

1 Monat DeEsGeVauO

Sehr geehrte Leser,

wir haben Ihnen wieder aktuelle Informationen zum Datenschutz, gerade in Bezug auf die Umsetzung der DSGVO, zusammengefasst und wollen Ihnen einen Eindruck der aktuellen Situation nach einem Monat DSGVO vermitteln...

Während die Politik nur langsam einsieht, dass die DSGVO zwar gut gemeint und sinnvoll ist, aber letztlich zu viele offene Fragen hinterlassen hat, haben erste Abmahner ihre Angriffsfläche entdeckt und versuchen diese zu nutzen. Da hilft es dann auch nur begrenzt, dass die Aufsichtsbehörden 2018 keine Bußgelder verhängen wollen, ächzen diese doch auch unter der Last der DSGVO und können derzeit selbst kaum Antworten liefern. Noch dazu leiden die Unternehmen darunter, dass die Aufsichtsbehörden der Länder sich nur in wenigen Punkten wirklich einig sind. Leider führt diese Einigkeit dann zeitweise auch dazu, dass es für die, die die DSGVO umsetzen müssen, eher noch unübersichtlicher wird, was die aktuelle Problematik in Bezug auf die Nutzung von Google-Diensten zeigt.

Irgendwo dazwischen stehen wir – die Datenschützer. Zum einen ist es unsere Aufgabe die Meinung und die Gedanken der Aufsichtsbehörden und der Politik zu verstehen, damit wir den Unternehmen eine sinnvolle Antwort auf die vielen Fragen geben können, die uns täglich erreichen. Auf der anderen Seite müssen wir leider zu oft darauf hinweisen, dass dies unsere aktuelle Interpretation und Auslegung der Regeln der DSGVO ist, die auf Basis von gründlichen Überlegungen und Recherchen gebildet wurde. Auch wir können derzeit in vielen Situationen nur davon ausgehen, was der Gesetzgeber mit den jeweiligen Regelungen bezweckt und wie man dieses Ziel in der Praxis erreichen kann.

Wie bereits in unserer letzten Information angemerkt: „Es wohl noch einige Zeit dauern, bis in das Thema Datenschutz etwas Ruhe einkehren wird, derzeit sind einfach noch zu viele Fragen ungeklärt.“

Aber auch wir bitten um Verständnis, dass die Antwort nicht immer aus dem Ärmel geschüttelt werden kann und im Moment viele Punkte unklar und offen sind. Auch für uns heißt es täglich: Viele Recherchen, viele Interpretationen, viele Abwägungen und viele neue Herausforderungen. Daher kann die Beantwortung einer (An-)Frage auch mal ein paar Tage Zeit in Anspruch nehmen.

Wir bleiben für Sie am Ball und werden Sie auch weiterhin in regelmäßiger Form über Neuerungen informieren. Zudem stehen wir Ihnen auch weiterhin gerne mit Rat und Tat zur Seite.

Aktuelle Entwicklungen im Datenschutz / 07-2018

IHRE DATENSCHUTZBEAUFTRAGTEN

INHALTSVERZEICHNIS

1 Monat DeEsGeVauO.....	1
PRE 25.05.2018 - Panik im Land	3
POST 25.05.2018 – Der Tag X ist vorüber	3
Abmahnungen?	3
Ist denn nun alles klar?.....	3
Google Analytics – nur noch mit Einwilligung?!.....	4
Google Fonts – vom Google-Server oder lokal hosten?	4
Cookies – es hört nicht auf... ..	4
Facebook und co. – soziale Medien als Plugin	5
keine aktuelle Datenschutzerklärung – jetzt aber schnell... ..	5
Fehlende Verschlüsselung in der Datenübertragung.....	5
Facebook (nochmal): Verantwortung für die Fanpage	5
Benötigen Kontaktformulare eine Checkbox für den Datenschutz?	6
War es das jetzt?	7
Wann muss ich informieren?	7
Dauerthema: Erstkontakt am Telefon... ..	7
Womit beschäftigen wir uns aktuell sonst noch?	8
Womit können Sie schon mal beginnen?.....	8

Aktuelle Entwicklungen im Datenschutz / 07-2018

IHRE DATENSCHUTZBEAUFTRAGTEN

PRE 25.05.2018 - PANIK IM LAND

Die DSGVO hat bereits im Vorfeld für Panik bei Unternehmen und Vereinen gesorgt. Kurz vor Scharfschaltung der neuen Regelungen sind immer neuen Katastrophenmeldungen auf dem Tisch gelandet. Fotografen, die nicht mehr frei arbeiten dürfen, Textänderungen am Gesetzestext kurz vor Schluss und viele andere Unsicherheiten hielten die Unternehmen und damit uns, die Datenschützer, im Würgegriff. Unser Bestreben war es immer schon den Unternehmen die Panik zu nehmen.

POST 25.05.2018 – DER TAG X IST VORÜBER

Was sollen wir sagen: Die Welt hat sich auch nach dem 25.05.2018 weiter gedreht. Lediglich bei unserem Mailserver hatten wir zeitweise die Befürchtung, dass dieser unter der immensen Flut an Nachrichten am Ende alle Viere von sich streckt. Diese Flut an Anfragen hat auch uns in die Knie gezwungen – aber wir beißen uns durch und tragen den Berg Stück für Stück ab.

Aber auch den Aufsichtsbehörden geht es nicht anders¹. Auch diese haben aktuell mehr zu tun, als sie bewältigen können. Unternehmen, Datenschützer und Aufsichtsbehörden – alle kämpfen mit der DSGVO und den letztlich offenen Interpretationsspielräumen...

ABMAHNUNGEN?

Die Angst vor Abmahnungen von Mitbewerbern war groß. Immerhin war dies eines der größten für die Unternehmen greifbaren Risiken, die mit der Einführung der DSGVO einhergingen.

Ja, es gibt sie – einige Abmahnungen wurden wahrgenommen und ein paar Rechtsanwälte haben versucht damit den einen oder anderen Euro zu verdienen. Die erwartete Flut an Abmahnungen blieb aber aus.

Woran liegt das? Wir wissen es nicht. Vermutlich liegt es daran, dass die Themen, die bisher in den Abmahnungen moniert worden sind, nicht vor Gericht geklärt worden sind und damit auch für den Abmahnenden ein Risiko darstellen könnten.

IST DENN NUN ALLES KLAR?

Leider nicht. Immer noch sind einige Themen unklar. Dies liegt daran, dass diese Themen entgegen der bisherigen Auffassungen plötzlich mit einer neuen bzw. abweichenden Meinung seitens der Aufsichtsbehörden bedacht wurden, oder einfach auf Grund des butterweichen Gesetzestextes noch frei in der Auslegung sind. Nachfolgend möchten wir ein paar dieser Punkte aufgreifen und den aktuellen Stand dazu aus unserer Sicht schildern:

¹ <http://www.faz.net/aktuell/wirtschaft/diginomics/behoerden-verzweifeln-am-neuen-datenschutz-15657324.html>

IHRE DATENSCHUTZBEAUFTRAGTEN

GOOGLE ANALYTICS – NUR NOCH MIT EINWILLIGUNG?!

Bisher war es üblich, dass die Einbindung von Google Analytics in anonymisierter Form ohne Rückfrage beim Webseitenbesucher eingebunden und aktiv genutzt wurde. Wollte der Internetnutzer einer Analyse seiner Seitenaufrufe entgehen, hatte er die Möglichkeit zum Widerspruch (OptOut). Die Konferenz der Landesdatenschutzbeauftragten und die Bundesdatenschutzbeauftragte haben jedoch ein Positionspapier² herausgegeben, worin eine Zulässigkeit von Google Analytics nur mit expliziter Einwilligung des Betroffenen, also per OptIn, als gegeben angesehen wird. Diese Position hat erst einmal keine rechtliche Bindung, trotzdem werden die Aufsichtsbehörden diese Position im Streitfall wohl vertreten wollen. Dies gilt auch heute noch.

Handlungsoption: Mangels rechtlicher Bindung kann Google Analytics weiterhin in üblicher Art und Weise eingebunden werden, ein gewisses Risikopotenzial für Ärger mit der Aufsichtsbehörde ist jedoch vorhanden. Wenn Sie Risiken meiden wollen, sollte eine OptIn-Einbindung in Betracht gezogen werden.

GOOGLE FONTS – VOM GOOGLE-SERVER ODER LOKAL HOSTEN?

Die Abmahnenden stellen sich dabei auf den Standpunkt, dass die Information des Betroffenen nicht korrekt durchgeführt wurde, genauer: Eine Datenübermittlung an den Dritten (Google) bereits stattgefunden hat, bevor der Betroffene nach Art. 12 DSGVO informiert werden konnte.

Handlungsoption: Hosten Sie die genutzten Fonts im eigenen Webspace und vermeiden so den Download von den Google-Servern.

COOKIES – ES HÖRT NICHT AUF...

Cookies waren schon oft ein Streitthema und dies hat beispielsweise dazu geführt, dass nahezu jede Webseite heute auf die Nutzung von Cookies hinweist. Interessanterweise werden diese teilweise bereits auf dem PC des Betroffenen gespeichert, bevor dieser überhaupt auf OK geklickt hat. Auch dies passiert, bevor der Betroffene informiert wurde oder die Möglichkeit hatte sich gegen die Datenverarbeitung zu entscheiden.

Handlungsoption: Achten Sie darauf, dass tatsächlich keine Cookies gesetzt werden, bis der Betroffene den Hinweis bestätigt hat.

² https://www.lidi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf

Aktuelle Entwicklungen im Datenschutz / 07-2018

IHRE DATENSCHUTZBEAUFTRAGTEN

FACEBOOK UND CO. – SOZIALE MEDIEN ALS PLUGIN

Was für Google gilt, gilt natürlich auch für alle anderen Medien. Auch die Nutzung der Plugins der sozialen Medien, Facebook und Twitter seien hier nur stellvertretend erwähnt, stellt eine Datenübermittlung an einen Dritten dar.

Handlungsoption: Um den Abmahnungen aus dem Weg zu gehen, empfiehlt es sich die 2-Klick-Lösung oder die Einbindung mittels Shariff³ vorzunehmen.

KEINE AKTUELLE DATENSCHUTZERKLÄRUNG – JETZT ABER SCHNELL...

Bereits vor dem 25.05.2018 war dies ein Dauerbrenner in unserem Beratungsalltag – zum 25.05.2018 sollten die Webseiten über aktualisierte Datenschutzinformationen verfügen, damit die Informationspflichten nach Artikel 12 und 13 DSGVO erfüllt werden. Wir haben Ihnen dazu Musterbausteine bereitgestellt und aktiv bei der Zusammenstellung der Informationen beraten. Es gibt jedoch immer noch genügend Webseiten, die bis heute nicht aktualisiert worden sind.

Handlungsoption: Aktualisieren Sie, sofern noch nicht geschehen, Ihre Datenschutzerklärung.

FEHLENDE VERSCHLÜSSELUNG IN DER DATENÜBERTRAGUNG

Auch hierauf haben wir immer wieder aktiv hingewiesen. Der Schutz der Daten muss nach dem Stand der Technik erfolgen. Dazu gehört, dass die Datenübertragung – zumindest immer dann, wenn personenbezogene Daten erhoben oder ausgegeben werden – verschlüsselt erfolgt.

Hierzu gibt es bereits eine Abmahnung mit einer unrealistisch hohen Schmerzensgeldforderung von 12.500 EUR!⁴

Handlungsoption: Aktivieren Sie die SSL-Verschlüsselung Ihrer Webseite.

FACEBOOK (NOCHMAL): VERANTWORTUNG FÜR DIE FANPAGE

Ziemlich frisch hat der EuGH entschieden, dass der Betrieb einer Fanpage bei Facebook nicht nur in der Verantwortung von Facebook liegt, was die Datenverarbeitung betrifft. Immerhin ist Facebook ja nur deshalb in der Lage die Daten zu verarbeiten, weil der Autor der Fanpage diese aktiviert hat. Damit sieht der EuGH eine gemeinsame Verantwortung in der Verarbeitung⁵.

³ <https://www.heise.de/ct/ausgabe/2014-26-Social-Media-Buttons-datenschutzkonform-nutzen-2463330.html>

⁴ <https://t3n.de/news/dsgvo-abmahnung-ssl-fehlt-1091180/>

⁵ <https://diercks-digital-recht.de/2018/06/update-entscheidung-der-dsk-zum-eugh-urteil-c-210-16-im-hinblick-auf-eine-gemeinsame-verantwortung-von-facebook-und-seitenbetreibern-spoiler-sie-muessen-was-tun/>

IHRE DATENSCHUTZBEAUFTRAGTEN

Aber haben die Autoren der Fanpage überhaupt Einfluss auf die Datenverarbeitung durch Facebook? Nein. Jedoch fehlt es für die Richter an der Transparenz im Umgang mit den Daten seitens Facebook.

Die fehlende Transparenz wird deutlich, wenn man den Umfang der Datensammelei betrachtet, den Facebook vor dem US-Kongress⁶ zugegeben hat. Die Rede ist von ausgelesenen Kontaktlisten, Anrufrufen, SMS-Verläufe, Standorte, Fotos, Mausbewegungen und Browser-Fenster.

Wie kann man diesem Thema nun begegnen? Für völlige Transparenz kann nur Facebook sorgen, wir rechnen aber nicht damit, dass dies so schnell passieren wird. Als erste Maßnahme würden wir empfehlen, dass die Datenschutzerklärung der eigenen Webseite um den Betrieb der Fanpage erweitert wird und dass dieser Text als „Datenrichtlinie“ auf der Fanpage eingebunden wird. Diesen Menüpunkt stellt Facebook zur Verfügung.

Bereits 2016 hat die Datenschutzaufsicht in Rheinland-Pfalz hierzu ein Muster⁷ bereitgestellt. Wir sind ein großer Freund von der Nutzung solcher durch die Aufsichtsbehörden bereitgestellten Informationen. Auch wenn diese die Rechtssicherheit nicht erhöhen, liefern sie doch Argumente, wenn es zum Streit mit den Behörden kommt.

Handlungsoption: Erweitern Sie Ihre Datenschutzerklärung um den Betrieb einer Facebook-Fanpage und verlinken Sie die Datenrichtlinie. Bewahren Sie Ruhe... Wenn Sie das Restrisiko nicht tragen möchten, können Sie derzeit die Fanpage nur deaktivieren.

BENÖTIGEN KONTAKTFORMULARE EINE CHECKBOX FÜR DEN DATENSCHUTZ?

Für uns ein klares NEIN! Die Kontaktaufnahme mittels Formular auf der Webseite erfolgt aus der freien Entscheidung des Betroffenen heraus. Er stellt an uns die Forderung sein Anliegen zu bearbeiten und wir liefern darauf die Antwort und verarbeiten dazu die Daten, die benötigt werden. Im Idealfall wird daraus ggf. (je nach Formular) ein Anstellungsverhältnis, ein Kaufvertrag usw... Es handelt sich also um eine vorvertragliche Tätigkeit und bedarf daher keiner separaten Einwilligung durch den Betroffenen. Auch sind die Datenschutzinformationen nur Informationen, hier wird kein Vertrag geschlossen. Auch aus diesem Grund ist eine Checkbox nicht notwendig.

Achten Sie bei der Verlinkung der Datenschutzinformationen aber bitte darauf, dass der Text „ich nehme zur Kenntnis“ oder „habe verstanden“ genutzt werden. Die Formulierungen „es gelten“ oder „akzeptiere“ könnten bei Juristen dazu führen, dass diese die Datenschutzinformation als AGB werten. Eine Änderung der Datenschutzinformation würde dann immer auch mit einer Information aller Bestandskunden einhergehen und würde ein Widerspruchsrecht gegen die Änderungen enthalten.

⁶ <https://www.computerbase.de/2018-06/us-kongress-facebook-umfang-daten-tracking/>

⁷ https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Muster_Datenschutzerklaerung_Facebook.pdf

IHRE DATENSCHUTZBEAUFTRAGTEN

WAR ES DAS JETZT?

Mit Blick auf das Internet soll es das vorerst aus unserer Sicht gewesen sein. Tatsächlich ist es damit aber nicht vorbei. Ebenfalls ein Dauerbrenner in der Beratungspraxis: Die Informationspflichten nach Artikel 12 bis 14 DSGVO.

WANN MUSS ICH INFORMIEREN?

Kurz: Die Information muss immer dann erfolgen, wenn wir erstmalig Daten eines Betroffenen erheben. Dabei regelt Artikel 12 DSGVO die Form der Kommunikation (Transparenzgebot) und die Rechte der Betroffenen. Artikel 13 klärt auf, welche Informationen wir zu leisten haben, wenn die Datenerhebung direkt beim Betroffenen stattfindet und Artikel 14, wenn die Erhebung über einen Dritten erfolgt.

DAUERTHEMA: ERSTKONTAKT AM TELEFON...

Bereits vor dem 25.05.2018 haben wir darauf hingewiesen, dass die wortlautmäßige Auslegung von Artikel 13 DSGVO eine Information bereits am Telefon notwendig macht. Notwendig macht dies der Wortlaut von Satz 1: „... so teilt der Verantwortliche ... zum Zeitpunkt der Erhebung ... mit ...“

Seitdem wurde über den Umfang der Informationspflicht am Telefon diskutiert. Seitens der Aufsichtsbehörden wurde Entgegenkommen signalisiert, so dass das LDI NRW am Ende nur noch auf eine Kommunikation nach etwa folgendem Muster bestand: Nennung des Verantwortlichen, der primären Zwecke der Datenverarbeitung und dass die restlichen Informationen auf der Webseite bereitgehalten werden. Schön war das immer noch nicht...

Weiteres Nachbohren verhalf uns dann zur Auskunft, dass bei der Kommunikation im B2B-Bereich die vernünftigen Erwartungen des Betroffenen erfüllt werden sollten. Sofern also keine ungewöhnlichen oder nicht zu erwartenden Verarbeitungen erfolgen sollten, würde es wohl reichen, wenn auf die Speicherung der Daten mündlich hingewiesen wird. Schon besser....

Am besten hat uns bisher aber eine Veröffentlichung des ULD Schleswig Holstein gefallen. Nach Meinung dieser Aufsichtsbehörde reicht es bei Ärzten aus, wenn diese am Telefon keine Information liefern, sondern diese in der Praxis als Flyer zur Verfügung stellen und damit die Informationen „im zeitlichen Zusammenhang mit der Erhebung der Daten“⁸ bereitgestellt werden.

Auch wir haben in unseren Beratungen bisher eine ähnliche Argumentation verfolgt, auch wenn wir damit eher auf die Nachweisbarkeit gem. Artikel 5 Abs. 2 DSGVO im Blick hatten. Wir argumentieren hier jetzt wie folgt:

⁸ <https://www.datenschutzzentrum.de/artikel/1220-Die-Datenschutz-Grundverordnung-tritt-in-Kraft-das-muessen-selbstaendige-Heilberufler-beachten.html>

Aktuelle Entwicklungen im Datenschutz / 07-2018

IHRE DATENSCHUTZBEAUFTRAGTEN

- 1) Die DSGVO unterscheidet weder nach Unternehmensgröße, noch nach Tätigkeitsschwerpunkt. Eine Arztpraxis ist ein Verantwortlicher, wie jedes andere Unternehmen auch.
- 2) Ärzte verarbeiten Gesundheitsdaten und bewegen sich daher im Bereich der besonderen Kategorien personenbezogener Daten und zudem im Bereich der Verschwiegenheitspflicht nach §203 StGB. Und damit immer im Bereich eines zumindest höheren Risikos für den Betroffenen.
- 3) Wenn es für die Aufsichtsbehörde trotz des Risikos ausreichend ist, dass die Information zeitnah erfolgt, kann es für alle anderen Unternehmen – außer wir reden über soziale Netzwerke oder BigData-Anwendungen – keine höhere Hürde bei der Einhaltung der Informationspflicht geben.

Wie wir schon immer beraten haben und es auch weiterhin tun:

Sorgen Sie dafür, dass der Betroffene zeitnah informiert wird. Im Idealfall erhält dieser kurz nach dem Telefonat eine Bestätigung (z.B. eine automatische E-Mail nach der Anlage im CRM-System), worin der Betroffene auf die Datenspeicherung hingewiesen wird und dass die Datenschutzinformationen stets in aktueller Form auf der Webseite zur Einsicht und Kenntnisnahme bereitstehen. Im Mindestfall würden wir eine Erweiterung der E-Mail-Signatur mit einem entsprechenden Link zur Datenschutzerklärung vorsehen. Je weiter Sie sich vom Wortlaut des Artikel 13 DSGVO entfernen, umso größer ist das für Sie verbleibende Restrisiko.

Solange die Aufsichtsbehörden hier keine klare und einheitliche Linie verfolgen, wird nur die vollständige Information am Telefon eine Rechtssicherheit bringen, jedoch sind wir – wie oben zu Facebook bereits angemerkt – immer froh, wenn die Aufsichtsbehörden uns argumentativ etwas an die Hand geben, was uns zumindest vor den Themen Fahrlässigkeit oder Vorsatz schützt. Sollte sich die Ansicht der Aufsichtsbehörden ändern, werden wir Sie natürlich weiterhin auf dem Laufenden halten.

WOMIT BESCHÄFTIGEN WIR UNS AKTUELL SONST NOCH?

Neben den aktuellen Beratungsanlässen und den oben genannten Punkten sind wir immer noch mit der Einholung der Vereinbarungen zu Auftragsverarbeitung nach Artikel 28 DSGVO beschäftigt. Es gibt immer noch Dienstleister (nicht unbedingt nur kleinere Unternehmen), die keine oder unvollständige Informationen bereitstellen können.

WOMIT KÖNNEN SIE SCHON MAL BEGINNEN?

Wenn die Themen „Webseiten“ und „Dienstleister“ soweit erstmal abgeschlossen sind, werden wir wahrscheinlich als nächstes „Formulare“ und „Einwilligungen“ als Schwerpunktthema adressieren. In

Aktuelle Entwicklungen im Datenschutz / 07-2018

IHRE DATENSCHUTZBEAUFTRAGTEN

Vorbereitung dazu können Sie sich Ihre aktuellen Formulare schon einmal ansehen und die abgefragten Informationen wie folgt klassifizieren:

- 1) Welche Daten benötigen Sie aus rechtlichen Gründen, oder sind notwendig, damit der Vertrag mit dem Betroffenen erfüllt werden kann?
- 2) Welche Daten helfen Ihnen nur bei der Erfüllung, sind aber eigentlich nicht notwendig, bzw. werden Daten auf Basis eines berechtigten Interesses verarbeitet?

Die DSGVO gibt uns vor, dass wir nur die Daten verarbeiten sollen, die wir für die Vertragserfüllung zwingend benötigen. Alle verarbeiteten Daten müssen rechtmäßig erhoben worden sein. Sofern die Rechtmäßigkeit auf einer Interessenabwägung beruht, sind diese in den Datenschutzinformationen zu benennen.