Daten gut geschützt?

Die Ende Mai in Kraft tretende EU-weite Datenschutz-Grundverordnung betrifft auch den Alltag von Chören. Worauf es jetzt zu achten und was es zu verändern gilt

Von Nora-Henriette Friedel

Es ist in aller Munde: Ab dem 25. Mai tritt die neue EU-Datenschutz-Grundverordnung in Kraft. Die gilt dann europaweit für alle, die personenbezogene Daten verarbeiten, sofern sie das nicht im privaten Rahmen tun. Also auch für kleine Vereine, die eine Mitgliederdatenbank pflegen. Diese neue Gesetzgebung hat zum Ziel, das Recht auf informationelle Selbstbestimmung jedes und jeder Einzelnen zu stärken. Denn in der Informationsgesellschaft zeigt sich mehr und mehr, dass persönliche Daten für diverse Zwecke ausgenutzt oder missbraucht werden – sei es für individualisierte Produktwerbung, die im Internetbrowser erscheint, oder für politische Beeinflussung mittels gezielter Facebook-Posts.

«Hintergrund der neuen EU-weiten Datenschutz-Grundverordnung ist es im Prinzip, einer Gewinnmaximierung auf der Basis von vermeintlich unbedeutenden Informationen wie den personenbezogenen Daten Einhalt zu gebieten. Außerdem soll mehr Transparenz beim Umgang mit Daten hergestellt werden», sagt Jan Morgenstern, Fachanwalt für IT-Recht. Der Rechtsanwalt aus Speyer berät Unternehmen bundesweit und international in allen IT- und internetrechtlichen Fragen. Als zertifizierter Datenschutzbeauftragter überwacht er zu-

dem die datenschutzrechtlichen Strukturen diverser Unternehmen und Unternehmensgruppen.

Doch was hat das alles mit der alltäglichen Praxis im Chor zu tun, der ja meist als Verein organisiert ist? Wie hängt der Choralltag mit dem zusammen, was man allenthalben lesen kann, dass zum Beispiel Verstöße gegen die neue EU-Datenschutz-Grundverordnung (EU-DSGVO) mit Bußgeldern bis zu 20 Millionen Euro beziehungsweise vier Prozent des weltweiten Jahresumsatzes geahndet werden. «Das ist natürlich etwas, das die Leute aufschreckt, zusammen mit den Medienberichten über Hackerangriffe, Trojaner oder jüngst dem Cambridge-Analytica-Skandal bei Facebook», sagt Jan Morgenstern. «Und die gesteigerte Haftungsträchtigkeit im Zusammenhang mit Verstößen gegen die neue Datenschutzverordnung sorgt natürlich dafür, dass die Wertigkeit von Datenschutz anders wahrgenommen wird als bislang.» Sprich: Die hohen Bußgelder schrecken ab und genau das sollen sie.

WENIG BAHNBRECHEND NEUES IN DATENSCHUTZ-GRUNDVERORDNUNG

Doch wer bisher den Vorgaben des Bundesdatenschutzgesetzes (BDSG) entsprochen hat, für den stellt sich die Situation relativ entspannt dar, der muss jetzt nur an einigen Stellen Anpassungen vornehmen und feinjustieren, um der EU-DSGVO nachzukommen. «Denn die EU-DSGVO enthält gegenüber dem aktuell geltenden Recht nicht viel bahnbrechend und grundsätzlich Neues», sagt Jan Morgenstern. «Das eigentliche Problem ist, dass den wenigsten ihre Pflichten in puncto Datenschutz nach aktueller Gesetzeslage bekannt sind. Folglich ist in der Praxis oft nicht umgesetzt, was längst hätte umgesetzt sein müssen», so der Rechtsanwalt, der auch Seminare und Lehrgänge zum Thema Datenschutz für Betriebe und Verbände durchführt.

«Das eigentliche Problem ist, dass schon die Datenschutz-Pflichten nach aktueller Gesetzeslage den wenigsten bekannt sind.»

Jan Morgenstern,
Fachanwalt für IT-Recht in Speyer

Doch noch einmal ganz von vorn: Worum geht es in der neuen Datenschutz-Grundverordnung? Die EU-DSGVO betrifft personenbezogene Daten, also sämtliche Informationen, die sich auf eine identifizierbare oder identifizierte natürliche Person beziehen. Das sind zum Beispiel Name, Geburtsdatum, Wohnort, Steuernummer, Bankverbindung, Religionszugehörigkeit oder auch bestimmte Gesundheitsdaten wie etwa eine Lebensmittelallergie. Auch Fotos, die Menschen abbilden, enthalten personenbezogene Daten. Das neue Gesetz regelt die Verarbeitung solcher Daten, worunter man deren Erhebung, Speicherung, Änderung, Nutzung, Übermittlung, Verknüpfung mit anderen Daten und Löschung versteht. In welcher Form man die Daten verarbeitet – digital oder im Aktenordner – ist dabei egal.

DIENT DATENERHEBUNG WIRKLICH DEM VEREINSZWECK?

Laut EU-DSGVO dürfen Daten nur dann verarbeitet werden, wenn es dafür entweder eine gesetzliche Grundlage gibt oder aber eine ausdrückliche Einwilligung der Betroffenen. Eine gesetzliche Grundlage besteht etwa, wenn Daten im Rahmen einer vertraglichen Beziehung verarbeitet werden müssen. Bei Vereinen ist diese vertragliche Beziehung die Mitgliedschaft. Die für die Mitgliederverwaltung erforderlichen Daten – Name, E-Mail-Adresse, Telefonnummer, Stimmgruppe, gegebenenfalls Kontoverbindung – dürfen also in jedem Fall verarbeitet werden. Auch beispielsweise das vereinsinterne Veröffentlichen der E-Mail-Adressen aller Mitglieder in einer Kontaktliste wäre rechtmäßig, wenn der Vereinszweck auch darin besteht, den Austausch unter den Mitgliedern zu fördern. Daten, die nicht zwingend zum «Zwecke der Vertragserfüllung» erforderlich sind, dürfen nur nach Einwilligung der Betroffenen verarbeitet werden, so zum Beispiel das Geburtsdatum.

Fragt ein Vorstandsmitglied in der Vorbereitung einer Probenfahrt zum Beispiel die Essenswünsche der Mitglieder ab – Egal? Vegetarisch? Glutenfrei? – besteht auch hier eine eigene vertragliche Grundlage, nämlich das Veranstaltungsmanagement der Reise, das ein berechtigtes Interesse daran hat, diese Informationen zu verarbeiten. Es wäre also legitim, diese Daten zu erheben, ebenso wie sie zu speichern, sofern solche Reisen regelmäßig organisiert werden.

Die eben erläuterte *Rechtmäßigkeit* der Datenverarbeitung ist einer der Grundsätze der Verarbeitung personenbezogener Daten. Diesen und weitere Grundsätze nennt die EU-DSGVO im Artikel 5: so auch die gerade angesprochene *Zweckbindung:* Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden. Außerdem sollen nicht mehr Daten verwendet werden als wirklich notwendig, das ist der Grundsatz der *Datenminimierung*. Vorsichtshalber alle Geburtsdaten der Mitglieder zu erheben, auch wenn man damit nichts Bestimmtes vorhat, wäre also zum Beispiel «abstrakte Datenhaltung» und damit rechtswidrig. Ein weiterer Grundsatz ist der der *Richtigkeit*, sprich: Falsche Daten sind unversehens zu löschen und zu korrigieren. Zudem gilt der Grundsatz der *Speicherbegrenzung*: Gespeicherte Daten dürfen die Identifizierung der betroffenen Personen nur so lange ermöglichen, wie es erforderlich ist. «Karteileichen» ausgetretener Vereinsmitglieder müssen daher schnellstmöglich gelöscht werden. Der Grundsatz der *Integrität und Vertraulichkeit* schreibt vor, dass verarbeitete Daten gesichert und geschützt werden müssen: vor unbefugtem Zugriff, vor unbeabsichtigtem Verlust oder versehentlicher Schädigung.

WER DATEN ERHEBT, IST ZUR AUSKUNFT DARÜBER VERPFLICHTET

Vereinsvorstände sollten sich also fragen, ob sie all dem bei der Verarbeitung ihrer Mitgliederdaten Genüge tun – und wo nicht, entsprechend aufräumen: ungenutzte und veraltete Daten löschen, Transportverschlüsselungen beim E-Mail-Server und auf Webseiten einrichten (zu erkennen am «https» beziehungsweise dem geschlossenen Vorhängeschloss-Symbol in der Adresszeile des Browsers), Dateien und Dokumente verschlüsseln beziehungsweise mit passwortgeschütztem Zugriff versehen, Sicherheitskopien anfertigen und so weiter. Hat man das erledigt, ist schon einmal viel gewonnen.

Erhebt ein Verein Daten, etwa von künftigen Mitgliedern im Beitrittsformular, von Förderern oder von Menschen, die den Chor-Newsletter abonnieren wollen, hat er zudem die Pflicht, darüber zu informieren, was er mit den Daten zu welchem Zweck vorhat. Sofern ein Verein über seine Website personenbezogene Daten erhebt – zum Beispiel mit einem Kontaktformular – muss er auch dort in einem Datenschutzhinweis beziehungsweise einer Datenschutzerklärung folgendermaßen informieren: Er muss eine oder einen Verantwortlichen benennen und diese Person auf ihre Aufgaben verpflichten. Er muss die Zwecke der Datenverarbeitung samt deren Rechtsgrundlage darlegen sowie den Empfänger der Daten angeben, sofern sie weitergegeben werden sollen – beispielsweise an den Dachverband oder den Veranstalter eines Wettbewerbs, an dem ein Chor teilnehmen möchte. Außerdem muss informiert werden, wie lange die Daten gespeichert werden sollen – oder was Kriterien für die Löschung sind – und es muss auf folgende Betroffenenrechte hingewiesen werden: auf das Recht auf Auskunft, Berichtigung und Löschung der Daten, darauf, dass die Einwilligung in die Datenverarbeitung jederzeit widerrufen werden kann, und auf das Beschwerderecht bei der Aufsichtsbehörde. An die können sich Mitglieder nämlich wenden, falls ein Verein den genannten Betroffenenrechten nicht zügig nachkommt.

Manch ein Vereinsvorstand wird sich jetzt fragen, ob er nun seine Mitglieder rückwirkend noch über die Verarbeitung von Daten informieren muss, die er längst erhoben hat. Hier rät Jan Morgenstern, ⤶

den Ball flach halten, denn die Informationspflicht sei erst ab dem 25. Mai bindend. Ab dann gilt es jedoch, sich an die genannten Richtlinien zu halten.

Was ebenfalls hinzukommt, ist im Grundsatz die Verpflichtung, sämtliche Vorgänge der Datenverarbeitung zu dokumentieren. Genauer: Man muss ein so genanntes «Verzeichnis von Verarbeitungstätigkeiten» anlegen. Mit dessen Hilfe soll man gegenüber der Aufsichtsbehörde jederzeit nachweisen können, dass man sich rechtmäßig verhalten hat. Sowohl Betriebsführungen als auch Vereinsvorstände stellt das vor die Aufgabe, sämtliche Strukturen der Datenverarbeitungen zu erfassen. Doch die Mühe lohnt sich, verschafft man sich selbst doch dadurch Transparenz über interne Vorgänge.

Konkret muss das Verzeichnis von Verarbeitungstätigkeiten, egal ob digital oder schriftlich, mindestens Name und Kontaktdaten des oder der Verantwortlichen enthalten, die Zwecke der Datenverarbeitung benennen, die Kategorien betroffener Personen und personenbezogener Daten beschreiben, die Kategorien von Datenempfängern auflisten sowie möglichst die zur Datenlöschung vorgesehenen Fristen benennen. Zusätzlich empfiehlt es sich, die konkreten Verarbeitungstätigkeiten zu beschreiben und die entsprechenden Rechtsgrundlagen hierfür aufzuführen.

NACHBESSERUNG NÖTIG, WENN DIENSTLEISTER MIT IM BOOT SIND

Gibt ein Verein Daten in die Hände von Dritten, die in seinem Auftrag Daten verarbeiten, muss er mit den Dienstleistern einen Vertrag abschließen. Das betrifft etwa Anbieter webbasierter Chormanagement- beziehungsweise Mitgliederverwaltungsprogramme oder Online-Datenspeicher. Auch der Website-Provider zählt dazu, wenn dort im Passwort-geschützten Bereich beispielsweise Kontaktdaten der Mitglieder zu finden sind oder wenn es auf der Homepage ein Kontaktformular gibt, um Nachrichten an eine E-Mail-Adresse weiterzuleiten. Der Vertrag zwischen Verein und dem sogenannten Auftragsverarbeiter schreibt das Weisungsrecht des Vereins sowie die Aufgaben des Dienstleisters fest, verpflichtet diesen zu Vertraulichkeit und Sicherheit und legt fest, was nach Abschluss der Auftragsverarbeitung mit den Daten geschehen soll. An dieser Stelle werden auf viele Vereine wohl besonders aufwändige Nachbesserungen zukommen.

Das Bundesdatenschutzgesetz in seiner ab dem 25. Mai neuen Form schreibt außerdem vor, einen Datenschutzbeauftragten oder eine Datenschutzbeauftragte zu bestellen, sobald mindestens zehn Personen regelmäßig, also wiederkehrend personenbezogene Daten verarbeiten. Die Aufgabe von Datenschutzbeauftragten besteht vor allem in der Unterstützung des Vereins bei der Selbstkontrolle. Die oder der Datenschutzbeauftragte sollte sich fit machen in Sachen Datenschutz, die Verantwortlichen zu ihren Pflichten und die Betroffenen zu ihren Rechten beraten sowie die Einhaltung der gesetzlichen Vorschriften überwachen. Außerdem ist sie oder er Anlaufstelle für die Aufsichtsbehörde.

ÜBER BUSSGELDER WIRD IM EINZELFALL ENTSCHIEDEN

Was kann einem Verein drohen, wenn es zur Verletzung des Datenschutzes kommt – wenn personenbezogene Daten verloren gehen, fälschlicherweise gelöscht oder verändert werden, in unbefugte Hände geraten? Bei ernsthaften Verstößen ist durchaus mit Geldbußen in vier- bis fünfstelliger Höhe zu rechnen, laut EU-DSGVO sollen Geldbußen nämlich «in jedem Einzelfall wirksam, verhältnismäßig und abschreckend» sein. Eine Haftpflichtversicherung helfe hier in aller Regel nicht weiter, so Jan Morgenstern. Doch wie gesagt, es wird im Einzelfall entschieden. Und auch Gemeinnützigkeit fließe bei der Bußgeldbemessung ein – denn Vereinen die Existenzgrundlage zu entziehen, das sei auch von der EU-DSGVO nicht gewollt.

Die Autorin ist Redakteurin der *Chorzeit*.

Lesetipps & Vorlagen

«Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine. Das Sofortmaßnahmen-Paket», herausgegeben vom Bayerischen Landesamt für Datenschutz, Verlag C. H. Beck, Euro 5,50

Die Landesdatenschutzbeauftragten bieten Leitfäden zum Herunterladen an, beispielsweise: «Datenschutz im Verein nach der Datenschutz-Grundverordnung DSGVO»
www.baden-wuerttemberg.datenschutz.de

Hilfreich auch der Leitfaden des Schwäbischen Chorverbands:
www.s-chorverband.de/vereinsfuehrung/vereinsrecht

Muster und Vorlagen unter anderem für Verarbeitungsverzeichnis, Datenschutzerklärung für Vereinssatzung und -homepage, Verpflichtungsvertrag mit Dritten finden sich auf:
www.deutscher-chorverband.de