DSGVO-konformer Datenschutz im Veranstaltungsmanagement

Die wichtigsten Fragen und Antworten für Organisatoren von Seminaren, Kursen & Weiterbildungen

Das Thema Datenschutz hat mit der Datenschutz-Grundverordnung (DSGVO) weiter an Bedeutung gewonnen. Unternehmen haben noch bis zum 25.05.2018 Zeit, ihre Prozesse mit den Anforderungen der DSGVO in Einklang zu bringen. Die Zeit drängt und nicht allen Unternehmen ist im Einzelnen bewusst, was auf sie zukommt. Als Hersteller und Betreiber einer Seminarmanagementsoftware haben wir uns mit dem Thema natürlich ausführlich auseinandergesetzt und geben heute einen Einblick in das Thema speziell für Organisatoren von Veranstaltungen, Weiterbildungen und Seminaren. Als Experten steht uns der auf Software- und Datenschutzrecht spezialisierte Rechtsanwalt Dr. Christoph Giebel in einem Interview Rede und Antwort.

Herr Dr. Giebel, ab dem 25.05.2018 muss die Datenschutz-Grundverordnung in der EU unmittelbar angewandt werden. Sie harmonisiert damit weitergehend die bisherigen Regelungen der einzelnen Mitgliedsländer und bringt etliche der schon im bestehenden BDSG verankerte strenge Grundsätze auf die europäische Ebene. Auf welche Neuerungen müssen Unternehmen vorbereitet sein?

Die Datenschutz-Grundverordnung schreibt in der Tat in vielen Bereichen bereits bestehende Regelungsansätze fort. So gab es schon unter der bisherigen EU-Datenschutzrichtlinie und dem deutschen BDSG z.B. Grundprinzipien wie Zweckbindung und Datensparsamkeit sowie Meldepflichten bei Datenschutzverstößen. Die DGSVO geht nun unter dem Gesichtspunkt der Harmonisierung allerdings einen Schritt weiter. Sie beansprucht – anders als die Richtlinie – unmittelbare Geltung in allen Mitgliedstaaten und will damit für eine weitgehende Vereinheitlichung der Rechtsanwendung und Verfahrensvereinfachung in allen Mitgliedstaaten sorgen.

Zugleich verschärft die DSGVO in vielen Bereichen nachhaltig die inhaltlichen und operativen Anforderungen an die Datenverarbeitung. So müssen Unternehmen z.B. künftig im Rahmen einer sehr weitreichenden Rechenschaftspflicht ihre Datenverarbeitungsprozesse viel genauer dokumentieren und dies auf behördliches Verlangen nachweisen. Zugleich sind Betroffenenrechte deutlich erweitert worden, etwa im Bereich der Informationspflichten, bei Auskunfts- und Widerspruchsrechten oder durch die Einführung des neuen Rechts auf Datenportabilität.

Die Stärkung der Betroffenenrechte betrifft aber auch die Sanktionen bei Datenschutzverstößen. Betroffene können dabei künftig immaterielle Schäden im Sinne eines Schmerzensgeldes geltend machen und sich im Übrigen bei sonstigen Schäden auf nennenswerte Beweiserleichterungen berufen – ein nicht zu unterschätzendes Risiko für Unternehmen. Zudem hat die DSGVO den Bußgeldrahmen bei Datenschutzverstößen deutlich angehoben. Während bislang unter dem BDSG maximal Bußgelder in Höhe von EUR 300.000,- verhängt werden konnten, sind künftig unter der DSGVO Bußgelder von bis zu EUR 20 Millionen oder gar 4% des weltweiten Konzernumsatzes möglich.

Unternehmen sollten sich ferner bewusst sein, dass der durch die DSGVO angestoßene Änderungsprozess mit dem 25. Mai 2018 noch nicht zu Ende ist, sondern viele weitere Jahre andauern wird. So fehlen etwa noch viele normkonkretisierende Vorschriften, wie z.B. delegierte Rechtsakte der EU-Kommission und Richtlinien der Aufsichtsbehörden. Die Rechtsanwendungspraxis der Aufsichtsbehörden und Gerichte – insbesondere des Europäischen Gerichtshofs – wird aufmerksam zu verfolgen sein und immer wieder Anlass zu Anpassungen geben. Es bleibt also spannend.

Ein zentraler Punkt der Verordnung sind die definierten Grundsätze zur Verarbeitung personenbezogener Daten:

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**
- **Zweckbindung**
- **Datenminimierung**
- **Richtigkeit**
- **Speicherbegrenzung**
- **Integrität und Vertraulichkeit**
- **Rechenschaftspflicht**

Dabei findet zur Einhaltung immer eine Abwägung der Interessen der Beteiligten statt. Können Sie kurz skizzieren, wie diese Abwägung sinnvoll umgesetzt werden kann?

Datenschutzrecht ist seit jeher kein mathematisch-akkurates Recht mit klarem Wenn-Dann-Schema. Es ist davon gekennzeichnet, dass dort, wo belastbare Einwilligungserklärungen fehlen, berechtigte Interessen und widerstreitende Belange gegeneinander abgewogen werden müssen. Dass dabei Wertungsspielräume bestehen, liegt in der Natur der Sache. Ich empfehle allen Lesern und Leserinnen, einmal beispielhaft einen Blick in die zentrale Norm des Art. 6 der DSGVO zu werfen, der die Rechtmäßigkeit der Datenverarbeitung regelt. Ich vermute, dass viele Nicht-Juristen sich wohl stirnrunzelnd fragen werden: Was ist denn das für ein Gummi-Paragraf? Trotz der Abstraktionshöhe mancher Vorschriften schafft es die Rechtspraxis aber, diese Bestimmungen verlässlich zu handhaben. Die bereits erwähnte Rechenschaftspflicht und die mit ihr einhergehende Verschriftlichung sind in diesem Zusammenhang hilfreich. Sie zwingen Unternehmen zu einer sehr ernsthaften und gründlichen Befassung mit der Thematik und ermöglichen damit argumentative Feinsteuerung. Wo Unsicherheiten im Abwägungsprozess verbleiben, kann es manchmal auch sinnvoll sein, proaktiv das Gespräch mit der Aufsichtsbehörde zu suchen, vorzugsweise durch die Vermittlung eines Rechtsanwalts, der gegebenenfalls vertraulich auf einer „No Names“-Basis bei der Behörde vorspricht.

Für die Abwägung bei besonders kritischen Datenverarbeitungen sieht die DSGVO darüber hinaus das Instrument der sog. Datenschutz-Folgenabschätzung vor. Sie findet Anwendung bei besonders risikoträchtigen Datenverarbeitungen, insbesondere der Einführung neuer Technologien, wie etwa im Bereich des Profiling zum Zweck von Predictive Analytics. Es müssen dann Risiken und Risikominimierungsansätze zusammen mit dem Datenschutzbeauftragten im Einzelnen erörtert und dokumentiert werden. Erforderlichenfalls kann das Unternehmen sogar gehalten sein, sich proaktiv mit seinem Vorhaben gegenüber der Aufsichtsbehörde zu öffnen.

Wenn ein Veranstaltungsorganisator sich entscheidet, eine Seminarverwaltungs-software einzuführen, dann kann dies entweder in der Cloud oder On-Premises erfolgen. Was muss man im letzteren Fall, also bei der Installation auf unternehmens-eigenen Rechnern, beim Betrieb der Software beachten?

Wie bei anderen Datenverarbeitungsvorgängen muss das Unternehmen angemessene technische und organisatorische Maßnahmen ergreifen, um die Datensicherheit auf den eigenen Servern zu gewährleisten. Das durch die DSGVO bekräftige „Privacy by default"-Prinzip (Datenschutz durch datenschutzfreundliche Voreinstellung) verlangt, die Software dabei so zu betreiben und zu administrieren, dass DSGVO-Postulaten wie etwa der Datenminimierung fortwährend Rechnung getragen wird, also z.B. durch ein Löschungs-management sichergestellt ist, dass nicht mehr benötigte personenbezogen Daten fortlaufend gelöscht werden. Auch wenn die Software auf unternehmenseigenen Rechnern betrieben wird, muss natürlich im Blick behalten werden, welche Dritten auf die gespeicherten Daten Zugriff nehmen. Sofern externe Dienstleister im Rahmen der Softwarepflege – vor Ort oder Remote – Zugang zu der Applikation erhalten, kann dies den Abschluss einer Auftragsverarbeitungsvereinbarung erforderlich machen.

Was muss man berücksichtigen, wenn man sich für eine Seminarverwaltungssoftware in der Cloud entscheidet und damit eine Auftragsverarbeitung bei externen Dienstleistern durchführen lässt?

Bei Nutzung einer cloud-basierten Lösung gelten im Grundsatz die gleichen Maßstäbe. Daher muss der Verantwortliche mit dem Cloud-Anbieter regelmäßig eine Auftrags-verarbeitungsvereinbarung schließen und sicherstellen, dass der Auftragsverarbeiter für die nötige Daten-sicherheit sorgt. Besonderes Augenmerk ist zudem gefordert, wenn der betreffende Server des Cloud-Anbieters, auf dem die personenbezogenen Daten gespeichert sind, in Drittstaaten, d.h. außerhalb von EU oder EWR, gelegen ist. Ein solcher Daten-transfer in Drittstaaten ist datenschutzrechtlich prinzipiell zusätzlich rechtfertigungsbedürftig. Es muss dabei durch den Verantwortlichen sichergestellt werden, dass der Auftrags-verarbeiter im Drittstaat ein angemessenes Datenschutzniveau beachtet. Eine solche Absicherung bieten nach gegenwärtigem Stand etwa die Vereinbarung der Standard-vertragsklauseln der EU-Kommission, Binding Corporate Rules oder aber – speziell für die Vereinigten Staaten – eine Zertifizierung im Rahmen des US Privacy Shield.

Veranstalter von Seminaren und Weiterbildungen speichern Informationen darüber, welche Seminare eine Person besucht hat, um Empfehlungen für weitere Veranstaltungen zu geben oder z.B. eine pflichtmäßige Auffrischung bestimmter Kurse zu überwachen. Diese Informationen sind der Verordnung nach besonders schützenwerte Daten, da sie Rückschlüsse über das Verhalten von Personen ermöglichen. Welche Anforderungen ergeben sich dadurch in Punkto Transparenz über die Verarbeitung sowie Datensicherheit bei der Verarbeitung?

Für Transparenz sorgen in diesem Zusammenhang insbesondere die Pflicht, bereits bei der Erhebung der Daten über die Zwecke der Verarbeitung zu informieren. Dies gilt übrigens auch, wenn sich die Zweckbestimmung später ändern sollte und z.B. im Rahmen eines Data Science- oder Big Data-Ansatzes unterschiedliche Datensätze zu neuen analytischen Zwecken zusammengeführt werden sollen. Dann bedarf es einer erneuten Information

gegenüber dem Betroffenen. Gleichermaßen muss ein Unternehmen, welches eine wirksame Einwilligung des Betroffenen zu einer bestimmten Datenverarbeitung einholen will, hierzu in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache auffordern. Unter Datensicherheitsgesichtspunkten dürfen sich indes keine substanziellen Abweichungen von dem bislang Gesagten ergeben; es sind dem jeweiligen Einzelfall angemessene technische und organisatorische Maßnahmen zu ergreifen.

Wir danken Herrn Dr. Giebel für die ausführlichen Erläuterungen zur aktualisierten DSGVO!

Fazit

Abschließend können wir also festhalten, dass eine zentrale Herausforderung speziell für Organisatoren von Veranstaltungen und Seminaren darin besteht, jederzeit Auskunft zu gespeicherten personenbezogenen Daten geben und diese auf Anfrage vollständig löschen zu können.

Die Nutzung unterschiedliche Systeme oder das Arbeiten mit Excel-Listen erschwert oder verhindert gar die nötige Transparenz. Daher scheint es von entscheidender Bedeutung, mit einem zentralen Tool zu arbeiten, das sämtliche Prozesse und Daten rund um die Veranstaltungen einheitlich und übergreifend abwickelt und so eine konsistente und jederzeit aktuelle Datenbasis gewährleistet.

Dr. Christoph Giebel ist Gründungspartner von JURICITY Rechtsanwälte, einer maßgeblich auf Technologie- und Immobilienrecht ausgerichteten Kanzlei mit Standorten in München und Frankfurt am Main. Als Fachanwalt sowohl für IT-Recht als auch für Urheber- und Medienrecht ist Herr Dr. Giebel maßgeblich auf die technologienahe Rechtsberatung spezialisiert, dies insbesondere in den Bereichen Software und Datenschutz. Herr Dr. Giebel hat in den vergangenen Monaten zahlreiche Unternehmen in ihren Vorbereitungen auf die Anforderungen der DSGVO beratend begleitet.

simplyOrg

simplyOrg ist eine Software zum umfassenden Wissensmanagement. Durch das Tool werden Arbeitsabläufe bei der Organisation von Kursen, Seminaren und Weiterbildungen automatisiert und die Arbeit damit wesentlich erleichtert.

Sämtliche Prozesse lassen sich zentral und übersichtlich steuern - von der Planung und Vorbereitung über die Teilnehmerverwaltung und -gewinnung per Online-Portal bis zur Nachbereitung und Abrechnung der Kurse. Checklisten und Vorlagen erleichtern die Arbeit der einzelnen Planer und fördern die Transparenz in Abteilungen und Teams.

plus-IT GmbH

Dr.-August-Einsele-Ring 20
82418 Murnau am Staffelsee

http://simplyorg.de +49 (0)8841 487760 kontakt@plus-it.de