XQUEUE
Advanced E-Mail-Marketing Technologies

E-Mail Marketing mit der EU-DSGVO

Ein EMM-Guide der XQueue GmbH
Oktober 2017

E-Mail-Marketing mit der EU-DSGVO

Was ändert sich für Versender von Werbe-E-Mails?

Am 25. Mai 2018 löst die EU-DSGVO das bisherige Datenschutzgesetz (BDSG) ab. Einige Punkte werden in einem Nachfolgegesetz zum BDSG durch die Bundesregierung ergänzend geregelt. Und zu guter Letzt wird auch eine europaweite Novellierung der E-Privacy-Verordnung erwartet.

Datenschutz ist nicht das beliebteste Thema unter Marketing-Experten, dennoch werden die neuen Verordnungen für alle Unternehmen relevant, die digitales Marketing – insbesondere E-Mail- Marketing – betreiben oder betreiben wollen. Schon bei geringfügigen Verstößen gegen den Datenschutz drohen mit der EU-DSGVO massive Sanktionen bis zu 20 Millionen Euro!

Mit dieser Handreichung wollen wir Ihnen kurz aufzeigen, was Sie im E-Mail-Marketing bezüglich der neuen Datenschutzgesetze beachten sollten.

Teil 1 – Grundlagen

Das Verbot mit Erlaubnisvorbehalt – quasi ein „alter Bekannter“

Die aus dem BDSG bekannte Regelung „**personenbezogene Daten dürfen nur mit Einwilligung der Betroffenen** oder **aufgrund einer rechtlichen Erlaubnis verarbeitet werden**" gilt auch weiterhin und stellt für Sie die wichtigste Grundlage für die Verarbeitung personenbezogener Daten dar.

Bei der Ausgestaltung der Einwilligung und der Aufklärung des Betroffenen, gibt es strengere Anforderungen als bisher. Auf diesen Punkt gehen wir in **Teil 3 - Datenschutzrechtliche Einwilligung** genauer ein.

Gesetzliche Erlaubnisse, die keine persönliche Einwilligung der Betroffenen erfordern, gelten wie bisher - zum Beispiel die Verarbeitung zur Durchführung eines Vertrages, zur Erfüllung einer rechtlichen Verpflichtung und die Verarbeitung zur Wahrung berechtigter Interessen eines Unternehmens – sofern die Interessen und Grundrechte der betroffenen Nutzer nicht überwiegen.

Aber hier ist Vorsicht geboten: die Persönlichkeitsrechte der Betroffenen werden in den meisten Fällen schwerer wiegen als die berechtigten Interessen der Unternehmen (siehe hierzu Kurzpapier des Bayerischen Landesamts für Datenschutzaufsicht „Verarbeitung personenbezogener Daten für Werbung“ - https://www.lda.bayern.de). Nicht jedes Geschäftsmodell lässt sich mit der Abstellung auf *berechtigte Interessen* rechtfertigen. Die Verarbeitung von Namen und Adressen zur Versandabwicklung wird weiterhin erlaubt sein, das sehr verbreitete Nutzertracking wird sich aber auch zukünftig nicht ohne eine Einwilligung der betroffenen Nutzer rechtfertigen lassen.

Software-Hersteller werden strenger in die Pflicht genommen

In der EU-DSGVO finden sich zwei wichtige Neuerungen zum Thema technischer Datenschutz.

Verantwortliche sind zukünftig explizit aufgefordert, datenschutzfreundliche Techniken einzusetzen („**Privacy by Design**“) und Produkte mit datenschutzfreundlichen Voreinstellungen („**Privacy by Default**“) anzubieten.

Das bedeutet konkret, dass Sie ihre Datenverarbeitung nach diesen Vorgaben ausrichten müssen, egal ob Sie Arbeitsprozesse gestalten oder Software Dritter zur Verarbeitung nutzen möchten (z.B. Cloud Lösungen) – in jedem Fall müssen Sie dafür Sorge tragen, dass die eingesetzten Techniken und Systeme den beiden oben genannten Grundsätzen folgen und nur personenbezogene Daten verarbeitet werden, deren Verarbeitung auch für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind.

Die EU-DSGVO erwähnt z.B. die *Pseudonymisierung* als geeignetes Mittel, um diesen Vorgaben gerecht zu werden.

Weiterhin gilt der schon im BDSG vorgesehene **Grundsatz der Datenminimierung**. Neu ist, dass zur Verarbeitung eingesetzte Software diesen Grundsatz durch technische Voreinstellungen erfüllen muss. Dies betrifft die Menge der erhobenen Daten, den Umfang der Verarbeitung, Speicher- und Löschfristen, sowie die Zugänglichkeit durch Dritte. Diese Regelungen zielen zwar vorwiegend auf die bisherige Verarbeitungspraxis bei sozialen Netzwerken ab, gelten aber ebenso für alle anderen Unternehmensformen und Softwarelösungen.

Sie müssen also in Zukunft bereits bei der Erhebung von personenbezogenen Daten prüfen, ob diese Informationen für die Dienstleistung tatsächlich erforderlich sind, die erbracht werden soll. Für die Missachtung dieses Gebots drohen bereits empfindliche Bußgelder.

Recht auf Datenübertragbarkeit

Betroffene (also die Personen, deren Daten Sie speichern und verarbeiten), haben mit der EU-DSGVO ein Anrecht darauf, die durch ein Unternehmen gespeicherten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Sie müssen also dafür Sorge tragen, dass Sie die Daten jederzeit unverzüglich in einer Form übermitteln können, die der oder die Betroffene am PC ohne Schwierigkeiten öffnen und lesen kann.

Ebenso haben Nutzer damit das Recht, ihre Daten auf einfachem Weg an neue Anbieter übermitteln zu lassen – davon werden vor allem Cloud-Anbieter betroffen sein. Nutzer, die ihre personenbezogenen Daten zu einem neuen Anbieter umziehen wollen, haben nun per Gesetz einen Anspruch darauf, dass ihnen dies einfach und reibungslos ermöglicht wird. Theoretisch fallen hier Anbieter von E-Mail-Marketing-Software unter diese Definition, es wird aber sicher eher eine Ausnahme sein, dass ein Empfänger seine Anmeldedaten zu einem anderen Anbieter übertragen lassen möchte.

Datenschutzerklärungen müssen angepasst werden

Nutzer hatten schon nach BDSG und TMG das Recht Einblick in die über sie gespeicherten Daten und den Verwendungszweck zu nehmen, die EU-DSGVO geht an dieser Stelle aber deutlich über die alten Vorschriften hinaus. Allerdings hat sie diese Regelungen mit einer Öffnungsklausel versehen, die es dem deutschen Gesetzgeber erlaubt, hier eigene Vorschriften zu den Informationspflichten zu erlassen. Die Entwürfe zu einem ergänzenden Datenschutzgesetz in Deutschland zeigen bereits, dass der Gesetzgeber diese Öffnungsklausel eher zugunsten von Unternehmen auslegen möchte. Ob diese nationale Regelung dann mit EU-Recht vereinbar sein wird und nach Beendigung des Gesetzgebungsverfahrens Bestand hat, bleibt abzuwarten.

In jedem Fall müssen Sie aber die Datenschutzerklärungen nach BDSG auf Webseiten bis Mai 2018 angepasst haben. Sie müssen nun zum Beispiel nach EU-DSGVO die **Speicherfristen** und die **Gründe für die Datenerhebung** detaillierter angeben. Auch die **Kontaktdaten des Datenschutzbeauftragten** sind nun zwingend anzugeben. Wir empfehlen Ihnen hier Anrede, Name, E-Mail-Adresse und eine Rufnummer anzugeben, sowie die postalische Anschrift, sofern diese nicht der Unternehmens-anschrift entspricht. Eine anonyme E-Mail-Adresse wie *datenschutz@company.com* alleine ist nicht ausreichend.

Regelungen zur Dokumentation von Verarbeitungstätigkeiten

Sie als Verantwortlicher im Sinne der EU-DSGVO müssen, ebenso wie der Auftragsverarbeiter, sämtliche Verarbeitungstätigkeiten dokumentieren. Die sogenannten **Verzeichnisse von Verarbeitungstätigkeiten** sind in gewissenhaft zu führen und den Datenschutzbehörden auf Verlangen unverzüglich vorzulegen.

Folgende grundsätzliche Anforderungen gelten an die Dokumentation:

- Die Verzeichnisse sind regelmäßig in deutscher Sprache zu führen. Zumindest muss das Unternehmen in der Lage sein, von der Aufsichtsbehörde angeforderte Verzeichnisse unverzüglich in deutscher Sprache vorzulegen.

- Die Verzeichnisse sind schriftlich zu führen. Dies kann auch in einem elektronischen Format erfolgen.

- Die Aufsichtsbehörde kann das Format der Vorlage (schriftlich in Papierform oder elektronisch in Textform) eigenständig festlegen und daher auch bei einem im elektronischen Format geführten Verzeichnis den Ausdruck verlangen.

- Um Änderungen der Eintragungen im Verzeichnis nachvollziehen zu können (z.B. wer war wann Verantwortlicher, Datenschutzbeauftragter etc.), sollte eine Dokumentation der Änderungen mit einer Speicherfrist von einem Jahr erfolgen.

Welche konkreten Informationen in den Verzeichnissen enthalten sein müssen, entnehmen Verantwortliche Art. 30 DSGVO Absatz 1, Auftragsverarbeiter Art. 30 DSGVO Absatz 2.

Konkrete Mustervorlagen der Aufsichtsbehörden für Auftragsverarbeiter und Verantwortliche finden Sie auf der Webseite des Berufsverbands der Datenschutzbeauftragten Deutschlands (bvdnet.de). Sie können diese auch bei uns erhalten.

Diese Verzeichnisse müssen Sie nicht mehr öffentlich machen, aber den Behörden auf Verlangen vorlegen können. Haben Sie die Verzeichnisse nicht oder nicht ausreichend geführt, drohen empfindliche Bußgelder. Kleine Unternehmen (weniger als 250 Mitarbeiter), die nicht regelmäßig personenbezogene Daten verarbeiten, müssen diese Dokumentation nicht erstellen – im Regelfall erfolgt aber heutzutage in nahezu jedem Unternehmen die Verarbeitung regelmäßig, zum Beispiel in der Personalabteilung. Die besonderen Ausnahmen finden Sie in Art. 30 Abs. 5 DSGVO.

Neue Sanktionen – es kann richtig teuer werden!

Nach BDSG sind im Einzelfall Bußgelder bis zu 300.000 € möglich, in den letzten Jahren wurden tatsächlich Bußgelder in Höhen von mehreren Tausend, selten aber über Zehntausend Euro verhängt – weil die meisten Unternehmen ihre Verfahren schnell angepasst und sich einsichtig gezeigt hatten. Zukünftig sieht die DSGVO deutlich erhöhte Sanktionen vor, mit dem Ziel auch große internationale Unternehmen zu treffen.

Mögliche Bußgelder erhöhen sich auf bis zu **20.000.000 Euro** oder **4% des weltweit erzielten Jahresumsatzes** im vorangegangenen Geschäftsjahr – je nachdem, welcher Wert höher ist.

Natürlich wird nicht jedes Vergehen gleich mit dem Höchstsatz sanktioniert, die DSGVO ist die Grundlage für die Bemessungskriterien, nach denen die Behörden Schwere und Dauer der Verstöße eingestuft werden. Grundsätzlich drohen aber deutlich höhere Bußgelder und auch vermeintlich geringfügige Verstöße, wie eine nicht ordnungsgemäße Bestellung eines Datenschutzbeauftragten oder die fehlende Dokumentation der Verarbeitungstätigkeiten, können bereits mit sehr hohen Bußgeldern belegt werden. Dazu kommt, dass die Datenschutzaufsichtsbehörden voraussichtlich zusammengelegt und mit mehr Personal und Geld ausgestattet werden sollen, also auch stärker kontrollieren können als zuvor.

Was Sie umgehend prüfen sollten

- Liegen für alle Verarbeitungstätigkeiten die Einwilligungserklärungen der Betroffenen vor?
- Haben Sie Ihre Dienstleister und die verwendete Software auf **Privacy by Design** und **Privacy by Default** hin überprüft?
- Werden personenbezogene Daten in einem übertragbaren und maschinell lesbaren Format gespeichert, das zur Auskunftserteilung oder Datenübertragung geeignet ist?
- Haben Sie Ihre Datenschutzerklärung angepasst (Speicherfristen, Gründe der Datenerhebung)? Kontaktdaten Ihres Datenschutzbeauftragten genannt?
- Dokumentieren Sie bereits alle Verarbeitungstätigkeiten mit allen erforderlichen Angaben? Können Sie diese Verzeichnisse unverzüglich Behörden zur Einsicht vorlegen?

Teil 2 – Datentransfer & Tracking

Datenverarbeitung durch Dienstleister und in der Cloud

Heute ist es schon eher der Regelfall, dass personenbezogene Daten in Unternehmen mit Hilfe von Dienstleistern bzw. von Cloud-Anbietern verarbeitet werden. Alleine die Übertragung und Speicherung der Daten an einen Cloud-Anbieter (also alle Softwarelösungen, die nicht zu 100% von und bei Ihnen selbst betrieben werden) ist eine solche Verarbeitung. Die Übertragung an ein Rechenzentrum fällt ebenso darunter.

Die bekannten Voraussetzungen für die vertraglich geregelte Auftragsdatenverarbeitung bleiben erhalten, werden aber nach DSGVO strenger ausgelegt und erweitert. Beauftragte Dienstleister sind zukünftig streng weisungsgebunden und dürfen die übermittelten Daten nicht für eigene Zwecke verarbeiten. Aus diesem Grund müssen Sie beauftragte Unternehmen sorgfältig auswählen und kontrollieren.

Vor Aufnahme der Datenverarbeitung durch einen Dienstleister müssen alle Rechte und Pflichten in einem Vertrag festgelegt werden. Weiterhin ist in erster Linie (aber nicht mehr ausschließlich!) das beauftragende Unternehmen für die Einhaltung des Datenschutzes verantwortlich. Werden diese Anforderungen nicht eingehalten, drohen bereits Bußgelder bis zu 10 Millionen Euro!

Nach DSGVO werden zukünftig auch die Dienstleister selbst in die Pflicht genommen. Da auch neue formelle Pflichten auf den Auftragsverarbeiter zukommen, müssen bestehende Vertragsdokumente angepasst werden. Im Regelfall werden die alten Auftragsdatenverarbeitungsverträge nach BDSG durch einen neuen Vertrag nach DSGVO zu ersetzen sein. Das frühere strenge Schriftformerfordernis (eigenhändige Unterschrift) entfällt zukünftig, die Verträge können also auch elektronisch abgeschlossen werden.

Internationaler Datentransfer – Datenaustausch mit den USA

Nahezu alle großen Cloud-Dienstanbieter sind US-Unternehmen – Google, Apple, Microsoft, Salesforce, Dropbox usw. Beim Datentransfer in die USA bzw. zu Diensten die von US-Unternehmen angeboten werden, sind einige Anforderungen zu beachten, die sich aber nicht wesentlich von den bisherigen nach BDSG unterscheiden.

Im Falle einer Datenübermittlung in Drittstaaten (z.B. USA) ist eine **zweistufige Prüfung** vorzunehmen:

1. Zunächst muss, wie bei Datenübermittlungen im Inland bzw. EU-Ausland, ein Rechtfertigungsgrund der DSGVO greifen (etwa die Einwilligung des Betroffenen, überwiegendes berechtigtes Interesse des Unternehmens oder auch Vereinbarung einer Auftragsverarbeitung).

2. Ist dies der Fall, muss in einem zweiten Schritt festgestellt werden, ob bei dem Drittstaat oder zumindest bei dem konkreten Empfänger ein angemessenes Datenschutzniveau vorliegt. Dieser zweite Schritt wird häufig nicht beachtet, was zur generellen Unzulässigkeit der Datenverarbeitung führen kann.

Für die Feststellung der Angemessenheit sieht die DSGVO eine Reihe verschiedener Instrumente vor. Für den Datentransfer in die USA kann noch auf EU-Standardvertrags-klauseln und Zertifizierungen wie dem „Privacy Shield“ vertraut werden. Der europäische Gesetzgeber ist also weiterhin bestrebt, den internationalen Datentransfer zu ermöglichen.

Allerdings sind diese Instrumente auch mit einem Risiko verbunden. Insbesondere das „Privacy Shield“ steht in der Kritik, was bedeutet, dass die Vereinbarung in naher Zukunft entweder durch den EUGH oder durch das EU-Parlament gekippt werden könnte.

Auch die Absicherung mittels EU-Standardvertragsklauseln ist bisher nicht durch den EUGH bestätigt. Schaut man sich das Urteil zu „Safe Harbour“ an, ist auch bei den EU-Standard-vertragsklauseln nicht auszuschließen, dass es den europäischen Datenschutzgesetzen nicht standhält.

Die ePrivacy-Verordnung – Auswirkungen auf Tracking und Cookies

Neben der Auslagerung der Datenverarbeitung sind Cookies und Trackingmaßnahmen kaum aus dem Alltag digitaler Unternehmen wegzudenken. Neben der DSGVO soll im Mai 2018 noch eine zusätzliche Verordnung neu geregelt werden – die ePrivacy-Verordnung.

In Deutschland galt für Cookies auf Webseiten bislang das Opt-Out-Verfahren. Danach müssen Unternehmen über die Verwendung von Cookies innerhalb einer Datenschutz-erklärung informieren und den Nutzern die Möglichkeit geben, der Verwendung dieser Cookies zu widersprechen. In der Praxis hat sich hierfür auch die Verwendung von Cookie-Bannern etabliert. Da diese Regelung von der EU-Kommission für richtlinienkonform erklärt wurde, konnten sich Unternehmen bislang ziemlich sicher darauf verlassen.

Der im Januar 2017 bekannt gewordene Entwurf der neuen e-Privacy-Verordnung wird der DSGVO aufgrund speziellerer Regelungen vorgehen (speziellere Gesetze haben immer Vorrang vor den allgemeineren). Nach den dort enthaltenen Regelungen dürfen **Cookies grundsätzlich nur noch mit Einwilligung der Nutzer (Opt-In)** verwendet werden. Ausnahmen bestehen nur dann, wenn die Datenerhebung der Ermöglichung von Kommunikation über ein Netzwerk dient oder wenn die Nutzung erforderlich ist, um einen Informationsdienst in Anspruch zu nehmen, dessen Benutzung der Nutzer ausdrücklich verlangt.

Das Setzen von Cookies für reine Kommunikationszwecke (z.B. Benutzerprofile oder Warenkorb) ist demnach weiterhin ohne Einwilligung möglich. Auch soll es keiner Einwilligung bedürfen, wenn ein Session Cookie gesetzt wird, welches das Ausfüllen eines mehrseitigen Formulars ermöglicht.

Anders als nach derzeitiger Rechtslage in Deutschland, gilt dies aber nicht für Tracking oder sonstige Nutzerverfolgung. Bei sogenannten Third Party- und anderen Tracking-Cookies ist nach dem derzeitigen Entwurf der e-Privacy-Verordnung zukünftig eine ausdrückliche Einwilligung der Nutzer erforderlich. Die Einwilligung muss zudem jederzeit widerruflich sein. Laut Gesetzesentwurf soll die Einwilligungserklärung dabei auch über die Einstellung des Browsers möglich sein. Ob die Browser-Hersteller hierfür geeignete Instrumente liefern werden, ist aber noch völlig offen. Zudem dürfte aufgrund der Vorgabe „Privacy by Design“, ein generelles Einverständnis nicht vorausgesetzt werden. Nutzer müssten sich demnach konkret für die Speicherung von Third Party-Cookies in ihrem Browser entscheiden. Ob diese Einstellung von Nutzern bewusst gewählt wird, ist mehr als fraglich.

Was Sie umgehend prüfen sollten

- Prüfen Sie bestehende Auftragsdatenverarbeitungsverträge (ADVs) auf die neuen Anforderungen hin und schließen Sie ggf. rechtzeitig neue Verträge nach DSGVO ab.
- Prüfen Sie genau, ob der Datentransfer in Nicht-EU Staaten wirklich erforderlich ist und ob die Voraussetzungen nach DSGVO erfüllt werden. Nachlässigkeiten hier werden existenzbedrohend teuer - unzulässige Übermittlungen in Drittstaaten sind zukünftig mit Bußgeldern von 20 Millionen EUR oder bis zu 4% des gesamten weltweit erzielten Vorjahresumsatzes des Unternehmens bedroht.
- Prüfen Sie, ob Sie im E-Mail-Marketing Open/Click-Tracking einsetzen und die dafür erforderlichen Einwilligungen vorliegen. Sofern eine DSGVO-konforme Einwilligung des Nutzers zum personenbezogenen Tracking vorliegt (neben der Einwilligung zum Erhalt von Werbe-E-Mails), besteht voraussichtlich kein Handlungsbedarf.

Teil 3 – Datenschutzrechtliche Einwilligung

Die Einwilligung nach DSGVO

Grundlage einer zulässigen Datenverarbeitung ist auch zukünftig die **Einwilligungserklärung der Betroffenen**. Der Einwilligungstext muss nach Art. 7 DSGVO in verständlicher und einfacher Sprache formuliert und klar von anderen Sachverhalten getrennt werden. Zudem muss die Erklärung freiwillig erfolgen (dies ist z.B. bei Angestellten nicht einfach anzunehmen). Soweit sind die Anforderungen nicht neu gegenüber dem BDSG.

Gelten bereits nach BDSG erteilte Einwilligungen unter DSGVO fort?

Ja, bereits erteilte und nach jetziger Rechtslage gültige Einwilligungserklärungen dürften mit Geltung der DSGVO weiterhin bestehen bleiben.

Dies lässt sich auch einem aktuellen Beschluss des *Düsseldorfer Kreises*, einem gemeinsamen Gremium aller deutschen Aufsichtsbehörden für den Datenschutz, entnehmen (den Beschluss finden Sie am Ende dieses Dokuments). Danach gelten bisher erteilte Einwilligungen fort, **sofern sie der Art nach den Bedingungen der EU Datenschutzgrundverordnung** entsprechen.

Nach Ansicht der Behörden erfüllen bisher rechtswirksame Einwilligungen grundsätzlich diese Bedingungen. Allerdings müsste für die Fortdauer der bestehenden Einwilligungen die Altersgrenze von mindestens 16 Jahren (Schutz des Kindeswohls nach Artikel 8 DSGVO) sowie die Freiwilligkeit (Koppelungsverbot) berücksichtigt worden sein. Insbesondere das Koppelungsverbot könnte bei älteren Einwilligungserklärungen zu Problemen führen, da es nach bestehender Rechtslage weitaus weniger streng ausgestaltet ist.

Das neue Koppelungsverbot

Mit der DSGVO erhält das Koppelungsverbot in der DSGVO ein wesentlich stärkeres Gewicht. Danach gilt eine Einwilligung als unfreiwillig, wenn sie in Hinsicht auf solche personenbezogenen Daten erfolgt, die für die eigentliche Vertragserfüllung nicht erforderlich sind. Die Koppelung von Leistung und Datenschutzeinwilligung soll demnach

unzulässig sein, wenn dem Nutzer bei der Anmeldung zu einer Dienstleistung keine Wahl gelassen wird.

Das neue Koppelungsverbot ist für das E-Mail-Marketing dahingehend bedeutsam, dass in der Praxis häufig die Anmeldung zum Newsletter, neben der E-Mail-Adresse, noch mit weiteren Pflichtangaben (z.B. Name, Geschlecht, Alter etc.) verbunden wird. Nach der EU Datenschutzgrundverordnung besteht hierbei die Gefahr, dass gekoppelte Einwilligungen unzulässig sind und deren Einholung ggf. mit Sanktionen (Bußgeldern) durch Aufsichtsbehörden belegt werden können. Zur Vermeidung von Risiken, sollten demnach die Pflichtfelder bei der Anmeldung zum Newsletter zukünftig auf ein Minimum beschränkt werden.

Nachweis der Einwilligung

Stützt sich eine Datenverarbeitung auf eine Einwilligung, muss das Unternehmen nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat (Art. 7 Abs. 1 DSGVO).

Auch wenn die Nachweispflicht bereits nach bestehender Rechtslage zwingend erforderlich ist, wird sie in der DSGVO nun erstmals ausdrücklich benannt. Gleichwohl fehlt ein Hinweis, auf welchem Weg der Nachweis ausreichend erbracht ist.

Für das E-Mail-Marketing bedeutet dies, dass auch zukünftig auf Beweisinstrumente wie das Double-Opt-In-Verfahren und die Protokollierung von Anmeldeprozessen nicht verzichtet werden kann. Ohne belegbaren Nachweis ist die Einwilligung quasi nicht vorhanden, da sie vor Gericht nicht hinreichend bewiesen werden kann.

Geltung der Einwilligung

Von jeher unklar ist die Geltungsdauer erteilter Einwilligungserklärungen. Dies wird leider weder in der DSGVO noch im finalen Entwurf der ePrivacy-Verordnung ausdrücklich geregelt werden. Allerdings gibt Art. 9 der ePrivacy-Verordnung konkrete Vorgaben zum Widerruf und sich darauf beziehende Hinweise.

Zukünftig müssen Nutzer in periodischen Intervallen von sechs Monaten auf diese Widerrufsmöglichkeit hingewiesen werden. Bei einer regelmäßigen Nutzung eines Newsletters ist dies unproblematisch, da in jeder Werbemail regelmäßig Abmeldelinks und die Erklärung der Widerrufsmöglichkeiten enthalten sein müssen. Bleiben E-Mail-Adressen hingegen über einen längeren Zeitraum ungenutzt, müssen Nutzer alle sechs Monate darauf hingewiesen werden, dass die abgegebene Einwilligungserklärung widerruflich ist.

Wird diese Frist versäumt, besteht die Gefahr, dass abgegebene Erklärungen automatisch ihre Wirksamkeit verlieren. Erstmals könnte somit aus dieser Hinweispflicht eine Geltungsdauer von datenschutzrechtlichen Einwilligungserklärungen für das E-Mail-Marketing abgeleitet werden.

Ausnahmen für Newsletter an eigene Kunden bleiben bestehen

Bereits nach geltender Gesetzeslage ist eine Werbemail an eigene Kunden ohne Einwilligung erlaubt, wenn die Anforderungen des § 7 Absatz 3 UWG beachtet werden. Diese Ausnahme ist jedoch an sehr strenge Voraussetzungen gebunden, die in der Praxis häufig wenig beachtet oder schnell überstrapaziert werden.

Der europäische Gesetzgeber hat sich aber zur Beibehaltung dieser Ausnahme entschieden und im Entwurf der ePrivacy-Verordnung in Art. 16 Absatz 2 eine ähnliche Vorschrift für Bestandskunden festgeschrieben. Danach ist eine Einwilligung im E-Mail-Marketing weiterhin entbehrlich, wenn die E-Mail-Adresse im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung im Einklang mit der DSGVO erhoben wurde und zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen verwendet wird. Der Kunde muss dabei klar und deutlich darauf hingewiesen werden, einer solchen Nutzung kostenlos und auf einfache Weise widersprechen zu können. Das Widerspruchsrecht muss bei Erlangung der Angaben und bei jedem Versand einer Nachricht beachtet werden.

Die Herausforderung wird weiterhin bleiben, dass Unternehmen das Widerspruchsrecht bereits „bei Erlangung“ der E-Mail-Adresse beachten müssen. Ob dieser Hinweis innerhalb einer Datenschutzerklärung „versteckt“ werden darf oder gesondert erteilt werden muss, muss die Rechtsprechung durch Auslegung ermitteln. Dabei sei hier auch darauf hingewiesen, dass die ePrivacy-Verordnung noch im Entwurfsstadium steckt und etwaige Änderungen des Gesetzestextes nicht ausgeschlossen werden können.

Weitere Hinweispflichten

Hinweise zum Datenschutz waren bereits auf Websites gängige Praxis und nach den Vorgaben des Telemediengesetzes (TMG) verpflichtend. Die DSGVO ersetzt diese Hinweispflichten durch neue Regelungen in den Artikeln 13 und 14 DSGVO.

Bei der Einholung von Erklärungen müssen Betroffene zukünftig u.a. über die Kontaktdaten des Datenschutzbeauftragten, die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, eine mögliche Übermittlung in Drittländer und die Dauer der Speicherung informiert werden.

Elektronisch lässt sich dies mit einer Bestätigung der (auf das neue Recht angepassten) Datenschutzerklärung erledigen. Werden hingegen Erklärungen schriftlich eingeholt, müssten Unternehmen mit zusätzlichen Textbausteinen auf die Verwendung der erhobenen Daten gesondert hinweisen. Dies belastet nicht nur die Unternehmen, sondern dürfte im Regelfall auch die Verbraucher überfordern, die sich durch immer umfangreichere Texthinweise arbeiten müssen.

Fazit

- E-Mail-Marketing ohne ausdrückliche Einwilligungserklärung wird auch in Zukunft kaum möglich sein. Dabei bleiben elektronisch eingeholte Erklärungen, die über Double-Opt-In verifiziert wurden, nach bisheriger Auffassung weiterhin gültig, sofern nicht das Koppelungsverbot oder das erforderliche Mindestalter bei bestehenden Einwilligungserklärungen missachtet wurde.
- Das neue Koppelungsverbot verbietet zukünftig die Erhebung von Daten, welche für den Newsletter nicht benötigt werden. Unternehmen sind hier gut beraten ihre Registrierungsformulare hinsichtlich der Pflichtangaben rechtlich prüfen zu lassen.
- Die Geltungsdauer der Einwilligungserklärung ist weiterhin nicht gesetzlich geregelt. Aus den neuen Regelungen zum Widerspruchsrecht innerhalb der ePrivacy-Verordnung könnte jedoch eine maximale Geltungsdauer von sechs Monaten abgeleitet werden.
- In jedem Fall müssen sich Unternehmen mit den neuen Hinweispflichten auseinandersetzen und ihre Datenschutzerklärungen auf Websites und Textbausteine auf Formularen anpassen lassen.

Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 13./14. September 2016)

Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung

Bisher erteilte Einwilligungen gelten fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 Datenschutz-Grundverordnung).

Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen.

Informationspflichten nach Artikel 13 Datenschutz-Grundverordnung müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungs-grundes sind.

Besondere Beachtung verdienen allerdings die folgenden Bedingungen der Datenschutz-Grundverordnung; sind diese Bedingungen nicht erfüllt, gelten bisher erteilte Einwilligungen nicht fort:

- Freiwilligkeit („Kopplungsverbot“, Artikel 7 Absatz 4 in Verbindung mit Erwä-gungsgrund 43 Datenschutz-Grundverordnung),

- Altersgrenze: 16 Jahre (soweit im nationalen Recht nichts anderes bestimmt wird; Schutz des Kindeswohls, Artikel 8 Absatz 1 in Verbindung mit Erwä-gungsgrund 38 Datenschutz-Grundverordnung).