DIE DSGVO KOMMT – BIST DU VORBEREITET?

Veröffentlicht am 12. April 2018 von Malina

Die DSGVO kommt - bist Du vorbereitet? Der Countdown läuft: Ab dem 25 Mai 2018 sind die Vorgaben der Europäischen Datenschutz Grundverordnung rechtlich bindend! Wir haben uns mit den Neuerungen beschäftigt und geben Dir in unserem Blogartikel einen Überblick plus Checkliste an die Hand.

Zeitlich mehr als passend ist die DSGVO – **die Europäische Datenschutz Grundverordnung** – ab dem 25. Mai 2018 rechtlich bindend. Nach dem **Datenmissbrauchsskandal von Facebook/Camebridge Analytica** gibt es wohl keinen besseren Zeitpunkt, um eine gesetzliche Verordnung über die Verwendung von persönlichen Daten öffentlich zu machen. Auch wenn der Umsetzung der DSGVO eine lange Planungsgeschichte vorausgeht.

Es bleibt nur noch wenig Zeit, um die Vorgaben der EU-DSGVO umzusetzen. Insbesondere kleine und mittelständische Unternehmen wissen oft nicht, was auf sie zukommt. Wir haben uns mit der DSGVO eingehend beschäftigt und zeigen Dir hier auf, was für Neuerungen auf uns zukommen.

WAS IST DIE DSGVO?

Die DSGVO, e**nglisch: General Data Protection Regulation (GDPR),** ist eine **Verordnung der Europäischen Union**. Mit ihr erwarten uns **grundlegende Änderungen des Datenschutzrechts** innerhalb der gesamten EU. Die EU-DSGVO ist bereits am **25. Mai 2016** in Kraft getreten und muss bis spätestens zum **25. Mai 2018** umgesetzt werden. Sie löst die Datenschutzrichtlinie von 1995 ab - die am heutigen Stand des Internets gemessen - überholt ist.

Generelle Ziele der DSGVO sind die **Schaffung eines einheitlichen Rechtsrahmens** hinsichtlich des Datenverkehrs im Internet, der **Schutz von Verbrauchern** vor unseriösen Unternehmen und die bessere **rechtliche**

Verfolgung von Datenrechtsverstößen.

Letztendlich gibt die DSGVO einen Weg vor, wie Unternehmen über die **Verwendung von personenbezogenen Daten** informieren sollen und welche Vorkehrungen für die Einhaltung der **IT-Sicherheit** getroffen werden müssen.

WER MUSS HANDELN?

Jeder **Unternehmer, Online Händler, Webseitenbetreiber** ist betroffen. Allgemeiner: alle Unternehmen, die **personenbezogene Daten von EU-Bürgern** verarbeiten, müssen sich den Neuerungen durch die DSGVO stellen. Das können Daten von Mitarbeitern und von Kunden sein. Ansonsten winken Abmahnungen, Gerichtsverfahren oder sogar hohe **Bußgelder**. Bis zu 20 Millionen Euro, bzw. 4 % des weltweiten Jahresumsatzes des Unternehmens kann als Bußgeld von den **Datenschutzbehörden** veranschlagt werden. Angekündigt wurde eine strengere Überwachung der Datenschutzbedingungen durch die Aufsichtsbehörden. Vor allem Unternehmen, die bisher den Datenschutz vernachlässigt haben, müssen mit aufwendigen Anpassungen rechnen.

WAS SIND PERSONENBEZOGENE DATEN?

Unter personenbezogene Daten fallen **Kunden-, Mitarbeiter- und Nutzerdaten**. Denn hierfür werden Informationen gespeichert, mit denen die **Identität** von Personen erschlossen werden kann.

Darunter fallen unter anderem:

- Name
- Bilder
- Adresse
- IP-Adresse

Hier kannst Du die genaue Begriffsbestimmung zu personenbezogenen Daten der DSGVO nachlesen.

REICHWEITE DER DSGVO

Die Datenschutz-Grundverordnung gilt für **Personen** und **Körperschaften**, die personenbezogene Daten von **EU-Einwohnern** verarbeiten. Die DSGVO ist zwar eine europäische Verordnung, trotzdem greifen ihre Vorgaben auch außerhalb der EU, wenn Daten von EU-Bürgern verarbeitet werden. **Google, Amazon** und **Facebook** beispielsweise fallen demnach auch unter die DSGVO, da sie Daten von EU-Bürgern speichern und verwenden.

BISHERIGER DATENSCHUTZ IN DEUTSCHLAND

Deutschland gilt im internationalen Vergleich bereits als **streng** hinsichtlich des Datenschutzes. Das **Deutsche Bundesdatenschutzgesetz (BDSG)** ist zum Beispiel sehr viel strenger als der Datenschutz in den USA. Es gibt sogar US-Unternehmen, die - um gegenüber ihren Kunden ein Zeichen zu setzen - ihre Daten in deutschen Rechenzentren speichern, welche wiederum dem BDSG unterliegen. Die EU Verordnung zum Datenschutz ist zwar noch strenger, aber viele Bestimmungen sind **erweiterte Fassungen aktueller Vorgaben**. Wer also bisher schon **datenschutzkonform** agiert, sollte mit den Neuerungen keine großen Probleme haben. Experten gehen daher davon aus, dass vor allem deutsche Unternehmen leichter mit der Umstellung auf die DSGVO fertig werden als Unternehmen aus anderen EU-Ländern.

WAS SOLL DIE DSGVO BRINGEN?

Auf einen Blick:

- Mehr **Transparenz** bei der Verarbeitung von Daten durch Unternehmen
- Mehr **Kontrolle** für den Verbraucher über seine persönlichen Daten
- Bessere **Rechteverfolgung** bei Datenrechtsverstößen durch die Aufsichtsbehörden
- Schutz vor **Cyberangriffen** und **Datenklau** durch die Einrichtung von Abwehrmechanismen

WAS BEDEUTET DIE DSGVO FÜR UNTERNEHMER?

Alle Unternehmen, die online unterwegs sind und in irgendeiner Weise mit der Verwendung personenbezogener Daten zu tun haben, müssen sich auf die DSGVO einstellen und selbst prüfen, was sie aufgrund der europäischen Verordnung zutun haben. Sie müssen, um den Ansprüchen der DSGVO zu genügen, ein umfassendes **Konzept zur Sicherung und zum Schutz von Unternehmens- und Kundendaten** entwickeln. Im Falle der Überprüfung durch die Datenschutzaufsichtsbehörden müssen die Maßnahmen zur Sicherung der Daten offengelegt werden. Der Gesetzgeber möchte so unter anderem erreichen, dass Unternehmen sich eingehend mit dem Datenschutz beschäftigen.

UNTERNEHMER MÜSSEN ALSO ZUKÜNFTIG:

- **Datenverarbeitungsprozesse** an die Vorgaben der DSGVO anpassen

- Ihre **Datenverarbeitung dokumentieren** (es besteht eine Dokumentations- und Nachweispflicht) und ein Verzeichnis über ihre Datenverarbeitungen anlegen

- I**nterne Sicherheitsvorkehrungen** zum Schutz von Mitarbeiterdaten und Kundendaten treffen, zum Beispiel Firewalls und Virenscanner zum Schutz der eigenen IT einrichten, wenn diese noch nicht vorhanden sind

Durch die DSGVO besteht für Unternehmen eine **Rechenschaftspflicht** bzw. eine I**nformationspflicht** gegenüber dem Verbraucher. Mit dieser Bürde wollen wir Dich nicht alleine lassen und haben daher die ersten wichtigen Schritte in einer Checkliste für dich zusammengefasst. Einige **Empfehlungen** können wir Dir, aufgrund unserer Erfahrung als **Webdesign- und Werbeagentur**, mit auf den Weg geben. Auch wir haben uns bereits auf die DSGVO eingestellt und auch die Websites unserer Kunden nach bestem Wissen und Gewissen vorbereitet - dazu gleich noch mehr.

DSGVO CHECKLISTE

- Die DSGVO ordnet an, dass Unternehmen ihre Rechtsgrundlage für die Verarbeitung von

personenbezogenen Daten offenlegen. Diese muss auch in Deiner **Datenschutzerklärung** vermerkt sein. Wie Du Deine Datenschutzerklärung an die Ansprüche der DSGVO anpasst, erfährst Du gleich. Also fürs erste: **Überprüfe und dokumentiere die Rechtsgrundlage** auf der Du personenbezogene Daten sammelst.

- Richte ein Verzeichnis der Verarbeitungstätigkeiten ein.

- Bereite Dich auf mögliche **Anfragen von Nutzern** vor, die der DSGVO zufolge das Recht haben, unentgeltlich Auskunft über ihre gesammelten persönlichen Daten zu bekommen. Bestimme dazu am besten einen Prozess für die Beantwortung solcher Anfragen.

- Überprüfe, ob Dein Unternehmen dazu verpflichtet ist einen **Datenschutzbeauftragten** zu benennen. Vor allem **Unternehmen des öffentlichen Sektors** müssen, da sie mit sensiblen Personendaten zu tun haben, einen Datenschutzbeauftragten vorweisen. Der Datenschutzbeauftragte ist verantwortlich für die Einhaltung der Datenschutz Regelungen durch das Unternehmen. Dieser kann sowohl ein interner Mitarbeiter als auch ein externer Berater sein. Natürlich sollte er oder sie die notwendigen Kompetenzen besitzen.

- Dokumentiere Deinen Umgang mit persönlichen Daten.

- Prüfe, ob Du den Schutz der persönlichen Daten im Sinne der DSGVO einhalten kannst. Wenn Du unsicher bist, dann hole Dir am besten einen rechtlich geschulten Fachmann an Deine Seite.

Dies sind generelle Punkte, die mit der DSGVO auf Dich zukommen. Für die juristische Absicherung der rechtlichen Hinweise und Webseiteninhalte empfehlen wir unseren Partnern, diese durch einen Rechtsanwalt prüfen zu lassen. Ebenfalls sollten branchenspezifische Vorgaben, die mit Inkrafttreten der DSGVO zu beachten sind, ermittelt werden.

Ein sehr wichtiges To Do innerhalb der Checkliste ist die **Anpassung der Datenschutzerklärung** auf Deiner Website. Denn: So gut wie jede Website braucht spätestens ab dem 25. Mai 2018 eine neue Datenschutzerklärung!

WAS IST EINE DATENSCHUTZERKLÄRUNG?

Eine Datenschutzerklärung auf einer Website ist eine **Erklärung über die Verwendung von Daten**. Häufig ist sie im unteren Teil einer Website verlinkt. Der **Link** führt auf eine Unterseite, die die Datenschutzerklärung enthält.

Natürlich verfügst Du als Inhaber eines Unternehmens bereits über einen professionellen Webauftritt und damit hoffentlich auch über eine Datenschutzerklärung auf Deiner Website - diese ist schließlich schon länger obligatorisch. In der Regel schenken wir dieser eintönigen Datenschutzseite beim Besuch einer Website nicht besonders viel Aufmerksamkeit. Es besteht allerdings eine Pflicht zur Einbindung von Datenschutzerklärungen auf einer Website, diese ergibt sich aus **§ 13 des Telemediengesetzes (TMG)** – eine der bislang zentralen **Richtlinien des Internetrechts**. Demnach muss der Inhaber einer Website den Nutzer über die **Art, den Umfang und den Zweck der Datenspeicherung** sowie die eventuelle Weitergabe von Daten informieren.

DIE DATENSCHUTZERKLÄRUNG NACH DER DSGVO

Update Datenschutzerklärungen Website – wie sieht diese nach den **Neuerungen** der DSGVO aus?

Die DSGVO hat einen **Anwendungsvorrang** gegenüber der datenschutzrechtlichen **Vorgaben des TMG**. Eine fehlerhafte Datenschutzerklärung auf Deiner Website kann daher nach dem **25. Mai 2018** teuer werden. Es ist also ganz besonders wichtig, gründlich bei der Erstellung einer **Datenschutzerklärung** Deiner Website vorzugehen.

Die **DSGVO-konforme Datenschutzerklärung** muss unter anderem diese Angaben enthalten:

- **Aufklärung** über die Rechte der Personen, deren Daten verarbeitet werden
- Erklärung zur **Verwendung von Cookies**
- Speicherort und Art der **Information**
- Erklärung von Sicherheitsmaßnahmen zur **Datenverschlüsselung**

Das sind die Rechte der Personen, deren Daten Du verarbeitest und auf die Du in der Datenschutzseite eingehen musst:

- Auskunftsrecht
- Recht auf Vergessenwerden
- Recht auf Datenübertragbarkeit

Mit Hinweis auf das **Auskunftsrecht** muss in der Datenschutzerklärung einer Website versichert werden, dass Personen, deren Daten gespeichert wurden (zum Beispiel Besucher einer Website), jederzeit das Recht auf Auskunft haben. Bei Anfrage muss dementsprechend Auskunft gegeben werden über:

- die **Herkunft** der gespeicherten Daten
- den **Empfänger** der gespeicherten Daten
- der **Zweck** der Datenverarbeitung

Wenn Du solch eine Anfrage erhalten solltest, musst Du in der Lage sein diese innerhalb eines Monats mit entsprechenden Informationen zu beantworten. Die anfragende Person kann zudem auch eine
Kopie ihrer gespeicherten Daten verlangen. Unvorbereitet ist dies eine aufwendige Aktion, die im regulären Unternehmensalltag viel Arbeitskraft in Anspruch nimmt. Daher solltest Du auf Systeme setzen, die bereits eine **Auskunftsfunktion** haben und Daten, über die Auskunft gegeben werden muss, kennzeichnen. Natürlich musst Du auch prüfen, ob der Antragsteller berechtigt ist, eine Auskunft zu erhalten.

Das **Recht auf Vergessenwerden** bedeutet, dass eine Person, deren Daten Du gespeichert hast, zum Beispiel eine Emailadresse für einen Newsletter, das Recht hat eine Löschung dieser persönlichen Daten zu fordern. In dem Zuge musst Du dafür sorgen, dass die Emailadresse unwiderruflich entfernt wird.

Das
Recht auf Datenübertragbarkeit bedeutet, dass Personen, die Deinem Unternehmen Daten von sich bereitgestellt haben, zum Beispiel Patientendaten, das Recht auf die Weitergabe an Dritte haben. Die betroffene Person kann entscheiden, dass Du seine Daten an eine andere Arztpraxis weitergeben musst.

Grundsätzlich gilt: die Datenschutzerklärung muss vor allem in einfacher und verständlicher Sprache verfasst sein. Jeder soll verstehen können, was mit seinen hinterlassenen Daten, passiert.

Die DSGVO bringt viele Neuerungen mit sich und wirft einige Fragen auf. Unter anderem stellt sich die Frage, ob der **Cookie Hinweis auf der eigenen Website** angepasst werden muss. Schließlich fallen Cookies der DSGVO zufolge auch unter **personenbezogene Daten**.

WAS SIND COOKIES?

Cookies sind **Textdateien**, die angelegt werden, wenn Du zum Beispiel eine Website besuchst. Sie ermöglichen es nachzuvollziehen, welche Websites ein Nutzer besucht hat. Für **Online Händler und Marketer** ist dies wichtig, um passende **Werbung** - zum Beispiel bestimmte **Anzeigen** - auszuspielen.

Es gibt verschiedene Arten von Cookies. Diese jetzt alle aufzuführen und zu erklären würde den Rahmen hier sprengen. Für uns ist hinsichtlich der datenschutzrechtlichen Neuerungen durch die DSGVO wichtig, dass **Cookies als personenbezogene Daten** angesehen werden, da diese Informationen zu Webseiten Besuchern speichern. Diese Informationen können zur Identifikation der Person genutzt werden, wie zum Beispiel die IP-Adresse.

Cookies sind wie Fußabdrücke - nur nicht am Strand, sondern in den Weiten des Internets

DER COOKIE-HINWEIS AUF DEINER WEBSITE

In der Praxis wird oftmals über einen **Banner** auf die Verwendung von Cookies hingewiesen. So einen Banner hast Du sicher selbst auf Deiner Website implementiert oder zumindest schon oft beim Besuch einer Website gesehen hast. Wir haben ebenfalls solch einen Banner bei uns untergebracht.

Die Hinweise fallen teilweise unterschiedlich aus. Die **Verwendung von Cookies** und die vorgeschriebenen Regelungen des Gesetzgebers dazu waren schon immer eher verwirrend. Sie werden über **die datenschutzrechtlichen** Regelungen des deutschen Telemediengesetzes (TMG) vorgegeben.

Bereits seit dem 25.11.2009 gibt es zudem eine **Cookie Richtlinie der EU**, die vorschreibt, dass eine

Einwilligung des Nutzers über die Verwendung von Cookies eingeholt werden muss. Deutschland hat allerdings im Gegensatz zu anderen EU-Ländern, diese **Cookie Richtlinie** nicht als nationales Recht angenommen. Daher galt in Deutschland bisher weiterhin **§ 15 Abs. 3 Telemediengesetz (TMG)**.

Demzufolge muss der Nutzer **aktiv widersprechen**, dass Cookies bei seinem Webseiten-Besuch verwendet werden. Dieses Widerspruchsrecht gegen die Verwendung von Cookies wird auch als **Opt-Out Verfahren** bezeichnet. Eine andere Methode ist das **Opt-In Verfahren:** bei diesem werden Nutzer erst umfassend informiert und dann müssen sie aktiv eine Einverständniserklärung zur Cookie Nutzung abgeben. Die Opt-In Regelung wird in vielen anderen EU-Mitgliedsstaaten angewendet. Mit der DSGVO soll eine Vereinheitlichung geschaffen werden, die die Vorgaben zur Cookie-Pflicht für alle Länder gleich behandelt.

COOKIE HINWEIS – GIBT ES ÄNDERUNGEN?

Die DSGVO hat einen **Anwendungsvorrang** gegenüber der datenschutzrechtlichen Vorgaben des TMG. Trotzdem bleibt nach Auslegung der DSGVO von Spezialisten hinsichtlich der Verwendung von Cookies fast alles wie bisher. Du muss den Webseiten Besucher über einen Banner darauf hinweisen, dass **Cookies zum Tracking und zur Analyse** von Daten verwendet werden und dass, der Besucher sich durch die Nutzung der Website damit einverstanden erkären. Zusätzlich müssen Unternehmer jedoch ihre Datenschutzerklärungen auf die DSGVO ausrichten und darin die Verwendung von Cookies erklären. Dazu muss Art. 6 Abs. 1 lit f DSGVO berücksichtigt werden.

MERKE: Zukünftig ist es weiterhin ausreichend, den Webseiten Besucher über einen Banner darauf hinzuweisen, dass Cookies zum Tracking und zur Analyse von Daten verwendet werden. Natürlich solltest Du, wenn nicht bereits getan, Deine Datenschutzseite den Bedingungen der DSGVO anpassen und damit auch den Hinweis auf die Cookie-Nutzung darin unterbringen. Um vollends auf der sicheren Seite zu sein, empfiehlt es sich einen Rechtsberater an Bord zu holen. Außerdem gilt es zu beobachten, was sich hinsichtlich der **ePrivacy-Verordnung** für Änderungen auf uns zukommen – diese sollte ursprünglich mit der DSGVO umgesetzt werden und diese ergänzen. Bei der ePrivacy-Verordnung geht es um Regelungen zum **Schutz der Privatsphäre in der digitalen Kommunikation** und die **Regulierung kommerzielle Verarbeitung von Kommunikationsdaten**. Doch die EU konnte sich hinsichtlich der genauen Vorgaben der Verordnung noch nicht einigen.

FAZIT

Die Neuregelungen der DSGVO sind, betrachtet man die rasante Weiterentwicklung der digitalen

Technologien, unerlässlich. Die Regelungen der Verordnung richten sich daher nach dem aktuellen Stand der Technik.

Einerseits wirkt die DSGVO natürlich wie ein **bürokratisches Monster**, das uns bei der Dokumentation von Datenverarbeitungsprozessen den Aufwand erschweren kann. Andererseits besteht für Unternehmer aber hier auch die Möglichkeit, das **Vertrauen ihrer Kunden** zu stärken. Vor allem nach dem aktuellen Datenskandal kann ein Unternehmen, das einen verantwortungsvollen Umgang mit persönlichen Daten zeigt, seinen Kunden mehr **Sicherheit** geben. Wenn der Besucher Deiner Website möchte, kann er zukünftig mehr Antworten auf seine möglichen Fragen finden: Wie werden meine Daten verarbeitet? Wo werden die Daten gespeichert? Wofür werden Daten erfasst? Will ich, dass meine Daten erfasst werden?

Wichtig ist, jetzt nicht in **Panik** zu verfallen, sondern Schritt für Schritt vorzugehen und die **organisatorischen, rechtlichen und technischen Änderungen**, die notwendig sind, umzusetzen. Ein Pluspunkt ist es schon mal wenn Du gut vorbereitete Partner hast, die im Sinne des Datenschutzes verantwortungsvoll handeln.

Kontakt aufnehmen

Lichtblick: Zum Glück deckt die aktuelle Rechtslage des deutsches **Bundesdatenschutzgesetzes (BDSG)** schon einiges ab – wer hier also bisher gewissenhaft der Rechtsnorm gefolgt ist, braucht sich keine großen Sorgen machen. Um auf Nummer sicher zu gehen und branchenspezifische Regelungen der DSGVO zu berücksichtigen, empfehlen wir einen fachlichen Berater hinzuzuziehen.