doo SMART EVENT AUTOMATION

DSGVO IN EVENTS - WAS JETZT WICHTIG WIRD!

Was ändert sich durch den neuen EU-Datenschutz GDPR? Worauf müssen Sie achten und was sollten Sie unbedingt schnell umsetzen? Hier die wichtigsten Fragen und Antworten.

DATENSCHUTZ UND DIGITALE REGULIERUNG HABEN DURCH DIE EINFÜHRUNG DER NEUEN DATENSCHUTZGRUNDVERORDNUNG AM 25. MAI DEUTLICH AN RELEVANZ UND DRINGLICHKEIT GEWONNEN.

Auch bei doo sind die Anfragen bzgl. Informationen und Hilfe deutlich gestiegen. In unserem Datenschutz-Webinar **“DSGVO & Events”** haben weit über 300 Teilnehmer teilgenommen. Unser Datenschutzbeauftragter und Rechtsanwalt für Fachrecht IT hat die Umsetzung des DSGVO oder GDPR, wie das neue Gesetz auf Englisch bezeichnet wird, begleitet. **Was sich durch die neue Datenschutzgrundverordnung geändert hat und was Sie unbedingt beachten müssen, erfahren Sie in diesem eBook.**

AGENDA

AM 25. MAI 2018 WAR ES SO WEIT: DIE DSGVO IST IN IHRER GANZEN PRACHT UND HERRLICHKEIT ZUR ANWENDUNG GEKOMMEN.

WIE WEIT SIND SIE MIT DER UMSETZUNG UND IMPLEMENTIERUNG IN IHREM UNTERNEHMEN?

Hat man die Diskussion einiger Anbieter im Netz verfolgt, hätte man meinen können, am 25. Mai ginge die Welt unter. Das war zumindest der Eindruck, den man bekommen konnte, wenn man so manche Veröffentlichung zur DSGVO gelesen oder sich in den einschlägigen Foren, z.B. bei Facebook, umgeschaut hat. Natürlich war das alles nicht ganz richtig und auch viel Panikmache dabei.

WAS IST NUN ABER WIRKLICH AM 25. MAI PASSIERT UND WAS BEDEUTET DAS IN DER PRAXIS FÜR SIE IM EVENTBEREICH?

Die DSGVO ist nicht so schlimm wie ihr Ruf. Die grundlegenden Prinzipien bleiben gleich, es gibt lediglich einen recht grundlegenden Paradigmenwechsel.

-

DSGVO-CHECKLISTE
WO STEHEN SIE AKTUELL?

VERARBEITUNGSVERZEICHNIS

- Haben Sie ein Verfahrensverzeichnis mit der Übersicht aller Datenverarbeitungsprozesse erstellt?
- Haben Sie alle Datenverarbeitungsprozesse auf ihre Rechtmäßigkeit geprüft?

AUFTRAGSVERARBEITUNG

- Liegt eine Übersicht aller externen Auftragsverarbeiter vor?
- Haben Sie mit jedem Auftragsverarbeiter eine Vereinbarung Auftragsverarbeitung abgeschlossen?

DATENSCHUTZ UND DATENSICHERHEIT

- Haben alle Mitarbeiter ein Datenschutz-Training erhalten?
- Wurden alle Mitarbeiter nachweisbar auf Vertraulichkeit verpflichtet?
- Gibt es eine Dokumentation der technischen und organisatorischen Maßnahmen der Datensicherheit?
- Haben Sie geprüft, ob ein Datenschutzbeauftragter benannt werden muss (in Deutschland bereits ab 10 Mitarbeitern verpflichtend)?
- Wurde der Datenschutzbeauftragte gegebenenfalls der Aufsichtsbehörde gemeldet?

DATENSCHUTZINFORMATIONEN

- Haben Sie die Datenschutzinformationen auf der Webseite aktualisiert?
- Haben Sie alle Einwilligungserklärungen (z.B. für Newsletter) geprüft und aktualisiert?

DATENSCHUTZFOLGEABSCHÄTZUNG

- Wurde geprüft, ob eine Datenschutzfolgenabschätzung durchzuführen ist?
- Haben Sie ein Datenschutzmanagement installiert, das sicherstellt, dass die Datenverarbeitung kontinuierlich überwacht wird (bspw.jährliche Audits)?

BETROFFENENRECHTE

- Haben Sie einen Prozess definiert bei Geltendmachung von Betroffenenrechten (Auskunft, Löschung etc.)?

DSGVO BASICS

HARMONISIERUNG

Was passiert eigentlich? Worum dreht sich das Ganze? Die Leitidee ist **„Harmonisierung“**. Bisher haben wir 28 nationale Datenschutzgesetze basierend auf EU-Recht, zukünftig werden wir ein einheitliches EU-Datenschutzrecht haben, überall in der EU direkt anwendbar. Und das ist ja eigentlich eine tolle Sache. Insbesondere für international tätige Unternehmen, die sich dann nicht mehr mit 28 unterschiedlichen Gesetzen rumschlagen müssen, sondern nur noch mit dieser einen Datenschutzgrundverordnung.

In der Praxis sieht das leider nicht ganz so einfach aus: es gibt immer noch die nationalen Datenschutzaufsichtsbehörden, die das Recht dann interpretieren und anwenden. Und davon gibt es nicht wenige: in jedem EU-Mitgliedsland eine und in Deutschland nochmal 17. Und in diesen Aufsichtsbehörden sitzen Menschen. Und da diese nicht wie Roboter funktionieren, kann es passieren, dass aus ein und demselben Gesetz oftmals völlig unterschiedliche Dinge herausgelesen werden.

Hier wird sich dann über die nächste Zeit, über die nächsten Monate und Jahre hoffentlich eine einheitliche Lesart entwickeln. Aber grundsätzlich ist diese Harmonisierung in ganz Europa absolut zu begrüßen.

WELTWEITE WIRKUNG

Die DSGVO gilt nicht nur für die armen europäischen Unternehmen, sondern für jeden weltweit, wenn er in Europa seine Produkte und Dienstleistungen verkaufen oder Daten von EU-Bürgern sammeln und verarbeiten möchte. Wir schaffen hier also keinen Wettbewerbsnachteil für unsere EU-Unternehmen, es müssen sich eben nicht nur EU-Unternehmen mit der DSGVO herumschlagen, sondern ganz genauso beispielsweise die großen amerikanischen Internetkonzerne und auch der kleine kanadische Webshop, der eine deutschsprachige Seite anbietet und auch nach Deutschland verkauft. Und dass da in Europa etwas kommt, das merken die Unternehmen weltweit jetzt und es bricht aktuell eine gewisse globale Betriebsamkeit aus.

Das bedeutet also: Wir haben eine europaweite Harmonisierung des Datenschutzrechts mit weltweiter Wirkung

PERSONENBEZOGENE DATEN

Ganz grundsätzlich: **Der Datenschutz schützt personenbezogene Daten** – aber was sind eigentlich personenbezogene Daten?

Kurz gesagt alles an Daten, die eine natürliche Person identifizierbar machen.

Aber da fing der Streit an. Sind IP-Adressen personenbezogene Daten? Wie sieht es mit Lokalisierungsdaten aus?

Hier räumt die DSGVO auf und stellt klar, dass letzten Endes eigentlich alles, womit wir **im Eventbereich und im digitalen Marketing arbeiten, personenbezogene Daten sind.**

IP-Adressen, Tracking Pixel, Add IDs in den sozialen Medien, Geodaten, Pseudonyme in Cookies usw. Da gibt es keine große Diskussion mehr, all das sind personenbezogene Daten und wenn ich solche Daten anfasse, muss ich mich an die Regeln der DSGVO halten.

SANKTIONEN

Und wenn ich mich nicht an diese Regeln halte, lerne ich ziemlich schnell die Bußgelder nach der DSGVO kennen.

Die Bußgelder sind wahrscheinlich das, was man immer als allererstes liest, wenn es um die DSGVO geht.

Die Zahlen dürfte inzwischen fast jeder schon mal gehört haben: **20 Millionen Euro oder 4% vom weltweiten Konzernumsatz**. Das wären beispielsweise über 8 Mrd. Euro für Volkswagen. Und da kommt natürlich die große Aufmerksamkeit für die DSGVO her. Kein Finanzvorstand mag solche Risiken in seinen Büchern.

Aber auch hier sollte man die Kirche im Dorf lassen. Bußgelder sind bisher immer nur das letzte Mittel der Aufsichtsbehörden. Es ist äußerst unwahrscheinlich, dass am 27. Mai die Aufsichtsbehörde mit einem Bußgeldbescheid bei Ihnen vor der Tür steht.

Man darf eines nicht vergessen: Wir stochern bei so einigen Aspekten der DSGVO noch ziemlich im Nebel und wissen nicht so ganz genau, was wir an einigen Ecken jetzt genau machen sollen und müssen. Aber den Aufsichtsbehörden geht es ja ganz genauso. Die sind auch nicht allwissend und werden auch erst mal zurückhaltend sein, bei unklaren Sachverhalten Bußgelder zu verhängen. Wobei man seine Hausaufgaben schon machen muss, und dazu kommen wir jetzt gleich.

Die DSGVO hat zum Thema Sanktionen noch ein Schmankerl parat: **Sammelklagen**. Also wie in den USA. Das gibt es im Datenschutz bisher noch nicht und das kann unangenehm sein. Bei einem Datenschutzverstoß wird der einzelne Betroffene Sie wegen 100 € immateriellem Schadensersatz nicht verklagen. Aber wenn ein findiger Anwalt 100.000 Betroffene sammelt und bündelt, dann wird das auch schnell recht unangenehm.

Und, eigentlich unnötig zu erwähnen: Reputationsschäden sind im Datenschutzbereich ohnehin meist viel unangenehmer und schmerzhafter als alle Bußgelder.

RECHENSCHAFTSPFLICHT & TRANSPARENZ

Rechenschaftspflicht. Tolles Wort. Und Transparenz. Und damit einhergehend jede Menge Dokumentation. Das ist die große Leitidee der DSGVO.

Dahinter steht der etwas reaktionäre Grundgedanke „Schuldig bis zum Beweis der Unschuld“. Und das ist schon heftig. Das ist der Polizeibeamte, der abends auf dem Heimweg von der Arbeit anhält und sagt „Beweisen Sie mir bitte mal eben, dass Sie heute nichts Unrechtes getan haben“. Das ist nicht so ganz einfach. Sie müssen also beweisen, dass Sie der good guy sind und einen weißen Hut tragen. Und diese radikale Beweislastumkehr ist eben dieser Paradigmenwechsel, von dem ich am Anfang sprach.

Aber die DSGVO läßt uns damit nicht ganz alleine, sondern gibt uns bestimmte Werkzeuge an die Hand…

VERARBEITUNGSVERZEICHNIS

Das ist zum einen das wunderbare Verarbeitungsverzeichnis. Die Dokumentation sämtlicher Datenflüsse im Unternehmen. Die DSGVO will Transparenz. Wir müssen wissen, welche Daten wir im Unternehmen haben, woher sie kommen, wo sie gespeichert werden, warum wir diese Daten eigentlich verarbeiten dürfen, also die Rechtsgrundlage und so weiter.

Dieses Verarbeitungsverzeichnis ist wahrscheinlich die größte Hausaufgabe bei der DSGVO. Wobei es auch durchaus interessant sein kann, was man da so an Daten im Unternehmen findet. In den meisten Unternehmen findet sich irgendwo ein erstaunlich riesiger Datensatz, bei dem niemand so genau sagen kann, woher er kommt und warum man ihn eigentlich hat. Und in so einem Fall kann man dann auch tatsächlich mal über das „Löschen" nachdenken.

Niemand löscht gerne Daten, das ist klar. Löschen hat die unangenehme Eigenschaft, dass die Daten dann weg sind. Und bei Daten neigen wir alle so ein bisschen zum Messie-Syndrom: Alles sammeln und aufheben. Wer weiß, wofür man es noch brauchen kann. Aber bei personenbezogenen Daten muss man halt auch sagen: Daten, die man nicht mehr hat, können keinen Ärger mehr verursachen. Ein durchdachtes Löschkonzept ist also eine tolle Sache.

AUFTRAGSVERARBEITUNG

Diese Pflicht, alle Datenverarbeitungsaktivitäten zu dokumentieren, betrifft nicht nur die Daten, die im eigenen Unternehmen verarbeitet werden, sondern auch die Daten, die wir bei Auftragsverarbeitern verarbeiten lassen. Früher hießen diese Auftragsdatenverarbeiter, in der DSGVO jetzt nur noch Auftragsverarbeiter. Das ist aber dann auch die einzige Sache, die mit der DSGVO einfacher und kürzer wird.

Also, Sie müssen auch wissen und dokumentieren, was bei Ihren Auftragsverarbeitern mit Ihren Daten passiert. Die Pflicht zur Transparenz der Datenverarbeitung endet also nicht an ihrer Haustür bzw. ihrem Werkstor.

Und genau dafür gibt es in der DSGVO die Verpflichtung, bei einer Auftragsverarbeitung einen recht ausführlichen Vertrag abzuschließen, eine sogenannte Vereinbarung Auftragsverarbeitung, aktuell noch AuftragsDATENverarbeitung. Und in so einer Vereinbarung Auftragsverarbeitung ist dann eben unter anderem auch dokumentiert, welche Daten Ihre Auftragsverarbeiter im Auftrag verarbeiten, was sie damit machen, welche technischen und organisatorischen Maßnahmen der Datensicherheit ihre Auftragsverarbeiter vorhalten und so weiter.

Konkretes Beispiel hier doo:

Wenn sie über doo ein Event organisieren, werden natürlich unter anderem die Daten der Teilnehmer bei doo verarbeitet und diese Daten liegen dann in dem von doo genutzten Rechenzentrum in Deutschland. doo ist dann Ihr Auftragsverarbeiter und stellt dafür allen Kunden eine DSGVO-konforme Vereinbarung Auftragsverarbeitung zur Verfügung, in der dann ausführlich geregelt ist, was genau doo mit den Daten macht, dass doo diese Daten nur im Auftrag und nie zu eigenen Zwecken verarbeitet, dass alle Mitarbeiter zur Verschwiegenheit verpflichtet sind und so weiter. Und auch die technischen und organisatorischen Sicherheitsmaßnahmen bei doo sind hier ausführlich dokumentiert. Da ist man also in guten Händen.

DATENSCHUTZFOLGENAB-SCHÄTZUNG

Wir reden immer noch von der Rechenschafts-pflicht und Transparenz und den Werkzeugen, die uns die DSGVO dafür an die Hand gibt. Ein weiteres dieser Werkzeuge ist die **Datenschutz-folgenabschätzung**. Ein herrliches Wort, sowas kann nur die deutsche Sprache.

Worum geht's dabei? Nun, es geht darum, **Datenschutz im Herzen und in der Seele des Unternehmens zu verankern**. Und nicht nur im Herzen und in der Seele, sondern auch in den Prozessen im Unternehmen.

Momentan ist es doch, wenn man ganz ehr-lich ist, oft so, dass man ein tolles neues IT-Tool einführen oder eine abgefahrene Online-Mar-keting-Kampagne starten will – und am Tag vor dem Launch kommt jemand auf die Idee „Mensch, diesen Datenschutzfuzzi sollten wir vielleicht doch auch noch mal einbinden und fragen". Und dann stehen alle Räder still. Und genauso soll es nicht sein. Die DSGVO will, dass wir uns frühzeitig Gedanken machen über die Folgen für den Datenschutz, wenn wir ein neues IT-Tool einführen – und eben nicht erst am Tag vor dem Launch. Es geht also im Kern darum, Datenschutz von Anfang an mitzudenken und vor allem auch darum, die Prozesse gerade zu ziehen.

PRIVACY BY DESIGN, PRIVACY BY DEFAULT

In die gleiche Richtung geht das Privacy by Design (auf gut Deutsch „Datenschutz durch Technikgestaltung"). Auch hier ist die Idee, Datenschutz bei der Produktentwicklung von Anfang an mit auf dem Zettel zu haben. Und die Verpflichtung zu „Privacy by Default" sagt letzten Endes, dass wir immer die datenschutzfreund-lichste Voreinstellung wählen müssen. Das wird zum Beispiel für Browserhersteller interessant, da zukünftig eigentlich alle Browser by default Cookies ablehnen müssen. Wird spannend, ob und wie das umgesetzt wird.

DATENSCHUTZINFORMATIO-NEN

Und weiter geht es in Sachen Transparenz: Die Datenschutzinformationen auf der Webseite. Der nach außen hin sichtbarste Teil der DSGVO-Im-plementierung. Da sind so ein paar Dinge neu, ein paar kleinere zusätzliche Anforderungen, aber da sollte man auf jeden Fall etwas machen. Hier kann ich als Datenschutzaufsichtsbehörde – oder auch als böser Wettbewerber, mit einem Klick sehen, ob in Sachen DSGVO etwas gemacht wurde in Ihrem Haus oder eben nicht. Neu ist da-bei vor allem, dass ich die Rechtsgrundlage der Datenverarbeitung nennen muss. Und ich muss die Kontaktdaten des Datenschutzbeauftragten nennen.

Und wo ist das jetzt im Eventbereich relevant?

Auch die Teilnehmer an meinem Event muss ich darüber informieren, welche Daten über sie ich erhebe und was ich mit diesen Daten mache. Idealerweise natürlich gleich bei der Anmeldung.

Und wenn ich auf meiner Webseite die Anmeldung zu einem Event anbiete, muss sich diese Anmeldung bzw. diese Datenverarbeitung in den Datenschutzinformationen wiederfinden.

Diese Anpassung und Ergänzung ist wirklich ein Quick Win. Fragen Sie uns, wir unterstützen Sie gerne dabei.

BETROFFENENRECHTE

Jeder hat das Recht, zu Ihnen zu kommen und Sie zu fragen, welche Daten Sie zu seiner Person gespeichert haben. Und Sie müssen Auskunft erteilen. Und Sie müssen die Daten auch löschen, wenn das gewünscht ist. Und zwar eben nicht nur die Daten, die Sie bei sich liegen haben, sondern auch die Daten, die bei Ihren Auftragsverarbeitern liegen.

Und da sollten Sie unbedingt klären und sicherstellen, dass Ihre Dienstleister Sie da auch adäquat unterstützen und diese Rechte auch ordentlich umsetzen können. Gerade bei amerikanischen Cloud-Services ist das mit dem Löschen nämlich oft so eine Sache. Die sind zum Teil initial nicht zwingend dafür gebaut worden, Daten punktuell löschen zu können. Schauen Sie sich das an und lassen Sie sich das unbedingt bestätigen.

Wenn also ein Betroffener mit so einem Anliegen zu Ihnen kommt, sollte bei Ihnen keine helle Panik ausbrechen, sondern Sie sollten wissen, was zu tun ist. Dieser Prozess muss klar definiert sein und dieser Prozess muss sitzen.

Das ist nämlich genau der neuralgische Punkt, an dem man die Leute so richtig verärgern kann. Genau hier kommen die Beschwerden her. Beschwerden und Abmahnungen kassiert man fast nie wegen beispielsweise einer unaufgefordert versandten Werbe-E-Mail. Aber wenn ich ein Opt-Out ignoriere oder wenn ich so einem Auskunftsbegehren hier nicht nachkomme, dann werden die Leute sauer.

Auch hier: Durch sanfte Gewalt zwingt uns die DSGVO, unsere Prozesse zu durchdenken, gerade zu ziehen und sauber zu dokumentieren.

Wenn es konkret um Ihre Eventteilnehmer geht, deren Daten bei doo liegen, unterstützt doo Sie selbstverständlich vollumfänglich und sofort bei solchen Auskunftsbegehren oder Löschungswünschen.

ALS FAZIT AUCH HIER WIEDER:

Transparenz und saubere Prozesse. Ich muss wissen, wo meine Daten liegen und ich brauche einen sauberen Prozess, um auf sie zugreifen und sie eventuell löschen zu können.

RECHTSGRUNDLAGE DER DATENVERARBEITUNG

Das universelle Mantra des Datenschutzrechts: **Was nicht erlaubt ist, ist verboten.** Ein nicht so ganz liberales Grundprinzip. Was heißt das für uns? Nun, wir brauchen einfach definitiv immer eine Rechtsgrundlage, wenn wir Daten anfassen wollen.

Die einfachste Rechtsgrundlage ist dabei: Die Datenverarbeitung ist ERFORDERLICH FÜR DIE ERFÜLLUNG EINES VERTRAGES.

Im Eventbereich brauche ich nun grundsätzlich den Namen des Teilnehmers und die E-Mail-Adresse oder Postadresse, um das Ticket zuzusenden. Wenn das Ganze entgeltlich ist, muss ich auch irgendwie die Zahlung abwickeln. Auch dafür brauche ich bestimmte Daten. Diese Daten darf ich dann selbstverständlich auch verarbeiten.

Dann der Klassiker der Rechtsgrundlagen: DIE EINWILLIGUNG

Ja, ich will, dass Du meine Daten verarbeitest. Ja, ich will, dass Du mir Deinen E-Mail-Newsletter zuschickst.

Auch wenn man es überall anders liest – die Anforderungen an die Einwilligung, zum Beispiel in die Zusendung eines E-Mail-Newsletters, haben sich nicht wesentlich geändert. Zumindest aus deutscher Sicht. Das war schon immer nicht ganz leicht und wird es auch zukünftig nicht sein.

Wie sieht jetzt so eine Einwilligung im Detail aus?

Sie muss freiwillig sein, ich darf Sie nicht zu Ihrem Glück zwingen.

Dann beschert uns die DSGVO wahrscheinlich ein **Kopplungsverbot**. Das heißt, dass ich den Abschluss eines Vertrages nicht von einer Einwilligung abhängig machen darf. Das ist allerdings im Gesetz recht unklar formuliert und aktuell wild umstritten. Hier wird man sehen müssen, was die Aufsichtsbehörden und Gerichte daraus machen. Das wäre zum Beispiel im Eventbereich für die Weitergabe von Teilnehmerdaten ziemlich problematisch.

Die Einwilligung muss informiert erfolgen. Ich muss also wissen, in was ich da so einwillige.

Es muss eine eindeutige Handlung sein, also ein klares und lautes „Ja!“ und keine elegant und subtil untergeschobene, konkludente Erklärung. Und es muss klar sein, dass die Einwilligung jederzeit widerrufen werden kann.

Also, entweder brauche ich die Daten zur Vertragserfüllung oder ich habe eine Einwilligung – oder ich habe ein BERECHTIGTES INTERESSE an der Datenverarbeitung.

Es geht dabei um eine Abwägung der Interessen: auf der einen Seite mein Interesse, Daten zu verarbeiten. Auf der anderen Seite das Persönlichkeitsrecht des Betroffenen. Das Ganze funktioniert wie eine Waage, ich schaue mir die Interessen auf beiden Seiten an und lege kleine Bleigewichte in die jeweilige Waagschale und schaue, in welche Richtung die Waage sich neigt.

Und diese Bleigewichte können dabei ganz unterschiedliche Faktoren sein. Zum Beispiel:

Um welche Daten handelt es sich? Haben wir hier sensible Daten? Nicht gut.

Ist die Datenverarbeitung transparent und offengelegt? Kann ich widersprechen? Sind die Daten verschlüsselt? Ist so eine Datenverarbeitung üblich und zu erwarten oder ist das völlig unüblich?

Es läuft, kurz gesagt, auf die Frage hinaus, ob das, was ich da vorhabe in Sachen Datenverarbeitung, sich irgendwie komisch und unseriös anfühlt oder eben nicht.

Dieses berechtigte Interesse ist äußerst flexibel und ich kann damit, gerade im Bereich des Direktmarketings und auch im Eventbereich, tolle Sachen machen.

Die Sache hat allerdings leider einen kleinen Haken: Man weiß natürlich nie 100%ig, ob im Ernstfall die Aufsichtsbehörde oder ein Richter die Interessen genauso gewichtet, wie ich das tue. Hier wird manchmal eine gewisse Rechtsunsicherheit bleiben. Und da muss ich mir dann überlegen, ob ich bereit bin, dieses Risiko in Kauf zu nehmen, oder ob ich lieber auf Nummer Sicher gehe.

Ein praktisches Beispiel: Die Anmeldung zu einem Webinar zu „DSGVO & Events“

Welche Daten werden hier mit welcher Rechtsgrundlage erhoben?

Die E-Mail-Adresse wird zur Vertragserfüllung erhoben, um zum Beispiel dem Teilnehmer eine Anmeldebestätigung zuzusenden. Soweit, so klar.

Daneben werden aber noch Name und Firma abgefragt. Diese Daten brauche ich aber eigentlich doch nicht zwingend für die Erfüllung des Vertrages „Webinarteilnahme“. Sind wir hier also vielleicht einem riesigen Datenschutzskandal auf die Spur gekommen?

Selbstverständlich nicht! Diese Daten werden auf Basis eben dieses berechtigten Interesses erhoben, um zum einen eine Personalisierung der E-Mails zu ermöglichen und auch um zu sehen, wer an dem Webinar teilnimmt, für welche Branchen und für welche Firmen das Thema interessant ist und auch, um das Webinar entsprechend interessengerecht zu gestalten.

FRAGEN & ANTWORTEN

Genau dafür wurden die Teilnehmer bei der Anmeldung auch gefragt, welche Themen Sie besonders interessieren und welche speziellen Fragen Sie haben.

Aus diesen zahlreichen Fragen haben wir ein paar besonders relevante Fragen herausgesucht, auf die nachfolgend detaillierter eingegangen werden soll:

E-MAIL-MARKETING

Das digitale Marketing und insbesondere das gute, alte E-MAIL-MARKETING waren definitiv Tabellenführer bei den Fragen. Also, dass ich für E-Mail-Marketing eine Einwilligung brauche, ist allgemein bekannt. Wie so eine Einwilligung auszusehen hat, haben wir eben auch schon besprochen. Freiwillig, eindeutig, ausdrücklich und so weiter.

Nur die Anmeldung zu einer Veranstaltung stellt noch keine Einwilligung in die Zusendung von E-Mail-Werbung dar. Das sollte klar sein.

Ich kann aber natürlich bei der Anmeldung zu einem Event so eine Einwilligung gleich mit abfragen. Zum Beispiel durch eine **zusätzliche Checkbox,** wenn die Anmeldung online erfolgt. Dann kann ich die Daten anschließend auch für E-Mail-Werbung nutzen.

Wie war das mit der Kopplung? Also Anmeldung zum Event nur, wenn Du auch in E-Mail-Werbung einwilligst? Schwierig, wie gesagt. Kann man machen, da ist aber halt ein Risiko dabei, solange wir nicht wissen, wie die Damen und Herren in den Aufsichtsbehörden das so sehen. Wenn man auf Nummer Sicher gehen will also lieber eine separate Einwilligung in die Newsletterzusendung.

Das mit der Einwilligung gilt übrigens nicht nur für die klassische E-Mail-Werbung, sondern auch für elektronische Nachrichten in den sozialen Medien. Auch für eine Event-Einladung via Direct Message auf LinkedIn brauche ich streng genommen die Einwilligung des Adressaten. Hier kann man dann aber schon vielleicht auch risikobasiert herangehen und fragen, wie wahrscheinlich eine Abmahnung bei so etwas im B2B-Bereich ist und ob ich das Risiko nicht in Kauf nehmen kann

Auf welche Dinge muss bei einer Online-Anmeldemaske konkret hingewiesen werden

Bei der Onlineanmeldung zu einem Event muss man umfassend über die Datenverwendung informieren (siehe Art. 13 DSGVO), also darüber, welche Daten erhoben werden, zu welchen Zwecken diese Daten verarbeitet werden, auf welcher Rechtsgrundlage die Daten verarbeitet werden und wie lange die Daten aufbewahrt werden. Diese Information kann entweder in einem separaten Datenschutzdokument, bezogen nur auf die Eventanmeldung, oder in der allgemeinen Datenschutzinformation für die Webseite erfolgen.

Eine ausdrückliche Zustimmung des Anmeldenden ist dabei übrigens nicht erforderlich, es geht lediglich um eine Information zum Datenschutz.

Formulierungen wie “Ich stimme den Datenschutzinformationen zu” sind im Rahmen des Anmeldeprozesses nicht erforderlich.

Eine ausdrückliche Einwilligung des Anmeldenden, also z.B. in die Zusendung des E-Mail-Newsletters oder in die Weitergabe der Teilnehmerdaten an Sponsoren, muss ausdrücklich erfolgen und kann nicht in eine allgemeine “Zustimmung zu den Datenschutzinformationen” verpackt werden.

Darf ich Teilnehmer an einem Event auch ohne Newsletter-Opt-In zu anderen Events oder zum Beispiel zu Folgeveranstaltungen einladen?

Die Einladung zu einer Folgeveranstaltung oder anderen Events ist, zumindest rechtlich betrachtet, als E-Mail-Werbung anzusehen. Und für E-Mail-Werbung braucht man grundsätzlich immer die Einwilligung des Adressaten (“Opt-In”).

Allerdings gibt es hier eine interessante Ausnahme:

Bei einer bestehenden Kundenbeziehung dürfen Werbe-E-Mails zugesendet werden, wenn der Kunde dieser Zusendung nicht widersprochen hat (“Opt-Out”). Diese Ausnahmeregelung (in § 7 Abs. 3 UWG) hat jedoch bestimmte formale Voraussetzungen, weswegen man auch von einem „qualifizierten Opt-Out“ spricht. Im Einzelnen sehen diese Voraussetzungen wie folgt aus:

- Der Versender muss die E-Mail-Adresse des Kunden „im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden“ erhalten haben.
- Zudem muss der Kunde „bei der Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen“ worden sein, dass er der Verwendung seiner E-Mail-Adress für Werbung jederzeit widersprechen kann ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen“ – und der Kunde darf natürlich nicht widersprochen haben.
- Und in den anschließend an den Kunden gesendeten E-Mails dürfen ausschließlich „eigene ähnliche Waren oder Dienstleistungen“ beworben werden.

Entscheidend dabei ist: Der Hinweis auf das Widerspruchsrecht muss unmittelbar bei Erhebung der E-Mail-Adresse erfolgen, also in dem Moment, in dem der Kunde bei der Anmeldung seine E-Mail-Adresse angibt. Dieser Hinweis kann nicht später per E-Mail nachgeholt werden.

Umstritten ist die Frage, ob es sich um ein entgeltliches Rechtsgeschäft handeln muss, oder ob man sich auf die Ausnahmevorschrift auch z.B. bei einem kostenlosen Event berufen kann. Auch wenn es hierzu keine abschließende Rechtsprechung gibt und dementsprechend immer eine gewisse Rechtsunsicherheit bleibt, läßt sich meines Erachtens mit guten Argumenten vertreten, dass die Ausnahmevorschrift auch bei einem kostenlosen Event genutzt werden kann.

Auch bei der Frage, was “eigene ähnliche Waren und Dienstleistung” sind, herrscht Uneinigkeit. Allerdings dürfte man hier bei einer Einladung zu einer Folgeveranstaltung keine Probleme haben.

Ein Beispiel für das Wording im Rahmen einer Eventanmeldung:

Wir schicken Ihnen ihre Teilnahmebestätigung an Ihre angegebene E-Mail-Adresse. Zudem werden wir Ihnen zukünftig Einladungen zu weiteren ähnlichen Events, die für Sie interessant sein könnten, zusenden.

Dieser Zusendung können Sie jederzeit durch eine E-Mail an unsubscribe@xyz.de widersprechen, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen. Zudem ist in jeder E-Mail ein Abmeldelink enthalten. Nach Erhalt ihres Widerspruchs werden wir diese Zusendungen unverzüglich einstellen.

Gibt es einen Unterschied bzw. lockere Regeln bei Einladungen zu kostenlosen Veranstaltungen vs. kostenpflichtigen?

Nein. Bei der Frage nach der Rechtmäßigkeit der Zusendung von E-Mails geht es immer um die Frage, ob es sich bei einer E-Mail um Werbung handelt. Und die Rechtsprechung ist da ziemlich rigoros: Alles, was unmittelbar oder mittelbar dazu dient, Produkte und Dienstleistungen zu verkaufen, wird als Werbung angesehen. Auch die Einladung zu einem kostenlosen Webinar beispielsweise ist, durch die Brille des Juristen, Werbung, wenn auch nur irgendeine kommerzielle Absicht dahintersteckt und der Veranstalter, und sei es noch so mitttelbar, mit dem Webinar den Verkauf seiner Produkte und Dienstleistungen fördern möchte.

DATENSPEICHERUNG

Wie lange darf und muss ich denn die Teilnehmerdaten nach einem Event aufbewahren?

Juristisch nichtssagende Antwort: Ich darf Daten solange aufheben, wie ich sie benötige, um den Zweck zu erfüllen, zu dem sie ursprünglich erhoben wurden. Das hilft erstmal nicht so richtig viel. Also ganz grundsätzlich, wenn der Zweck nur „Teilnahme an dem einen Event“ ist, dann muss ich die Daten halbwegs zeitnah nach dem Event löschen. Ausnahme sind natürlich Rechnungsdaten, bei denen ich eine steuerrechtliche Aufbewahrungsfrist von sechs Jahren habe.

Ich kann aber den Zweck weiter fassen. Wenn ich den Teilnehmer bei Datenerhebung darauf hinweise, dass ich ihn gerne im Folgejahr wieder zum gleichen Kongress einladen würde, und er nicht widerspricht, dann habe ich natürlich eine Grundlage, die Daten dauerhaft zu speichern. Da muss ich halt ein bisschen kreativ werden und den Zweck der Datenspeicherung erweitern. Aber bitte immer transparent, der Zweck muss ja offengelegt werden.

WEITERGABE VON TEILNEHMERDATEN

Darf ich als Veranstalter die Teilnehmerliste weitergeben?

Rechtsgrundlage Vertragserfüllung? Nein, klappt nicht. Bleiben also berechtigtes Interesse und Einwilligung.

Die Weitergabe an einen externen Referenten kann ich, soweit würde ich mich hier aus dem Fenster lehnen, doch mit einem gewissen berechtigten Interesse rechtfertigen. Transparenz schadet hier aber sicher nicht, also der Hinweis auf die Weitergabe in den Datenschutzinfos und eventuell sogar ein Widerspruchsrecht.

Die Weitergabe der Teilnehmerliste an alle anderen Teilnehmer? Da wird es unter Umständen schon eng für ein berechtigtes Interesse. Das würde man wohl, wenn man es wasserdicht machen will, nur mit Einwilligung der Teilnehmer machen.

Wobei: Ich kann hier ja auch versuchen, am Vertragsinhalt zu arbeiten. Wenn ich den Vertrag dahingehend erweitere, dass es bei meiner Datenerhebung um die Teilnahme an einer Community geht, innerhalb derer in einer geschlossenen

Gruppe ein fachlicher Austausch stattfindet, und eben auch, aber nicht nur, um die Teilnahme an einem gemeinsamen Kongress, dann könnte ich da meiner Meinung nach durchaus die Weitergabe der Daten als Teil des Vertrages sehen.

VISITENKARTE

Wie sieht das aus, wenn mir jemand seine Visitenkarte überreicht? Darf ich dem dann E-Mail-Werbung schicken?

Es kommt darauf an, sagt der Jurist ja ganz gerne. Und hier ist es auch so. Es kommt darauf an, was im Zusammenhang mit der Übergabe der Visitenkarte gesagt wurde. Wenn der Visitenkarten-Überreicher sagt „Ich finde Ihre Produkte total toll und würde gerne Ihren Newsletter erhalten“, dann stellt das schon mal eine mündliche Einwilligung dar. Dummerweise muss ich diese Einwilligung aber im Zweifel vor Gericht beweisen – und wenn der Visitenkarten-Überreicher sich partout nicht mehr daran erinnern will, mündlich eingewilligt zu haben, dann stehe ich dumm da. Daher auch hier, wenn man auf Nummer Sicher gehen will: Double-Opt-In!

Apropos Visitenkartenübergabe: Eigentlich gelten die Informationspflichten aus der DSGVO auch hier. Ich müsste also jemanden, der mir seine Visitenkarte reicht, eigentlich darüber informieren, was ich mit den Daten zu tun gedenke, wo ich die Daten speichere, wie lange und so weiter. Das ist natürlich ein bisschen absurd, wenn man sich das so live vorstellt. Aber wenn Sie am Messestand so eine klassische Glasschüssel haben, in die ich meine Visitenkarte werfen kann, um auf den Newsletter-Verteiler zu kommen – dann legen sie da doch eine kurze, prägnante Datenschutzinfo aus. Ich denke nicht, dass das absurd rüberkommt. Ich persönlich finde das professionell und würde das positiv abspeichern.

Die Speicherung der Kontaktdaten im CRM-System kann auch ohne ausdrückliche Einwilligung auf Basis eines sogenannten “berechtigten Interesses” zulässig sein, wobei man sich dabei bewußt machen sollte, dass die Daten nicht für alle Ewigkeit gespeichert werden dürfen. Es sollten auch hier bestimmte Löschroutinen (z.B. “1 Jahr nach dem letzten Kontakt”) definiert werden.

Wie man bei der Übergabe einer Visitenkarte zu 110% rechtskonform seinen Informationspflichten nachkommen müsste, wird in diesem Artikel hier recht humorvoll pointiert dargestellt: The new procedure for exchanging business cards under GDPR

SPEICHERN DER TEILNAHME IM CRM

Darf ich die Information, dass ein Bestandskunde an meinem Event teilgenommen hat, in meinem CRM bei dem Kunden hinterlegen? Einwilligung habe ich nicht, aber auf Basis eines berechtigten Interesses kann ich das wohl rechtfertigen.

VERÖFFENTLICHUNG VON FOTOS

Fotos von Teilnehmern darf man grundsätzlich nur mit der Einwilligung der Abgebildeten veröffentlichen. Das steht so im Kunsturhebergesetz und das Kunsturhebergesetz sieht da dann auch nicht zahlreiche Ausnahmen vor. So zum Beispiel eben gerade für Bilder von Events – und das Kunsturhebergesetz geht in diesem Bereich dem Datenschutzrecht vor. Zumindest bisher. Wie das zukünftig sein wird, weiß man noch nicht so genau. Da streiten sich die großen Geister der Datenschutzzunft gerade feurig drüber. Die DSGVO sieht so einen Vorrang des Kunsturhebergesetzes nicht unbedingt vor. Das würde dann aber heftige Auswirkungen auf die journa-

listische Bildberichterstattung haben und theoretisch zu krassen Zensurmöglichkeiten führen. Und das kann ja eigentlich nicht sein und nicht gewollt sein. Insofern würde ich aktuell davon ausgehen, dass sich da nichts elementar ändern wird. Sein kann aber natürlich alles.

WEITERLEITUNG EINER EINLADUNG

Ist „Tell-a-friend“ bzw. die Weiterleiten einer Einladung an einen Dritten durch den Empfänger der originären Einladung weiter zulässig?

Der Empfänger einer Einladung zu einer Veranstaltung darf diese natürlich per E-Mail weiterleiten. Daran ändert die DSGVO ausnahmsweise mal gar nichts.

Die Nutzung von Tell-a-Friend-Funktionen auf der Webseite war schon immer heikel, auch daran ändert die DSGVO nichts. Bei Tell-a-Friend-Funktionen ist die große, entscheidende Frage immer: Wer ist Versender der E-Mail? Wenn der Veranstalter auf seiner Webseite eine Tell-a-Friend-Funktion anbietet, bei der ein Webseitenbesucher seine Freunde per E-Mail zu einem Event einladen kann, wird der Veranstalter auf jeden Fall als Versender der E-Mail angesehen, wenn er als Absender der jeweiligen E-Mail genannt wird. Die E-Mails sollten immer so gestaltet sein, dass der einladende “Freund” als Versender genannt wird. Weitere Maßnahmen zur Reduzierung des rechtlichen Risikos bei der Nutzung von Tell-a-Friend-Funktionen sind ausführlich in der “eco Richtlinie für zulässiges E-Mail-Marketing“ (Seiten 14 - 16) erläutert.

VEREINBARUNG AUFTRAGS-VERARBEITUNG

Wie muss eine Vereinbarung Auftragsverarbeitung mit Sub-Auftragnehmern aussehen. Gibt es Beispiele?

Wie schon bisher im guten, alten Bundesdatenschutzgesetz (BDSG) muss auch nach DSGVO mit Auftragsverarbeitern eine ausführliche Vereinbarung abgeschlossen werden, in der die Details der Datenverarbeitung geregelt sind. Die Anforderungen der DSGVO an eine solche Vereinbarung Auftragsverarbeitung unterscheiden sich dabei in einigen Punkten von den bisherigen Anforderungen des BDSG, so dass es leider meist erforderlich sein wird, bestehende Vereinbarungen zu ergänzen oder zu ersetzen.

Es gibt zahlreiche Vorlagen und Beispiele, manche sind wirklich gut und empfehlenswert, manche sind mit Vorsicht zu genießen.

Das Bayerische Landesamt für Datenschutzaufsicht hat eine Vorlage veröffentlicht, die absolut empfehlenswert ist (auch unabhängig davon, dass man mit einem Muster der Aufsichtsbehörde ja so falsch nicht liegen kann), abrufbar hier: https://www.lda.bayern.de/media/muster_adv.pdf

Die meisten großen Anbieter von SaaS-Plattformen stellen ihren Kunden jedoch ihrerseits bereits fertige Vereinbarungen Auftragsverarbeitung zur Verfügung, die im Regelfall lediglich gegengezeichnet werden müssen.

Auch doo stellt den Kunden selbstverständlich eine solche Vorlage zur Verfügung. Kontaktieren Sie dazu einfach unter datenschutz@doo.net.

VERARBEITUNGSVERZEICHNIS

Wie muss das Verarbeitungsverzeichnis aussehen?

Die Idee hinter dem Verarbeitungsverzeichnis ist es, die Datenverarbeitung im Unternehmen transparent zu machen. Das Verarbeitungsverzeichnis soll Auskunft geben darüber, welche personenbezogenen Daten erhoben werden, wo und wie sie verarbeitet werden, was die Rechtsgrundlage der jeweiligen Datenverarbeitung ist, wie der Datenschutzbeauftragte erreicht werden kann etc.

Auch für das Verarbeitungsverzeichnis gibt es inzwischen jede Menge Vorlagen. Und auch hier bietet sich natürlich wieder das Muster der Datenschutzaufsichtsbehörden an: https://www.lda.bayern.de/de/infoblaetter.html

Das Bayerische Landesamt stellt darüber hinaus noch zahlreiche Musterverzeichnisse für kleine Unternehmen und Vereine zur Verfügung: https://www.lda.bayern.de/de/kleine-unternehmen.html

doo SMART EVENT AUTOMATION

Sprechen Sie mit einem Experten!

doo GmbH

Hultschiner Straße 8, 81677 München
+49 89 24 88 15 35 5
sales@doo.net
doo.net