Das Monster mit den vielen Buchstaben EU-DSGVO

Für mein Business, Geschäft, Praxis, Gaststätte?

Ja, denn das neue Monster Datenschutz betrifft jedes Unternehmen, und zwar unabhängig vom Umsatz oder der Anzahl der Beschäftigten.

Was ist neu? Was muss beachtet werden?

Unterrichtungspflicht:

Die DSGVO gibt vor, dass Daten nur verarbeitet werden dürfen, wenn auch eine rechtliche Grundlage besteht, beziehungsweise das Unternehmen die Einwilligung der betroffenen Person hat. Unternehmen werden nun beweispflichtig, dass die Daten rechtmäßig verarbeitet werden. Kunden, vor allem Neukunden, muss Folgendes klar dargestellt werden:

- Wofür werden Ihre Daten verwendet?
- Wo und wie lange werden Sie gespeichert?
- An wen werden Sie übermittelt? (vor allem bei Leistungsträgern / Lieferanten außerhalb der EU)
- Wie kann der Kunde seine Daten erhalten, berichtigen, einschränken oder löschen lassen?

Dokumentations- und Nachweispflicht: Alle personenbezogenen Datenverarbeitstätigkeiten müssen im Betrieb sorgfältig Dokumentiert werden und jederzeit auf Verlagen der Datenschutzbehörde vorgelegt werden. Es muss gewährleistet sein, das bei Änderung der IT eine Anpassung des Verfahrensübersicht erfolgt, ggf. schon bei einem WordPress[1] Update.

1 https://business-view.photo/?p=3699

Verfahrensverzeichnis: Welche Mitarbeiter, externe Dienstleister / Erfüllungsgehilfen und so weiter haben in welchem Umfang Zugriff auf die Daten? In welcher Verbindung stehen Sie zueinander?

Plicht zur Selbstanzeige: Hackerangriffe auf den Daten Server / Computer müssen sofort der zuständigen Landesdatenschutzbehörde[2] gemeldet werden.

Daten außer der EU: Wer Daten außerhalb der EU übermittelt, muss sicherstellen, dass die Informationen dort nach dem Standard der EU-DSGVO behandelt werden. Bei Verstößen des Dienstleisters kann man selbst in Haftung genommen werden!

Subunternehmer: Auch Subunternehmer wie Beispielweise Mailing-Dienste, müssen nach den neuen Richtlinien arbeiten, dieses muss bei Erteilung des Auftrages durch den Auftraggeber überprüft werden.

Recht auf Vergessen werden: Da gibt es zwar schon länger, nun wird es verschärft! Die Fristen zum Löschen personenbezogener Daten müssen unbedingt eingehalten werden, am besten durch eine Automatik im System (Datenbank, CRM, Buchhaltung etc.)

Datenschutz durch Technikgestaltung: Neue Produkte (Hardware & Software) müssen bereits in der Gestaltung den Prinzipien des Datenschutzes folgen. So muss zum Beispiel Software per Voreinstellung datenschutzfreundlich sein.

Informationspflichten gegenüber Betroffenen (Kunden & Lieferanten): Im Besonderen das Recht auf Datenportabiliät. Unternehmen müssen betroffenen Personen ihre Daten in einem maschinenlesbaren, gängigen Format aushändigen können, um Kunden so den Weg zu einem anderen Unternehmen zu erleichtern.

Datenschutzbeauftrage (DSB)

Eine solche Person muss jedes Unternehmen mit mindestens zehn Mitarbeitern benennen, kann aber auch darunter gelten, wenn die Daten einer Vorkontrolle unterliegen. Zu den beschäftigten zählen zum Beispiel Inhaber, Mitarbeiter, und alle Personen die evtl. mit Kunden- oder Mitarbeiterdaten in Kontakt kommen könnten. Im Zweifelsfall also auch das externe Reinigungspersonal, das die Mülleimer leert, oder der Hausmeister der die Lampe repariert.

Aktuell zum Beispiel, prüft die Datenschutz Aufsichtsbehörde Niedersachsen ob Reisebüros nicht grundsätzlich einen DSB benötigen, da diese ständig Daten an Dritte übermitteln. (Veranstalter, Hotels, Airlines usw.)

Der DSB kann ein Mitarbeiter oder ein externer Dienstleister sein. Datenschutzbeauftragte müssen Fachkunde nachweisen, Zuverlässig (keine Interessenkonflikte) und müssen sich regelmäßig weiterbilden. Der Geschäftsführer kann nicht gleichzeitig Datenschutzbeauftragter sein, wegen Interessenkonflikt.

Datenpanne? Was nun?

Es wird teuer, oder sehr teuer! Verletzungen gegen die EU-DSGVO können mit einer Strafe bis zu 4% des Jahresumsatzes geahndet werden. Die Strafe fällt allerdings deutlich Milder aus, wenn man

2 https://www.datenschutz-wiki.de/Aufsichtsbehörden_und_Landesdatenschutzbeauftragte

eine Selbstanzeige macht.

Wichtig: Im Zweifelsfall muss nicht der Kunde nachweisen, das mit seinen Daten nicht sorgfältig Umgegangen wurde, sondern der Unternehmer, dass er datenschutzkonform gearbeitet hat!

Wie sorge ich für Datensicherheit

Alle personenbezogenen Daten von Kunden und Mitarbeitern (auch Name oder E-Mail Adresse), egal ob auf Papier, PC oder Microfilm, müssen stärker als bisher, vor dem Zugriff Unbefugter geschützt werden.

Daten die nicht mehr benötigt werden, müssen vollständig gelöscht werden! Das gilt auch für Daten die mit einem Mindesthaltbarkeitsdatum (MHD) versehen und nach einer bestimmten Zeit gelöscht werden müssen. Papier Schreddern, auf elektronischen Datenträger, auch in Backups, unwiderruflich Löschen.

Alle Mitarbeiten des Unternehmens (Intern, Extern, Teilzeit), müssen über die Datenschutzverordnung in Kenntnis gesetzt und entsprechend geschult werden. Sie müssen eine entsprechende Erklärung unterschreiben, dass sie sich an die Datenschutz Vorschriften halten, und am besten auch bekanntgewordene Verstöße direkt an den DSB melden.

ePrivacy Verordnung (ePV)

Die ePrivacy Verordnung (ePV) baut auf der EU-DSGVO auf und soll deren Regelungsbereich spezifisch ergänzen. Sie soll die Vertraulichkeit in der elektronischen Kommunikation sicherstellen und den Umgang mit personengezogenen Daten im Online-Bereich regeln.

Nach aktuellem Stand tritt die ePV voraussichtlich zusammen mit der EU-DSGVO am 25. Mai 2018 in Kraft und erweitert deren Regelungswerk. Jeder datenbasierte Informationsaustausch ist betroffen, auch von Rechner zu Rechner.

Kontrolle über die Daten: Der Nutzer muss der Verwendung seiner Daten ausdrücklich zustimmen (Opt-in), nur dann dürfen Cookies oder andere Identifier eingesetzt werden.

Privacy Einstellung im Browser: Es ist zu erwarten, dass die Browserhersteller Lösungen für die ePV in ihren Browsern bereitstellen werden. Die wird aber nur Funktionieren, wenn der Browser up-to-date[3] ist!

DSGVO-Check für Ihr Unternehmen

Auch kleinere Online-Händler müssen ab 25. Mai 2018[4] laut Datenschutz-Grundverordnung, ein Verzeichnis der Verarbeitungstätigkeiten führen, um die Einhaltung der Vorgaben der Datenschutz-Grundverordnung nachzuweisen.

> Schon der Empfang von E-Mails, gehört zur Datenverarbeitung und damit zum Datenschutz.

3 https://business-view.photo/panoeditor/wuerden-sie-ohne-schutz-durch-ein-minenfeld-laufen/
4 https://business-view.photo/kalender-messen-events/

Die neue Datenschutz-Grundverordnung der EU (DSGVO) umfasst viele Regelungen bezüglich der Sammlung, Speicherung und Nutzung personenbezogener Daten. Wir empfehlen die einfachen vier Punkte durchzuarbeiten, damit Sie wissen, was zu tuen, was noch zu tuen ist – damit Sie keine Böse Überraschung 2018 erleben.

1. Von Microsoft Deutschland gibt es einen Test, 9 Fragen um zu wissen wo Sie stehen DSGVO-Check[5]
2. Das Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) hat eine DS-GVO – Selbsteinschätzung[6], bei dem man sich spielerisch auf eine Reise durch Datenschutz-Europa begeben kann.
3. Und so langsam wird es ernst, mit dem Fragebogen zur Umsetzung der DS-GVO zum 25. Mai 2018[7], als PDF Datei.
4. Vom Rechtsanwalt Max-Lion Keller, LL.M. (IT-Recht), erklärt das Verfahrensverzeichnis[8], welches Online-Händler nach künftiger Datenschutz-Grundverordnung vorweisen müssen

Cloud / Webspace

Abbildung 1: Cloud

© shutterstock 105420140

Quelle: DEin halbfertiges Fotobuch[9] - ISBN 9783737523387

Unter Cloud Computing (deutsch etwa: Rechnen in der Wolke) versteht man das Speichern von Daten in einem entfernten Rechenzentrum beziehungsweise Festplatte (umgangssprachlich: „Ich lade das Bild mal in die Cloud hoch.“), aber auch die Ausführung von Programmen, die nicht auf dem lokalen Rechner installiert sind, sondern eben in der (metaphorischen) Wolke (englisch cloud).

Der Zugriff auf die entfernten Systeme erfolgt über ein Netzwerk, beispielsweise das des Internet. Es gibt aber im Kontext von Firmen auch sogenannte „Private Clouds“, bei denen die Bereitstellung über ein firmeninternes Intranet erfolgt.

Daten fallen nicht in den Anwendungsbereich des Bundesdatenschutzgesetzes (BDSG), falls sie keinen Personenbezug aufweisen. Dies gilt etwa für statistische Auswertungen, technische Zeichnungen oder Warenverzeichnisse. Derartige Informationen können ohne datenschutzrechtliche Probleme auf jedem System verarbeitet und gespeichert werden, also auch in der Cloud.

Wenn personenbezogene Daten Dritter in die Cloud gegeben werden, müssen sich beispielsweise deutsche Auftraggeber vorab und anschließend regelmäßig nachvollziehbar vor Ort in der Cloud davon überzeugen, dass die Vorgaben des Bundesdatenschutzgesetzes eingehalten werden. Weil namhafte Cloud-Anbieter Datenbestände ihrer Kunden weitergeben, drohen den Kunden Bußgelder. Cloud-Betreiber mit Sitz in den USA unterliegen dem US-Recht und demnach dem Patriot Act. Unternehmen mit Sitz in den USA sind deshalb gezwungen, auch Daten an amerikanische Behörden auszuliefern, die sich auf Servern in fremdem Hoheitsbereich befinden. Dies ist beispielsweise von **Amazon**, **Microsoft** und **Google** bestätigt worden.

Aber meistens fängt es ja gerade mit dem gemeinsamen Kalender und Adressbuch an. Grundsätzlich gilt, dass das BDSG greift, sobald es sich bei den genutzten Inhalten um

5 https://www.microsoft.com/de-de/aktion/IT-Sicherheit/dsgvo-check-wizard.aspx
6 https://www.lda.bayern.de/tool/start.html
7 https://business-view.photo/wp-content/uploads/2017/12/dsgvo_fragebogen.pdf
8 https://www.it-recht-kanzlei.de/verfahrensverzeichnis-datenschutzgrundverordnung.html
9 https://business-view.photo/?p=10108

personenbezogene Daten handelt, also "Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". Ein Verstoß liegt folglich bereits vor, wenn die Sekretärin eines Fotografen ihrem Chef Termine mit Adressen und Telefonnummern der Kunden in den Google-Kalender einträgt oder ihm die Daten per Mail an seinen Google-Mail-Account schickt.

Lässt man fremde Daten von externen Anbietern verarbeiten, handelt es sich dabei üblicherweise um eine sogenannte Auftragsdatenverarbeitung. §11 BDSG.

BDSG §9 (Technische und organisatorische Maßnahmen)

> Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

http://www.gesetze-im-internet.de/bdsg_1990/__9.html *spiegel.de*

Weitere Informationen: www.spiegel.de/netzwelt/web/cloud-dienste-datenschutz-in-der-wolke-a-783446.html

Service	Beschreibung / Link	Onlinespeicher / Preise		Bemerkungen
flickr	www.flickr.com/photos/detlevmolitor	1 TB	./.	
Dropbox	Pro geworbenen Freud, gibt es 50MB Onlinespeicher Gratis dazu[10] https://business-view.photo/go/dropbox/	2 GB		Durch persönliche Links können Dateien und Order freigegeben werden.
		1 TB	9,99 EUR/mtl	
Google Drive	http://drive.google.com/	15 GB	./.	Google Drive unterstützt über 30 verschiedene Dateiformate, die direkt im Browser geöffnet werden können. Dazu zählen neben den Google-eigenen Dateitypen etwa auch Photoshops .PSD, PDF oder Video
		100 GB	1,99 $/Monat	
		1 TB	9,99 $/Monat	
		10 TB	99,99 $/Monat	
		20 TB	199,99 $/Monat	
		30 TB	299,99 $/Monat	

10 Bieten Sie Ihren Kunden, doch den Express Service, keine Versandzeit an. Senden Sie dem Kunden Ihren Werbelink zu Dropbox, dieser Meldet sich an, und erstellt ein Verzeichnis (Firmenname / Kd.-Nr. / Re.-Nr.) und gibt Ihnen dieses Frei. So können Sie die bearbeiteten Fotos bequem Übertragen und haben 50MB mehr Onlinespeicher.

Wuala	www.wuala.com	5 GB	./.	Daten werden vor Upload ins Internet verschlüsselt [11]
SkyDrive	https://onedrive.live.com/	7 GB	./.	Cloud-Speicher von Microsoft[12]
iCloud		5 GB	./.	
		20 GB	1 EUR/mtl.	
		200 GB	4 EUR/mtl.	
↓ Europäische / Deutsche Services ↓				
Telekom Cloud	www.telekom.de/telekomcloud	25 GB	./.	Zur Nutzung ist es nicht nötig Kunde der Telekom sind
HiDrive	https://business-view.photo/go/onlinespeicher/	500 GB	14,90 EUR/mtl.	30 Tage kostenlos testen
ownCloud	www.owncloud.org	./.	./.	Hier betreiben Sie Ihre eigene Cloud-Festplatte. Sie benötigen nur Internet-Speicherplatz, sogenannten Webspace.
SWINDI	www.swindi.de			Fotograf erstellt ein Album, mit Login, Bearbeiter brauchen nur einen Link um zusätzliche Fotos hochzuladen. Fotograf muss die Fotos freigeben
Fotoalbum	www.business-view.photo/?p=12462	./.	./.	Für den/die Private eigene Webseite

Tabelle 1: Cloud / Webspeicher (Stand Okt. 2017)

Mehr Informationen

#Datenschutz - https://business-view.photo/?p=13358

Wir halten Sie auf dem laufenden, mit unserem Newsletter.

Rechtliche Informationen

Bei „Links“ handelt es sich stets um „lebende“ (dynamische) Verweisungen. Der/die Autor(en) hat bei der erstmaligen Verknüpfung zwar den fremden Inhalt daraufhin überprüft, ob durch ihn eine mögliche zivilrechtliche oder strafrechtliche Verantwortlichkeit ausgelöst wird. Er überprüft aber

11 Bei Dropbox & Co. benötigen Sie Zusatz-Software wie BoxCryptor, um Ihre Daten zu verschlüsseln. (www.boxcryptor.com)
12 Microsoft arbeitet in Deutschland, seit 2015, mit der Telekom zusammen, und will so eine „deutsche“ Lösung anbieten

die Inhalte, auf die er in seinem Angebot verweist, nicht ständig auf Veränderungen, die eine Verantwortlichkeit neu begründen könnten. Wenn feststellt wird oder von anderen darauf hingewiesen wird, dass ein konkretes Angebot, zu dem er einen Link bereitgestellt hat, eine zivil- oder strafrechtliche Verantwortlichkeit auslöst, wird der Verweis auf dieses Angebot aufgehoben.

Gerichtsurteile und rechtliches dienen nur Informationszwecken und erheben keinen Anspruch auf Vollständigkeit. Die Artikel / Links zu Recht und verwandten Themen dienen der allgemeinen Bildung und Weiterbildung und nicht der Beratung im Falle eines individuellen rechtlichen Anliegens. Wie alle Projektbereiche sind sie ständigen Veränderungen unterworfen. Diese Artikel / Links entstehen offen und ohne redaktionelle Begleitung und Kontrolle. Es ist möglich, dass Sie hier auf unrichtige, unvollständige, veraltete, widersprüchliche, in falschem Zusammenhang stehende oder verkürzte Angaben treffen. Das gilt auch für Texte auf Diskussions[13]-, Hilfe– und sonstigen Internet Seiten, zu dieser Publikation.

Inhaltsverzeichnis

13 https://business-view.photo/diskussionen-kommentare/