DEUTSCHER MARKETING VERBAND

COMPETENCE CIRCLE DIGITAL MARKETPLACES WHITEPAPER **NOV. | 17**

EU-Datenschutzgrundverordnung (DSGVO): Was ist Sache für Marketing Manager, Geschäftsleitung und Vorstand?

Stand November 2017

Abstract

Für Verbraucher in der EU bringt der strengere und transparentere Umgang mit ihren Daten Vorteile. Doch für Unternehmen ist die konforme Umsetzung der EU-Datenschutzgrundverordnung (DSGVO) bis zum 25. Mai 2018 eine große Herausforderung.

Dieses Whitepaper zeigt im Zusammenhang mit der neuen DSGVO auf, was die wichtigsten Änderungen sind, auf die sich Unternehmen einzustellen haben.

Viele stellen sich die Frage, wann genau die Schwelle zu einem bußgeldpflichtigen Verstoß überschritten ist.
In dem Whitepaper bieten wir Lesern in dieser Hinsicht Hilfestellung. Darüber hinaus gibt es Links zu weiteren Informationen wie Studien, Checklisten usw.

Schlagwörter

#CCdigitalM, Datenschutz, Datenspeicherung, Datensicherheit, DSGVO, EU, Recht, Marketingdaten, Marktforschung, DMV

Zitiervorschlag

Gattiker, Urs E., Temmen, Taina, Sinistra, Patrizia (2017-11). EU-Datenschutzgrundverordnung (DSGVO):
Was ist Sache für Marketing Manager, Geschäftsleitung und Vorstand? Whitepaper. Düsseldorf: Deutscher Marketing Verband e.V. (DMV).
Aufgerufen am 2017-12-01 auf http://MCLago.com/download/13/

Einführung

Dieses Whitepaper steht Ihnen auch als PDF-Datei zur Verfügung. Durch das Anklicken von Links erhalten Sie Zugang zu vielen weiteren kostenlosen Ressourcen von Experten und öffentlichen Organisationen:

- **http://mclago.com/best-practice-5/** mit Ressourcen zu diesem Whitepaper und
- die PDF-Datei als Download (1,8 MB): **http://MCLago.com/download/13/**

Dies ist ein Whitepaper vom Deutschen Marketing Verband (DMV) des Competence Circles Digital Marketplaces (#CCdigitalM) (Temmen & Gattiker, 2017-05-13). Der Fokus liegt auf der neuen EU-Datenschutzgrundverordnung oder kurz DSGVO (englisch: GDPR für General Data Protection Regulation), die bis zum 25. Mai 2018 von Unternehmen umgesetzt werden muss.

Die neue DSGVO löst mit dem Datenschutz-Anpassungs- und -Umsetzungsgesetz-EU (DSAnpUG-EU) das bisherige Bundesdatenschutzgesetz (BDSG) in Deutschland ab (Bundesgesetzblatt, 2017-07-05). Auf der einen Seite ist eine Vereinheitlichung des Datenschutzes aus Sicht der Wirtschaft in der EU zu begrüßen, jedoch kommen dadurch auf die Unternehmen erweiterte Pflichten in Kombination mit abschreckenden Bußgeldern hinzu.

Insbesondere wir als Marketing-Experten sind besorgt, inwieweit sich unsere Tätigkeiten im Marketing mit Kundendaten, Newslettern, Marktforschung, Direktmarketing, Vertrieb etc. durch diese neuen europaweiten Datenschutz-Regulierungen verändern werden.

1. Datenschutz heute: Ein Potpourri von Problemen

Für die Beurteilung der neuen EU-Datenschutzgrundverordnung oder eines Gesetzes ist es sicherlich hilfreich, sich zu fragen, was damit bezweckt wird. Mit der DSGVO sollen die Persönlichkeit und die Grundrechte von Personen, deren Daten bearbeitet werden, geschützt werden.

Grundsätzlich bedeutet die DSGVO, dass Personen neben anderen Rechten zukünftig auch diese sechs wichtigen Rechte besitzen:

1. Auskunftsrecht darüber, welche Daten gespeichert werden.
2. Widerspruchsrecht gegen das Verarbeiten personenbezogener Daten z.B. im Direktmarketing.
3. Recht auf Vergessenwerden, d.h. Löschung der eigenen Daten.
4. Recht auf Datenübertragbarkeit, d.h. Transfer der eigenen Daten an Dritte.
5. Recht auf eine vollständige und verständliche Datenschutzerklärung.[1]
6. Recht auf Information innerhalb von 72 Stunden im Falle einer Datenpanne z.B. durch Hackerangriffe.

Dabei sind vom Schutzbereich sowohl natürliche als auch juristische Personen erfasst. Unter „Bearbeitung“ ist dabei jeder Umgang mit Personendaten zu verstehen – von der Erhebung bis zur Archivierung und Vernichtung.

[1]Eine einfache und verständliche Datenschutzerklärung ist Pflicht. Beispiel - 1 Seite lang - unter Punkt 8 (Resources) vom Bundesministerium für Justiz und Verbraucherschutz - IT Gipfel 2015 - hier: http://blog.drkpi.de/dsgvo-eprivacy-auswirkungen-3/#unique-identifier-4

Ein Paradebeispiel dafür war im Jahr 2017 das Datenschutz-Fiasko des Unternehmens Equifax. 143 Millionen Einwohner der USA waren davon betroffen. Dazu ebenfalls einige Equifax-Kunden aus Kanada und allein in Großbritannien weitere 600.000 Kunden.

Der Hacker-Angriff ist insbesondere aus drei Gründen sehr speziell:

1. das Ausmaß des Datendiebstahls,
2. der Schweregrad und
3. wie teilweise unprofessionell das Management mit der Situation umging.

2016 drangen Hacker in das Datenerfassungssystem der Regulierungsbehörde Securities und Exchange Commission (SEC) der USA ein. Hier geben Firmen Online-Finanzdaten ein, die die Regulierungsbehörde SEC benötigt.

Diese Informationen sind nicht öffentlich zugänglich. Die Behörde SEC hat versucht, dieses Debakel im Sicherheitsdispositiv zu verschweigen. Unbekannte Personen haben jedoch mit Hilfe dieses Datenlecks Finanztransaktionen getätigt, die erhebliche Gewinne generierten. Dies sickerte an die Öffentlichkeit. Die SEC sah sich deshalb gezwungen, die Öffentlichkeit über die Datenpanne zu informieren (Masters, 2017-09-23/24).

Ein weiteres Beispiel kommt aus der Schweiz. Aufgrund einer Sicherheitslücke bei der schweizerischen Bundesverwaltung wurden deren Systeme zwischen 2014 und 2017 durch unautorisierte Personen missbräuchlich genutzt. Diese haben womöglich Daten entwendet. Doch genau dies konnte nicht verifiziert werden. Das Problem wurde erst Anfang 2017 entdeckt. Innerhalb weniger Wochen konnte die Sicherheitslücke behoben werden.
Allerdings dauerte es Monate, bis sich die schweizerische Bundesverwaltung dazu entschlossen hat, diesen Datenmissbrauch öffentlich zu machen.

Die obigen Beispiele verdeutlichen zwei Dinge:

1. Wenn private Firmen sowie öffentliche Organisationen ein Datenleck oder den illegalen Zugang zu Daten feststellen, dauert es oft Monate, bevor betroffene Personen und die Öffentlichkeit informiert werden.
2. Bei Firmen oder Verwaltungen dauert es im Durchschnitt gut 200 Tage, bis realisiert wird, Opfer einer Cyberattacke geworden zu sein.

Punkt 1 ist damit geregelt, dass die DSGVO Unternehmen verpflichtet, die betroffenen Personen innerhalb von 72 Stunden informieren zu müssen.

Doch Punkt 2 ist womöglich der heiklere von beiden. Wenn es Monate dauert, bis ein Sicherheitsleck überhaupt entdeckt wird, kann der Schaden massiv sein.

Hinzu kommt die Dunkelziffer an Fällen, in denen der Missbrauch von Daten nie festgestellt werden konnte. Diese Ziffer wird als nicht unerheblich eingeschätzt. Dadurch entsteht ein großer materieller wie auch immaterieller Schaden, den die IT Sicherheitsbranche nicht genau beziffern kann.

Umsetzung EU-DSGVO: Was ist zu tun vor dem 25. Mai 2018?

Viele Unternehmen sind in ihrer Datenschutz-Umsetzung bereits weit fortgeschritten. Doch es lohnt sich auf jeden Fall, unsere Inventarliste von Fragen zur Hilfe zu nehmen. Diese 12-Fragen-Checkliste bietet schnell den notwendigen Überblick: **http://blog.drkpi.de/dsgvo-eprivacy-auswirkungen-3/**.

Die schriftlich verfassten Antworten zur Checkliste ermöglichen Ihnen eine genaue Bestandsaufnahme. Die Antworten zeigen auf, worin die Stärken Ihres Unternehmens in Sachen Datenschutz liegen und wo noch vor dem 25. Mai 2018 schleunigst aufgebessert werden sollte. Anhand dieser Checkliste erhalten Sie dann auch einen besseren Überblick darüber, mit welchen finanziellen Aufwendungen die Compliance-Arbeiten in Sachen DSGVO verbunden sein dürften.

Beim Ausfüllen der Checkliste oben empfiehlt es sich, die Tabelle 1 vor sich liegen zu haben. Diese zeigt beim Beantworten der Fragen sehr schnell, welche Situation aktuell vorliegt.

Zum Beispiel macht das Recht auf Vergessenwerden (Punkt 9) gewisse Prozesse notwendig, mit deren Hilfe die Daten einer Person in allen Dateien im Unternehmen gelöscht werden können. Dies muss dann dokumentiert werden.

Wie anfangs angekündigt, erhält der Kunde, der die Einwilligung zur Nutzung seiner Daten an ein Unternehmen abgetreten hat, künftig auch eine Opt-out-Option. Er kann nach der DSGVO die Nutzung seiner Daten verhindern oder aber auch widerrufen (siehe oben, sechs wichtige Rechte für Personen – Punkt 2 – Widerspruchsrecht). Das hat natürlich signifikante Konsequenzen für das Direktmarketing.

Tabelle 1. EU-Datenschutzgrundverordnung (DSGVO): verantwortlich ist die Geschäftsleitung

11 wichtige Dinge, die es zu beachten gilt – Was müssen wir jetzt tun?

1. Wann muss ein Datenschutzbeauftragter bestellt werden?
Die Verpflichtung zur Benennung eines Datenschutzbeauftragten ist vorhanden, wenn die Kerntätigkeit in der systematischen Überwachung oder Verarbeitung besonderer personenbezogener Daten besteht.
Öffentliche Stellen haben in jedem Fall einen Datenschutzbeauftragten zu benennen. Grundsätzlich gilt: Wenn zehn oder mehr Personen mit einem mobilen Endgerät oder PC arbeiten, muss in der Regel ein betrieblicher Datenschutzbeauftragter bestellt werden. Obwohl dies nicht für die Schweiz oder Österreich zutrifft, spielen hier Überlegungen in Sachen Extraterritorialität eine wichtige Rolle (siehe Punkt 10, Daten von Personen aus der EU...).

Der Datenschutzbeauftragte kann auch für eine Unternehmensgruppe bestellt werden (z.B. Konzern).

Compliance: Wenn Kundendaten gesammelt werden (siehe Punkt 4), wird ein Datenschutzbeauftragter benötigt.

2. Welche Expertise ist notwendig, um den Datenschutz richtig auszuführen?
Natürlich muss das Datenschutz-Gesetz gelesen und verstanden werden. Neben rechtlichem Grundwissen wird zusätzlich ein hohes technisches Verständnis benötigt. Kaum eine Person wird all das notwendige Wissen mitbringen.
Daher ist eine Teamarbeit mit Kompetenzen aus unterschiedlichen Fachbereichen empfehlenswert.

Compliance: Rechtliches und technisches Fachwissen inkl. IT sollte unbedingt im Team vorhanden sein.

3. Wer ist zuständig und verantwortlich für den Datenschutz?
Bisher war die Aufgabe der Datenschutzbeauftragten, auf die Einhaltung der datenschutzrechtlichen Vorschriften hinzuwirken. Mit der DSGVO kommt nunmehr die entsprechende Überwachungsaufgabe hinzu. Verantwortlich für den Datenschutz ist weiterhin die Leitung einer öffentlichen Agentur oder Behörde.

Compliance: Im Unternehmen liegt die Verantwortung bei einem Mitglied der Geschäftsleitung.

4. Wann muss eine Dokumentation vorgenommen werden?
Die Dokumentationspflicht betrifft Unternehmen

- mit mindestens 250 Mitarbeiter/innen
- wenn ein erhebliches Risiko für die betroffenen Personen im Falle einer Datenpanne besteht
- wenn die Datenbearbeitung nicht nur gelegentlich erfolgt
- wenn sensible Personendaten bearbeitet werden, z.B. Name, Alter, Geschlecht, Postanschrift, E-Mail-Adresse, Telefonnummern von Kunden

Compliance: Auf die meisten Unternehmen, eingetragene Vereine (z.B. Mitgliederdaten) oder NGOs (z.B. Daten von Spendern) trifft einer dieser Aufzählungspunkte zu (siehe auch Punkt 1 oben).
Somit trifft automatisch die Dokumentationspflicht zu.

5. Was ist im Falle eines Hacker-Angriffs zu tun?
Die neue DSGVO macht die Meldung von Datenschutzverletzungen (data breach notification) zur Pflicht. Dies hat innerhalb von 72 Stunden, nachdem die unautorisierte Einsicht in eine solche Datenbank festgestellt wurde, zu geschehen.

Compliance: Das Unternehmen hat die notwendigen technischen und strukturellen Vorkehrungen getroffen, um z.B. unautorisierte Loginversuche schnellstmöglich feststellen zu können. Auch bei langen Wochenenden muss der Prozess jederzeit funktionieren.

6. Welche Bußen drohen bei Datenpannen oder Fehlverhalten?
Die DSGVO sieht vor, dass gegen Unternehmen ein Bußgeld von bis zu 20 Mio. Euro oder 4 Prozent des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verfügt werden kann (gem. Art. 83 V, VI DSGVO siehe auch https://dsgvo-gesetz.de/art-83-dsgvo/)

Compliance: Der Datenschutzbeauftragte ist auch künftig voraussichtlich nicht bußgeldpflichtig.

7. Ist das Tracking der Besucher auf unserer Webseite noch zulässig?
Das Tracking der Besucher von Webseiten ist zulässig, sofern der Webseitenbetreiber dieses selbst durchführt. Das heißt PIWIK ist zugelassen und Google Analytics (übernimmt dies als Auftragsverarbeitung) ebenso. Verantwortlich bleibt der Webseitenbetreiber, d.h. das Unternehmen (siehe auch Punkt 8).
Privacy-by-Design bedeutet nun auch, dass der Do-Not-Track Standard sich vielleicht noch in den Gremien durchsetzt, d.h. z.B. Browser haben die datenschutzfreundlichste Voreinstellung ab Werkseinstellung (LIBE Ausschuss des Europäischen Parlaments, 2017-10-17). Tracking-Walls sollen gemäß LIBE untersagt sein, d.h. ein Medienhaus kann Usern den Zugang nicht mehr verweigern, wenn diese Cookies ablehnen.

Compliance: Hier ist noch nicht klar, ob sich LIBE durchsetzen wird.

8. Inwieweit betrifft die DSGVO meine Kundendaten in der Cloud?
Diese Daten werden im Auftrag des Unternehmens in der Cloud gespeichert (d.h. der Cloud-Provider führt dies als Auftragsspeicherung durch). Verantwortlich bleibt das Unternehmen.
Bei der Heranziehung eines Auftragsverarbeiters muss ein schriftlicher Vertrag abgeschlossen werden. Punkt 5 muss die für diesen Punkt notwendige Dokumentation beinhalten, d.h. es muss dokumentiert sein, welche Daten, wo und wie in der Cloud gehostet werden.

Compliance: Der Vertrag muss den Gegenstand und die Dauer der Verarbeitung sowie deren Art und Zweck definieren. Ebenfalls müssen die Art der personenbezogenen Daten, Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sein.

9. Was bedeutet Recht auf Vergessenwerden?
Dies beinhaltet die Pflicht des Unternehmens zur Berichtigung. Ein Beispiel: Wenn Daten unrichtig sind, also mit der Wirklichkeit nicht übereinstimmen (z.B. falsches Alter), müssen wir dies in der Datenbank richtigstellen.
Die Löschung kann verlangt werden, wenn wir z.B. die personenbezogenen Daten nicht mehr benötigen. Ebenfalls, wenn die Person die Einwilligung zur Datenverarbeitung widerrufen hat (und es keine andere Rechtsgrundlage vorliegt). Es kann auch sein, dass die Person Widerspruch gegen die Verarbeitung eingelegt hat, und es keine vorrangig berechtigten Gründe zur Verarbeitung gibt oder die Daten unrechtmäßig verarbeitet wurden. Eine Einschränkung der Verarbeitung liegt z.B. vor, wenn die Verarbeitung unrechtmäßig ist und die Person Antrag auf Löschung gestellt hat.

Compliance: Voraussetzung, um gemäß Punkt 9 regelkonform arbeiten zu können ist, dass Punkt 5 richtig umgesetzt wurde.

10. Marketing & Kommunikation: Wie schaffen wir die Kür?
Kundendaten dürfen nicht für andere Zwecke als für das Bereitstellen von Dienstleistungen genutzt werden. Wollen wir diese anderweitig nutzen, muss der Kunde zuerst um Erlaubnis gefragt werden.
Wenn wir z.B. Marketing- oder Personaldaten von EU-Bürgern in der Schweiz, den USA oder der Ukraine bearbeiten oder in der Cloud speichern, muss die DSGVO angewendet werden. Hier wird das Konzept der Extraterritorialität eingeführt. Somit findet diese Regulierung weit über die Grenzen der EU Anwendung.

Compliance: Sich in eine Liste einzutragen, um den Newsletter zu bekommen (Single Opt-In), ist in Nordamerika gang und gäbe. Doch die DSGVO verlangt weiterhin, dass der Abonnent diesen Vorgang zusätzlich durch Anklicken eines Links in einer Follow-Up Mail bestätigt (Double Opt-In).
Ebenfalls ist hier Punkt 7 (Tracking der Besucher) ein Thema. Es könnte dank LIBE auch dazu führen, dass eine transparente Leistungsmessung digitaler Angebote inklusive Werbung noch schwieriger wird.

11. Was ist Pflicht für Verbände und Vereine?
Der Deutsche Marketing Verband (DMV) hat z.B. über 60 Marketing Clubs als Mitglieder. Jeder dieser Vereine hat wiederum Einzelpersonen und Firmen als Mitglieder. Von diesen werden natürlich notwendige Personendaten gespeichert und regelmäßig bearbeitet. Der DMV ist ein Auftragsbearbeiter von Mitgliederdaten seiner Clubs für die Verbandskommunikation, Mitgliederzeitschrift, usw. Der Marketing Club ist wiederum vor dem Gesetzgeber dafür verantwortlich, dass diese Daten sachgemäß und gesetzeskonform verarbeitet werden. Das bedingt einen Vertrag (siehe Punkt 8) zwischen dem DMV und seinen Clubs.

Compliance: Auch Verbände oder eingetragene Vereine, die Personendaten gespeichert haben und regelmäßig bearbeiten, sollten die Punkte 1 - 10 genau studieren.

Notiz: *Die EU-Datenschutzgrundverordnung (DSGVO) gilt ab 25. Mai 2018 unmittelbar. Der Text ist im Amtsblatt der EU veröffentlicht: http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016R0679*

2. Von der Pflicht zur Kür: Auf Wiedersehen WhatsApp

Die Folgeabschätzung der Auswirkungen der DSGVO ist sehr schwierig vorzunehmen, insbesondere weil vieles noch in der Umsetzung und daher unklar ist.

Hier gilt es z.B., die Rechtssache C-210/16 vom 24. Oktober 2017 zu erwähnen. Ein Fall, der auf einer Anordnung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) aus dem Jahre 2011 basiert. Der Generalanwalt des Europäischen Gerichtshofes (EuGH) schlägt nun vor, dass Unternehmen mit einer Facebook-Seite als Auftraggeber für Datenschutzverstöße von Facebook mitverantwortlich sind – mehr Details siehe Punkt 12 der Checkliste: http://blog.drkpi.de/?p=8219/#unique-identifier-3.

Das obige Beispiel könnte zukünftig Unternehmen mit Social Media Profilen wie auf Facebook aber auch auf Instagram oder Twitter davon abhalten, diese aus zu hohen Datenschutzrisiken weiter zu nutzen. Schließlich muss dann mit dem jeweiligen Social Media Kanal wie Facebook oder Twitter als „Auftragsverarbeiter“ ein schriftlicher Vertrag abgeschlossen werden.

Ob diese Social Media Plattformen dazu bereit sind, wird sich erst noch zeigen. Hierzu empfiehlt es sich, den Entscheid des EuGH abzuwarten.

Datenschutz-Compliance: Von der Pflicht zur Kür

Was Pflicht ist, wissen wir zwar dann, wenn wir die DSGVO genau studieren. Doch einige Dinge sind noch unklar. Insbesondere weil sich die notwendigen Gremien in Europa noch nicht in allen Punkten zur DSGVO geeinigt haben.

Hier ein Beispiel aus einer sehr wichtigen Studie für das Policy Department for Citizens' Rights and Constitutional Affairs vom Europäischen Parlament (Institute for Information Law, May 2017). Die Studie hat im Zusammenhang mit der neuen DSGVO drei wichtige Dinge angesprochen. Unter anderem schlug das Institute for Information Law (IViR) in dem Bericht vor:

1. **„Tracking Walls”**: Webseiten, zu denen der Nutzer nur dann vollen Zugang bekommt, wenn er die Cookie-Policy akzeptiert hat, sollten nicht mehr erlaubt sein.

2. **Basiseinstellung des Browsers**: Dieser sollte in der Grundeinstellung (d.h. ab Herstellung oder nach Installation) Cookies[2] blockieren. In der Praxis heißt dies, er erlaubt das Setzen von Cookies nicht. Der Nutzer kann diese Einstellung ändern, wenn er möchte.

3. **Direktmarketing Kommunikation**: Fällt unter den Bereich „behavioural targeting“ in der Werbung[3] bzw. innerhalb des Bereiches der „direct marketing communications“.

In der Studie weist das Institute for Information Law (IViR) (Mai 2017) darauf hin, dass z.B. kontextuelle Werbung, d.h. in dem Fall, dass bei einem Besuch einer Auto-Webseite dem Nutzer eine Werbung eines weiteren Autoherstellers gezeigt wird, nicht als „direct marketing” eingestuft werden soll. Das bedeutet, es ist nicht „behavioural targeting“.

Diese drei oben aufgeführten Herausforderungen sind zurzeit noch nicht gelöst. Der LIBE (2017-10-17) Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments hat seine Haltung zur ePrivacy-Verordnung (auch Cookie-Richtlinie genannt) festgelegt.

In der LIBE-Sitzung vom 19. Oktober 2017 wurde über die drei oben aufgeführten Punkte abgestimmt. Alle drei Vorschläge wurden angenommen.

Bis diese Punkte von allen Gremien abgeklärt/abgestimmt wurden (d.h. Europäisches Parlament und Europäische Kommission stimmen beide zu), ist weiterhin noch nicht ganz klar, wie hier die Compliance aussieht. Speziell, wie Webseitenbetreiber oder Anbieter von Browsern diese oben aufgeführten drei Punkte bis zum 25. Mai 2018 umsetzen müssen.

Wenn alle drei der oben genannten Punkte mit Hilfe der ePrivacy (sogenannte Cookie-Richtlinie) von Unternehmen umgesetzt werden sollen, wird eine neutrale und transparente Leistungsmessung digitaler Angebote inklusive Werbung schwierig.

Tabelle 2 (auf der nächsten Seite) zeigt einige weitere Punkte, die die Nutzung von Social Media Marketing und Social Media Kanälen stark beeinflussen könnten.

Sucht der Surfer eine Webseite ein weiteres Mal auf, können diese Informationen über das Surf-Verhalten genutzt werden. Oft dient es dazu, die Webseite individuell an den Nutzer anzupassen (z.B. spezielle Einstiegsseite).

[2]Cookies (Cookie, englisch für Keks) erlauben einem Web-Server, auf dem PC oder auf dem mobilen Endgerät des Anwenders Informationen zu hinterlegen
[3]SEMPO definiert „Behavioral Targeting“ als: „The practice of targeting and serving ads to groups of people who exhibit similarities not only in their location, gender or age, but also in how they act and react in their online environment. Behaviors tracked and targeted include web site topic areas they frequently visit or subscribe to; subjects or content or shopping categories for which they have registered, profiled themselves or requested automatic updates and information, etc.„ aufgerufen am 2017-09-20 von http://www.sempo.org/?page=glossary#b.

Tabelle 2. Auswirkung in der Praxis

Vier Beispiele, die zeigen, welche Konsequenzen die DSGVO hat, was die Nutzung von internetbasierten Dienstleistungen und Werkzeugen betrifft.

2.1. Sind Bewerbungsgespräche via Skype, Google Talk und Facetime möglich?
§ 26 Abs. 2 BDSG-neu
Im Fall einer Einwilligung der Mitarbeiter in die Verarbeitung ihrer Daten via Skype wird die Freiwilligkeit – ausgehend von der neuen Rechtslage nach der Datenschutzgrundverordnung (DSGVO) – sehr wahrscheinlich bereits an einem fehlenden Hinweis auf den Widerruf der Einwilligung gemäß Art. 7 Abs. 3 DSGVO scheitern.
In der Praxis ist dieses Gespräch auch kaum freiwillig, da die Person ja die Stelle haben möchte.
Auch Microsoft kann diese Daten einsehen, wenn dies auch kaum geschehen dürfte.

Siehe § 26 Abs. 2, Bundesgesetzblatt Jahrgang 2017, Teil I, Nr. 44, (20017-07-05).
http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2097.pdf

Compliance: Bewerbergespräche über das Handy führen. Kostenlos können Sie auch Signal nutzen, ein Open Source Projekt mit End-to-End Verschlüsselung (siehe http://whispersystems.org). Funktioniert auf dem Desktop und auf mobilen Endgeräten.

2.2 Dürfen wir das Social Media Profil eines Bewerbers überprüfen?
Das Überprüfen von Social Media Profilen z.B. auf Instagram, LinkedIn oder Xing ist nur dann erlaubt, wenn dies für den auszuführenden Job notwendig ist. Dabei liegt die Beweislast beim Arbeitgeber. Wenn Social Media Profile der Bewerber zur Beurteilung herangezogen werden, muss dies gemäß der DSGVO im Stelleninserat offengelegt werden.

Siehe Details von der Datenschutz Working Group 29 (die Bundesdatenschutzbeauftragten der EU Mitgliedstaaten) zu dieser Problematik hier auf http://blog.drkpi.de/dsgvo-eprivacy-auswirkungen-2/#unique-identifier-1

Compliance: Wenn ein neuer Mitarbeiter z.B. einen Tweet auf dem Twitter Profil des Unternehmens publizieren soll, muss dies schon in der Stellenanzeige ersichtlich sein.

2.3 Ist die WhatsApp/Facebook Messenger Nutzung im Kundenservice DSGVO-konform?
Ein erstes mögliches Hindernis für den rechtskonformen Einsatz im Unternehmen ist der Datenabgleich von Telefonnummern oder E-Mail-Adressen aus dem Adressbuch mit Daten auf den Servern.

Sowohl bei der Telefonnummer als auch bei der IP-Adresse handelt es sich um personenbezogene Daten. Im Zuge einer professionellen dienstlichen Nutzung ist nach der neuen DSGVO wohl ein Auftragsdatenverarbeitungsvertrag zwischen dem Anbieter des Dienstes und dem betroffenen Unternehmen erforderlich.

Doch da werden voraussichtlich weder WhatsApp noch Signal oder Threema kooperieren. Alle drei stellen in ihren Nutzungsbedingungen die private Nutzung als Anwendungsbereich heraus. Abgesehen von der Threema Work-Lösung, offerieren Messenger keine Angebote, welche die Mobile Device Management (MDM) oder Schnittstellen für entsprechende Integrationslösungen anbieten.

Das heißt auch, dass die Nutzung von solchen Tools im Kundenservice zurzeit nicht zu empfehlen ist, denn sie erscheint unter jetzigen Bedingungen nicht DSGVO-konform.

Compliance: Bei Heranziehung eines Auftragsverarbeiters – in diesem Fall WhatsApp – muss ein schriftlicher Vertrag abgeschlossen werden. Kann dies nicht gemacht werden, ist die Sache nicht DSGVO-konform. Falls der Europäische Gerichtshof den Entscheid fällt, dass ein Unternehmen mit Facebook mitverantwortlich ist, was Facebook mit den Nutzerdaten im Hintergrund macht (z.B. betreffend der Firmen- oder Markenseite auf Facebook, Facebook Messenger oder Instagram), wird hier ein weiteres Compliance-Risiko für Unternehmen entstehen, das auch andere Anbieter betrifft.

2.4 Ist DSGVO Compliance in der Gig-Economy ein Traum?
Ein Beispiel ist die Erbringung immaterieller Güter, wie z.B. Dienstleistungen als Handwerker. Dieser bietet seine Dienste z.B. auf TaskRabbit (IKEA) an. Er baut Billy Bücherregale beim Kunden zusammen. Ein weiteres Beispiel ist der Uber Fahrer, der sein privates Auto nutzt, um Fahrten anzubieten.

In beiden Fällen werden z.B. Personendaten wie die Postadresse des Kunden, Kreditkartennummern, usw. bearbeitet und genutzt (z.B. Uber Fahrer). Doch handelt es sich nicht um einen Festangestellten, sondern um einen professionellen Teilzeitarbeiter bzw. Freelancer.

Inwiefern der Plattform-Eigner Datenschutz und Sicherheit garantieren kann und will, ist unklar. Können wir sicherstellen, dass das Privathandy vom TaskRabbit-Freelancer die Verarbeitung von Personendaten nach DSGVO-Standards sichert?

Compliance: Inwiefern in der schnell wachsenden Gig-Economy DSGVO Compliance sichergestellt werden kann, steht noch in den Sternen.

Notiz: *Die Problematik der oben aufgezeigten Anbieter und der Datensicherheit kann nicht definitiv eruiert werden. In einigen Fällen werden die Gerichte entscheiden, wie die Auslegung der DSGVO in der Praxis gehandhabt werden muss.*

All die obigen Beispiele – wie auch diejenigen aus Tabelle 2 – zeigen, dass sich die Dinge immer noch entwickeln, was die operative Umsetzung der DSGVO betrifft.

Es zeichnet sich ab, dass Messenger Services wie Facebook Seiten, Instagram oder Twitter Profile für Unternehmen neue Risiken manifestieren.

1. Nutzung der Social Media Plattformen ist nicht DSGVO-konform (z.B. WhatsApp für Mitglieder-Informationen in einem Marketing Club) und

2. mit erhöhtem Risiko und notwendigen Folgeabschätzungen verknüpft, um der DSGVO gerecht zu werden (siehe z.B. Facebook Seiten, Instagram oder Twitter Profile).

Schlussfolgerungen

Die Diskussionen hier zeigen, dass es gute Gründe gibt, die Umsetzung der DSGVO nicht einer einzelnen Abteilung im Unternehmen zu überlassen. Vielmehr empfiehlt sich ein Team mit Kompetenzen und Know-how aus verschiedenen Fachbereichen.

Die entsprechenden Prozesse und Abläufe, wie oben besprochen, müssen umgesetzt werden. Doch dann gilt es, die Wirksamkeit dieser Prozesse mit Hilfe der eigenen internen Kontrolle zu überprüfen.

Die DSGVO sieht vor, dass eine regelmäßige Überprüfung und Anpassung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit durchgeführt wird. Dabei müssen auch im Marketing die Abläufe und Aufgaben im Datenschutz – und wie diese umgesetzt werden – dokumentiert sein.

Die Verarbeitung von Kundendaten, die Erhebung von Kundendaten beispielsweise in der Marktforschung, usw. – all dies sind persönliche Daten, die zukünftig besonders geschützt werden müssen, z.B. durch Anonymisierung (d.h. Personen können nicht identifiziert werden) oder durch Sicherheitsmaßnahmen, die die unautorisierte Nutzung möglichst verhindern.

Deshalb sollten diese drei Punkte bei der Umsetzung der DSGVO mitberücksichtigt werden:

1. **Abschätzung der Risiken und die Wahrscheinlichkeit, dass diese eintreten, ist sehr schwierig.** Wissen wir denn, wie viele Zero-Day-Vulnerabilities (bis jetzt unbekannte Sicherheitslücken) in unserer Oracle Kunden-Datenbank stecken? Kaum. Wie sollen wir dann abschätzen, ob jemand eine solche Vulnerabilität ausnutzt und unseren Kunden Schaden zufügt? Zwischen Erkennen und Ausnutzen der Sicherheitslücke durch einen Hacker liegen null Tage. Dabei kann es Monate dauern, bis die Sicherheitslücke auch dem Unternehmen bekannt ist und von diesem eliminiert werden kann.

2. **Zeitfenster bis zur Meldung einer Verletzung beträgt 72 Stunden.** Wenn man nicht weiß, dass man seit über einem Jahr gehackt wurde, kann man weder informieren noch die notwendigen Gegenmaßnahmen einleiten. Die Folgeabschätzung hier ist fast unmöglich oder kennen Sie einen praktikablen Weg dieses Problem zu lösen?

3. **Wie werden die möglichen physischen, materiellen und immateriellen Schäden quantifiziert?** Denn nur anhand der Wahrscheinlichkeit des Eintritts eines Szenarios X ist es möglich zu entscheiden, welche Investitionen getätigt werden müssen, um adäquate Verbesserungen durchführen zu können.

Punkt 2 oben ist mit dem Fall Deloitte (Hopkins 2017-09-25) sehr gut dargestellt. Das Unternehmen Deloitte, das seinen Kunden als Dienstleistung auch IT-Sicherheitsdienste anbietet, entdeckte im März 2017, dass sich Unbekannte seit Oktober oder November 2016 illegalen Zugang zum Mail-Server verschafft hatten. Die Hacker nutzten ein Admin-Konto. Durch diesen Zugang konnten sie auch private Kundendaten einsehen.

Der Fall Deloitte illustriert, dass man nicht immer sofort nachvollziehen kann, ob eine Sicherheitslücke genutzt wurde, um sich unautorisierten Zugang zu Personendaten zu verschaffen. Doch zukünftig ist es Pflicht, innerhalb von 72 Stunden nach Entdeckung des Datenlecks betroffene Personen bzw. die Öffentlichkeit zu informieren.

Die Beispiele von Deloitte, Equifax, SEC und der schweizerische Bundesverwaltung aus dem Jahr 2017 zeigen, dass die ab dem 25. Mai 2018 geltende Pflicht laut EU-DSGVO zur Meldung einer Verletzung innerhalb von 72 Stunden nicht nachgekommen wurde. Hier ist zur Sicherstellung der Compliance noch viel Arbeit notwendig.

Auch in Sachen Kosten sind Unternehmen gefordert. Eine Studie der International Association of Privacy Professionals (IAPP) und EY befragte mehr als 500 Datenschutz-Spezialisten von Fortune 500 Firmen zum Thema Kosten und DSGVO-Compliance (Hughes & Saverice-Rohan, Nov. 2017).

Anhand der Antworten der Studienteilnehmer errechneten die Autoren Kosten von rund 141 $ pro Mitarbeiter, um alle Anforderungen in Sachen Datenschutz erfüllen zu können. Diese Kosten können aber je nach Geschäftsfeld auf bis gut 600 $ pro Mitarbeiter/in steigen.

Dabei haben Firmen mit weniger als 5.000 Angestellten deutlich höhere Kosten. Die Studie errechnet, dass die DSGVO-Compliance für einen Mittelständler 550.000 $ in zusätzlichen Kosten verursacht. Hier muss das notwendige Personal eingestellt werden und die Mittel im Budget bereitgestellt sein. Ansonsten ist das Unternehmen nicht bereit für die DSGVO, deren Übergangszeit am 25. Mai 2018 abgelaufen sein wird.

Referenzliste

Bundesgesetzblatt (2017-07-05). Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtline (EU) 2016/680 (Datenschutz-Anpassunbgs- und -Umsetzungsgesetz EU - DSAnpUG-eu) vom 30 juni 2017. Bundes- gesetzblatt Jahrgang 2017 Teil I Nr. 44, S. 2097 - -2132. Aufgerufen am 2017-11-06 auf http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2097.pdf

Hopkins, Nick (2017-09-25). Deloitte hit by cyber-attack revealing clients' secret emails. The Guardian, online. Aufgerufen am 2017-09-26 auf https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails

Hughes, Trevor, J., & Saverice-Rohan, Angela (Nov. 2017, Report nicht datiert). IAPP-EY Annual Privacy Governance Report 2017, Aufgerufen 2017-11-20 auf https://iapp.org/resources/article/iapp-ey-annual-governance-report-2017/

Institute for Information Law (IViR). (May 2017). An assessment of the Commission's Proposal on Privacy and Electronic Communications. Study for the Civil Liberty, Justice and Home Affairs' Committee (LIBE), commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs. Aufgerufen 2017-09-20 auf http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU%282017%29583152_EN.pdf

LIBE Ausschuss des Europäischen Parlaments, (2017-10-17). Online privacy: how Parliament wants to increase protection http://www.europarl.europa.eu/news/en/headlines/society/20171012STO85933/online-privacy-how-parliament-wants-to-increase-protection abgestimmt wurde 2017-10-19 http://www.europarl.europa.eu/committees/de/libe/home.html

Masters, Brooke (2017-09-23/24). SEC faces questions of its own as it seeks to boost disclosure. Financial Times, Companies. Week in Review, S. 11. Aufgerufen am 2017-10-31 auf https://www.ft.com/content/f026e24a-9ed9-11e7-9a86-4d5a475ba4c5, mehr auf https://www.ft.com/content/f5292994-9f09-11e7-8cd4-932067fbf946

Temmen, Taina & Gattiker, Urs, E. (2017-05-13). DMV Competence Circle. [Blog MCLago]. Aufgerufen am 2017-07-27 auf http://mclago.com/best-practice-1

Ressourcen

Zusätzliche Ressourcen in Form von Checklisten, Tools und Tipps gibt es zum Thema EU-Datenschutzgrundverordnung (DSGVO) auch hier:

- Marketing Club Lago: http://mclago.com/?p=8303
- DrKPI: http://blog.drkpi.de/?p=6239

Autor:
Professor Urs E. Gattiker Ph.D
Kontaktdaten:
gattiker@marketingverband.de

Professor Urs E. Gattiker Ph.D. ist Präsident des Marketing Clubs Lago (MCLago.com) und Co-Leiter des Competence Circles Digital Marketplaces, kurz #CCdigitalM
Sein Interesse in Sachen Datenschutz und IT-Sicherheit resultierte unter anderem in den Publikationen „Anti-Viren Buch“ und „Security Dictionary“ http://blog.drkpi.de/top-rank-2/
Er ist CEO von DrKPI® CyTRAP Labs GmbH

Competence Circle
Die zehn Competence Circle bilden eine inhaltliche Themen- und Kompetenz-Plattform für den DMV und sorgen mit ihrer Expertise u.a. durch die Erstellung der Whitepaper für einen Know-how Transfer auf allen Ebenen des Deutschen Marketing Verbands. Die einzelnen Gruppen stehen für folgende zehn Themen:

1. Bewegtbild
2. Data Driven Marketing & Decision Support Pricing
3. **Digital Marketplaces**
4. Employer Branding
5. Markenmanagement
6. Marketingplanung und -optimierung
7. Mediamanagement
8. Pricing
9. Sponsoring
10. Vertriebskanalmanagement

Autorin:
Patrizia Sinistra
Kontaktdaten:
Patrizia.Sinistra@DrKPI.de

Patrizia Sinistra ist Mitglied im Marketing Club Lago und dort verantwortlich für Kommunikation und visuelle Kommunikation. Sie studiert an der Universität Konstanz. Bei DrKPI betreut sie in Teilzeit die Bereiche Bewegtbild und Marketing.

Autorin:
Taina Temmen
Kontaktdaten:
Temmen@marketingverband.de

Taina Temmen ist im Vorstand des Deutschen Marketing Verbands und verantwortlich für Content & Social Media. Sie betreut die Competence Circles. Als Mitglied des Marketing Clubs Lago und Marketing Clubs Nürnberg ist sie Co-Leiterin des #CCdigitalM (Digital Marketplaces). Beruflich ist sie bei der WINTERSTEIGER AG in Österreich, als Head of Business Development & Strategic Marketing tätig.

Impressum
Herausgeber: Deutscher Marketing Verband e.V. (DMV)
Sternstraße 58, 40479 Düsseldorf
Fon +49 (0) 211.864 06-0, Fax: +49 (0) 211.864 06-40
info@marketingverband.de
www.marketingverband.de
Bildquellen: ©Fotolia, ©iStock, ©Death to Stock Photo
1. Auflage, November 2017
ISSN (Print) 2512-5842
ISSN (Online) 2512-5656