Datenschutzbeauftragter, wenn vorhanden
- Die Rechtsgrundlage der jeweiligen Datenerhebung/Verarbeitung (gesetzliche Regelung oder Einwilligung) muss konkret benannt werden

Die folgenden Punkte muss eine Datenschutzerklärung nach DSGVO mindestens enthalten:

- Nennung aller Datenverarbeitungsvorgänge auf der Webseite
- Umgang Kunden- / Bestelldaten

- Tracking, Cookies, Social Media
- Newsletter, A(D)V
- Dauer der Speicherung, Löschungsfristen
- Auskunft, Berichtigung, Löschung, Widerspruch
- Recht auf Datenherausgabe und Übertragbarkeit

Eine Einwilligung darf nicht innerhalb der Datenschutzerklärung erklärt werden.

Achtung! Löschpflicht Art. 17 DSGVO:

Daten müssen gelöscht werden, wenn:

- der Erhebungszweck weggefallen ist,
- die Einwilligung widerrufen wurde (Newsletter-Abmeldung),
- ein Widerspruch des Nutzers erfolgt („Löschen Sie meine Daten“) und keine gesetzlichen Speicherpflichten entgegenstehen (Steuern und Buchhaltung)

Im Impressum sind keine Änderungen notwendig. Allerdings wird momentan diskutiert, dass für Auskunfts-, Berichtigungs- und Löschungsansprüche ein spezielles Kontaktformular geschaffen werden soll, das in die allgemeine Menüstruktur (bei Datenschutzerklärung und Impressum) integriert werden soll.

3. Verarbeitungsverzeichnis (bisher: Verfahrensverzeichnis)

Sie benötigen ein Verarbeitungsverzeichnis, wenn Sie mehr als 250 Mitarbeiter beschäftigen und wenn Sie besondere Datenkategorien verarbeiten.

Die Pflicht gilt auch für Unternehmen unter 250 Mitarbeitern, wenn die Verarbeitung „nicht nur gelegentlich“ erfolgt. Es ist aber noch nicht abschließend geklärt, was dies genau bedeutet. Bis die Voraussetzungen abschließend geklärt sind, sollten Sie im Zweifel ein solches Verzeichnis anlegen.

Welche Inhalte gehören hinein?

- Angaben des Verantwortlichen
- Name und Kontaktdaten des Verantwortlichen, seines Vertreters und des Datenschutzbeauftragten
- Zwecke der Verarbeitung
- Kategorien betroffener Personen und personenbezogener Daten
- Kategorien von Empfängern
- Übermittlungen von personenbezogenen Daten an ein Drittland
- Fristen für Löschung
- Beschreibung der technischen und organisatorischen Maßnahmen
- Angaben des Auftragsverarbeiters
- Name und Kontaktdaten des Auftragverarbeiters und des Verantwortlichen, ihrer Vertreter und des Datenschutzbeauftragten
- Kategorien von Verarbeitungen
- Übermittlungen von personenbezogenen Daten an ein Drittland

Beispiele und Aufbau eines solchen Verarbeitungsverzeichnis finden Sie z.B. bei der Bitkom:

https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Verarbeitungsverzeichnis-online.pdf

4. Cookies und Tracking

Im Hinblick auf Cookies und Tracking gibt es momentan keine Änderungen. Cookies werden spezifisch durch die ePrivacy-Verordnung (ePV) neu geregelt. Diese kommt allerdings wohl erst 2019.

Die gute Nachricht: Google Analytics bleibt auch nach der DSGVO wie bisher „erlaubt“, wenn folgende Voraussetzungen erfüllt sind:

- A(D)V Vertrag mit Google abgeschlossen
- IP Anonymisierung aktiviert
- Opt-out Möglichkeiten für Desktop und Mobil

Achten Sie darauf, dass Sie ab dem 25. Mai 2018 einen DSGVO-konformen AV-Vertrag mit Google abschließen. Google wird vermutlich demnächst einen solchen Vertrag bereitstellen.

Eine Anleitung plus Tools zur korrekten Umsetzung finden Sie bei eRecht24 Premium.

https://www.e-recht24.de/premium-agenturpartner

Bei anderen Tools wie z.B. dem Facebook Pixel kann man momentan leider keine genaue Aussage treffen.
Allerdings wird die Rechtslage wahrscheinlich komplizierter.

5. Newsletter und Einwilligungen

Einwilligungen von Nutzern, z.B. zum Newsletter-Versand, die bereits nach altem Recht wirksam eingeholt wurden (double opt-in) gelten grundsätzlich weiter.

Ausnahmen:

- Koppelungsverbot bei alten Einwilligungen nicht beachtet
- Einwilligungen durch Minderjährige

Was ist mit neuen Newsletter-Aktionen oder Preisausschreiben?

Wenn keine gesetzliche Erlaubnis zum Speichern / Übertragen von Daten vorhanden ist, wird immer eine Einwilligung benötigt.

Auch unter der DSGVO sollte das double opt-in Prinzip beachtet werden, um die Einwilligung im Zweifel auch nachweisen zu können. Die Einwilligung muss in jedem Fall elektronisch dokumentiert werden.

Die Einwilligung muss dabei „freiwillig“ erfolgen: Echtes Koppelungsverbot in Art. 7 Abs.4 DSGVO.

In der Regel: Keine Daten gegen Inhalte (z.B. E-Books, Gewinnspiele, Checklisten) und keine Koppelung von Newsletter-Versand an Vertragsschluss.

6. Datenschutzbeauftragter

Unternehmen, die in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen oder zu einer Datenschutz-Folgeabschätzung nach Artikel 35 DSGVO verpflichtet sind (Einzelheiten unten bei Ziff. 9.), müssen einen Datenschutzbeauftragten benennen.

Interessenskonflikte

Bei der Besetzung des Datenschutzbeauftragten dürfen keine Interessenkonflikte bestehen. Daher kann ein Vorstandsmitglied, ein Geschäftsführer oder der Unternehmensinhaber nicht Datenschutzbeauftragter sein. Diese Personen können im Fall von Konflikten zwischen den Unternehmensinteressen und den datenschutzrechtlichen Vorschriften nicht vermitteln.

Sie können auch einen externen Datenschutzbeauftragten bestellen, um Konflikte zu vermeiden.

Qualifikationen des Datenschutzbeauftragten

Der Datenschutzbeauftragte muss zuverlässig sein. Juristische sowie technische Fachkunde sind ebenfalls unumgänglich für die Position des Datenschutz- beauftragten. Schulungen/Seminare inkl. Prüfung werden bundesweit angeboten, um die entsprechenden Qualifikationen zu erwerben, z.B. beim TÜV.

7. Mitarbeiterdaten

Mit der DSGVO kommen auch Neuregelungen zum Mitarbeiterdatenschutz. Die neuen Vorschriften enthalten zahlreiche Pflichten und Obliegenheiten, die Arbeitgeber künftig einhalten müssen.

Es sollen nur die Daten erhoben werden, die „erforderlich“ sind.

Mitarbeiterdaten sollen nur dann verarbeitet werden, wenn dies für die Entscheidung über die Einstellung eines Bewerbers oder zur Durchführung, Ausübung oder Beendigung eines Arbeitsverhältnisses erforderlich ist.

Erlaubt ist die Verarbeitung auch dann, wenn sie für die Erfüllung gesetzlicher Rechte und Pflichten, eines Tarifvertrags oder einer Betriebs- oder Dienstvereinbarung oder zum Zwecke der Strafverfolgung erforderlich ist. Ob und wann die Erhebung bestimmter Daten tatsächlich erforderlich ist, muss dabei immer anhand des konkreten Einzelfalls bestimmt werden.

Einwilligungen einholen

Wer sich den rechtlichen Unsicherheiten rund um die „Erforderlichkeit“ entziehen will, kann freiwillig abgegebene Einwilligungen von seinen Arbeitnehmern einholen. Im Streitfall muss eine behauptete Freiwilligkeit der Einwilligung vom Arbeitgeber allerdings nachgewiesen werden.

Eine wirksame Einwilligung muss bestimmte formale Kriterien erfüllen. So muss sie grundsätzlich in Schriftform erfolgen, d. h. eigenständig unterschrieben werden. Da das allerdings nicht immer praktikabel ist, kann unter besonderen Umständen auch eine elektronische Einwilligung eingeholt werden. Zudem muss der Beschäftigte in geeigneter Form darauf hingewiesen werden, dass die Einwilligung jederzeit widerruflich ist. Schlussendlich müssen durch den Arbeitgeber bestimmte Voraussetzungen für die Widerrufserklärung geschaffen werden.

Ein Arbeitgeber muss die Einhaltung der soeben genannten Pflichten im Zweifel nachweisen können (Dokumentationspflichten). Des Weiteren sind Arbeitgeber künftig mit strengeren Informationspflichten bei Datenschutzverstößen und zahlreichen weiteren Pflichten (z.B. Löschungspflichten) konfrontiert.

Arbeitgeber sollten im Hinblick auf diese Pflichten ihre unternehmensinternen Prozesse daher gründlich überprüfen und ggf. anpassen lassen (Stichwort: Compliance-Management).

8. Auftrags(daten)verarbeitung

Wenn das Erheben und Verarbeiten personenbezogener Daten durch ein „externes" Unternehmen erfolgt, muss dies – wie auch im alten Recht – vertraglich geregelt werden.

Beispiele

- Agentur führt Werbemaßnahmen aus
- Externer Newsletter-Anbieter
- Webhoster
- Externe Wartungsverträge

Was ändert sich am Inhalt der A(D)V-Verträge?

Wenige inhaltliche Neuregelungen:

- Auftragsverarbeiter muss u.U. ein Verfahrensverzeichnis führen
- Auftragsverarbeiter muss die Weisungen des Verantwortlichen protokollieren
- keine Schriftform der Verträge mehr notwendig

Woher erhalte ich Muster für meine A(D)V-Verträge?

Einen DSGVO-konformen Mustervertrag finden Sie bei eRecht24 Premium:

https://www.e-recht24.de/premium-agenturpartner

9. Datenschutz bei Minderjährigen

Bei Jugendlichen unter 16 Jahren müssen die Eltern einwilligen. Dies gilt aber nur für Fälle, bei denen die DSGVO eine Einwilligung vorschreibt (z.B. für Werbung) und in der Praxis nur dann, wenn es sich um Angebote handelt, die sich direkt an Kinder und Jugendliche richten.

Bei gemischten Angeboten (für Erwachsene und Jugendliche) sind keine spezifischen Vorgaben umzusetzen.

10. Datenschutz-Folgenabschätzung

In bestimmten Fällen sind Sie verpflichtet, die Folgen der Datenverarbeitung zu bewerten und dies in einer sog. Datenschutz-Folgenabschätzung nach Art. 35 DSGVO festzuhalten. Eine sog. DSFA ist grundsätzlich immer dann durchzuführen, wenn „eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge (hat)".

Dies ist z.B. bei den folgenden Konstellationen der Fall:

- Verarbeitung von Gesundheitsdaten, Religion, Sexualität
- Geschäftsgeheimisse
- Profiling/Scoring
- Strafbare Handlungen
- u.vm.

Wann und wie eine solche Datenschutz-Folgenabschätzung im Detail durchzuführen ist, können Sie im umfangreichen Whitepaper des Forum Privatfreiheit nachlesen:

https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf

11. Einsichtsrecht und Meldepflicht

Generell haben Betroffene Anspruch auf Auskunft zu ihren gespeicherten personenbezogenen Daten (Art. 15 DSGVO).

Form der Auskunft:

- schriftlich
- elektronisch (E-Mail)
- auf Verlangen mündlich

Frist der Auskunft: Unverzüglich, aber spätestens 1 Monat nach Eingang des Antrags

Wann müssen bei Datenpannen die Betroffenen und Aufsichtsbehörden informiert werden?

Hier gelten mittlerweile strengere Anforderungen als bisher. Nach Art 33 DSGVO müssen Datenpannen gegenüber Aufsichtsbehörden unverzüglich (möglichst binnen 72 Stunden) mittels umfassender Dokumentation vorgelegt werden.

Details zum Inhalt regelt Art. 33 Abs. 5 DSGVO

https://dejure.org/gesetze/DSGVO/33.html

12. Bußgelder und Abmahnungen

Datenschutzverstöße können abgemahnt werden!

Bei Verstößen drohen Abmahnungen und Gerichtsverfahren, denn:

- Datenschutzrecht hat wettbewerbsrechtliche Relevanz!
- Verstöße können auch nach der DSGVO abgemahnt werden!

Bußgelder

Die DSGVO sieht Bußgelder bis zu 20 Millionen Euro oder 4% des weltweiten Vorjahresumsatzes vor.

Bisher haben Datenschutzbehörden den oberen Rahmen der Bußgelder nur sehr selten und bei dauerhaften Verstößen ausgereizt.

Das wird sich aber sehr wahrscheinlich ändern, der hohe Bußgeldrahmen ist ein Kernbestandteil der DSGVO.

Wichtig: Anfragen/ Beschwerden von Nutzern ernst nehmen. Noch wichtiger: Anfragen/ Beschwerden von Datenschutzbehörden ernst nehmen.