

Die neue Datenschutzgrundverordnung kurz erläutert

Am 25.5. lief die die zweijährige Übergangsfrist der im März 2016 in Kraft getretenen EU-Datenschutzgrundverordnung (EU-DSGVO) ab, nach der alle vorherigen EU-Datenschutz Bestimmungen ungültig wurden. Parallel dazu wurde auch das Deutsche Bundesdatenschutzgesetz (BDSG) erneuert. Dies wurde im Juli 2017 verabschiedet und erhielt ebenso am 25.5.2018 volle Gültigkeit.

Der 25. Mai führte vielfach zu Verunsicherungen. Vor allem kommen damit auch auf Vereine ein paar Aufgaben zu. Sie müssen sich aber nicht verrückt machen, denn wie so oft, wird nichts so heiß gegessen wie es gekocht wird. Schlimm war und ist derzeit allerdings die Verunsicherung, die von einigen „Fachleuten“ aus „bestimmten Gründen“ forciert wird.

Wichtig ist nach wie vor erstmal nur eines: Ihre Website weitestgehend rechtssicher gegen Abmahner zu machen.

Alles andere kommt danach. Der Chorverband der Pfalz ist bestrebt, die Chorvereine in den Maßnahmen und den damit verbundenen Aufwendungen aus der DSGVO so weit wie möglich zu entlasten.

Worum geht's? Die Datenschutzgrundverordnung will soweit wie möglich den Umgang mit personenbezogenen Daten regulieren, zum Wohl des Dateneigentümers. Hierzu gibt es generelle Aussagen, auf denen die DSGVO basiert, dazu ein paar Hinweise.

1. „Meine Daten gehören mir“

Im Wesentlichen besagt dies, dass Sie ohne die ausdrückliche Einwilligung des Dateninhabers keine über die dem bekannten Nutzungszweck hinausgehende Datensätze speichern/bevorraten dürfen.

Als Beispiel: Nehmen wir an, Sie betreiben einen Online-Shop. Dann muss vom Besteller explizit ein entsprechender Haken bei der Bestellung gesetzt werden, der eine weitere Nutzung der Daten, über die Bestellabwicklung hinausgehend, erlaubt. Die Haken dürfen auch nicht „voreingestellt“ sein, z.B. das voreingestellte Setzen beim Newsletter.

Erlaubt der Besteller keine weitere Nutzung seiner Daten, ist der Datensatz nach erfolgter Geschäftsabwicklung – unter Berücksichtigung eventueller gesetzlicher Aufbewahrungspflichten - zu löschen. Die personenbezogenen Daten dürfen nicht für andere Dienste weiterverwendet werden, für die keine Zustimmung des Dateninhabers existiert.

2. „Sparsamkeit bei der Datenvorhaltung“

Ist der Grundsatz, der sich aus der vorgenannten Pflicht zu Datenlöschung ergibt.

Personenbezogene Daten die nicht mehr für weitere Dienste benötigt werden, sind zu löschen.

3. „Verantwortungsvoller Umgang mit Datenmaterial“

Es sollte klar definiert sein, wer mit personenbezogenen Datensätzen umgehen darf. Nicht jeder sollte Zugriff auf personenbezogenen Daten haben dürfen. Insbesondere auf Vorstände kommt hier Verantwortung zu. Sie sollten jederzeit wissen, wann was mit den Datensätzen gemacht wird/wurde. Dies ist nur möglich, wenn der Vorstand weiß, WER Zugriff auf das Datenmaterial hat.

4. Was sind personenbezogene Daten?

Dies sind Daten, die namentliche Rückschlüsse auf den Inhaber zulassen, auch E-Mails und IP-Adressen gehören dazu. Der Gegensatz dazu sind anonymisierte Daten. Hierzu ein weiteres Beispiel: Sie sind im Besitz nicht anonymisierter Daten, wenn der Datensatz Postleitzahl und E-Mail-Adresse enthält. Hintergrund ist, dass es Ihnen Möglich ist, mit diesen beiden Komponenten Name und dazugehörige Adresse zu recherchieren – theoretisch. Anonymisiert ist der Datensatz, wenn die Mailadresse der Postleitzahl nicht zuzuordnen ist, d.h., die E-Mailadresse gelöscht wird.

5. Datenschutzbeauftragter gem. Art. 39 der DSGVO

Ein wesentlicher Kern der DSGVO ist der Datenschutzbeauftragte. Dieser ist bei Betrieben und Institutionen zu benennen, in den mindestens 10 Mitarbeiter mit personenbezogenen Daten umgehen. Das heißt auch einfach E-Mails versenden, denn wie zuvor beschrieben, gehört auch die Mail zu personenbezogenen Daten. Wenn Sie als Vereinsvorstand nicht 10 Leute aufweisen, die STÄNDIG und REGELMÄSSIG mit Daten umgehen, die Verarbeitung personenbezogener Daten NICHT ihr HAUPTZWECK ist, **dann ENTFÄLLT die Benennung eines Datenschutzbeauftragten für sie. Dies ist in einem Chorverein, auch in einem Chorverband in den allermeisten Fällen so.**

Basierend auf den Anforderungen aus Pkt. 3 KÖNNEN (nicht müssen) Sie jedoch aus Ihren Reihen eine/n für den Datenschutz Verantwortliche/n benennen. Das ist kein Datenschutzbeauftragter, sondern lediglich eine Person, die die Dinge nachhält und dokumentiert, die Ansprechpartner/in für evtl. Datenschutzbelange der Mitglieder ist.

Dies alles sind aber grundsätzliche Maßnahmen, die jetzt - nach und nach - in zweiter Instanz erfolgen können, da diese im „Innenverhältnis“ auszuführen sind. Kein Abmahnanwalt wird sie hieraufhin abmahnen können, denn lediglich gegenüber der Aufsichtsbehörde sind diese Vorgänge darzulegen.

Schützen Sie Ihre Website vor Abmahnern.

Sas ist jetzt wichtig:

Betreiben Sie als Chor/Chorverein eine Website? Jede impressumpflichtige Website – dazu gehören auch Vereinsseiten – müssen die nachfolgenden Anforderungen erfüllen um abmahnsicher zu sein. Private Webseiten betreffen diese Anforderungen nicht.

Ist Ihnen die Umsetzung der nachgenannten fünf Punkte nicht möglich, stellen Sie Ihre Seite bitte einstweilen offline.

1. Nutzen Sie hierzu Google Analytics zur statistischen Auswertung?

Dann fragen Sie Ihren Webhoster/Website-Programmierer, ob das Script „anonymizeIP“ eingebunden wurde. Dies ist bereits seit 2016 vorgeschrieben und kann kostenpflichtig abgemahnt werden. Dieses Script weist die Google Server an, die letzten drei Ziffern der IP-Adresse zu löschen. Damit ist die IP nicht mehr einer Person zuordenbar.

2. Setzen Sie den Datenschutzhinweis über einen zusätzlichen Link „Datenschutz“ in Ihre Website ein, die der Chorverband für Sie vorhält oder Ihnen sogar bereits zugesendet hat. Diese Datenschutzbestimmung ist sehr umfassend und bildet fast alle Eventualitäten ab. Sie sollten für Sie nicht Zutreffendes aus diesem Datenschutzhinweis streichen und ggfs.

Passagen auf Ihre Belange abändern. Wenn Sie z.B. keine Google Analytics integriert haben, brauchen Sie dazu auch keinen Hinweis in Ihre Datenschutzerklärung zu schreiben. Allenfalls den Satz „Diese Seite nutzt keine Google Analytics“.

3. Es ist jetzt endgültig notwendig, dass Sie sich die Zustimmung zur Datennutzung auf Ihren Seiten einholen. Auf vielen Seiten haben Sie sicherlich schon einmal den Hinweis auf Cookies gesehen, den Sie akzeptieren müssen um die Seite weiter zu nutzen. Dieser Hinweis muss beim Aufrufen der Seite erscheinen, wenn Sie Cookies verwenden – dies ist heute meistens der Fall. Sie können den Cookie-Hinweis um einen Zusatz wie: „...ich habe den Datenschutzhinweis (Link zu Datenschutzhinweis) auf dieser Seite gelesen“ ergänzen. Der Seitenbesucher muss dies akzeptieren.
4. Ergänzen Sie eventuelle Kontaktformulare auf Ihrer Website um einen Haken, der die Einwilligung zur Datennutzung gibt und erklären Sie auch, was Sie mit den Daten machen.

Hier ein Beispiel von der Seite des CVdP:

1. HINWEISTEXT

„Wir versichern:

Alle hier gemachten Angaben werden streng vertraulich behandelt. Die Angaben werden niemals an Dritte weitergegeben und auch nicht für andere Zwecke verwendet. Alle durch Sie bekannt gemachten Daten werden ausschließlich und einmalig zum Zwecke Seminaranmeldung/Seminar Durchführung und ausschließlich durch den Chorverband der Pfalz sowie dessen Dozenten genutzt. Wenn Sie einem weiteren Kontakt zum Empfang von Informationen zur Chorlandschaft im Chorverband/Kreis-Chorverband nicht zugestimmt haben, werden Ihre Kontaktdaten unmittelbar nach erfolgreicher Bearbeitung Ihrer Anfrage / nach Seminarabschluss gelöscht. Sie haben jederzeit das Recht auf Einsicht sowie Korrektur oder Löschung Ihrer beim Chorverband der Pfalz gespeicherten Daten.“

2. TEXT ZUM MARKIEREN

„Ich habe den Abschnitt WIR VERSICHERN zur Kenntnis genommen sowie die Datenschutzhinweise unter <https://www.chorverband-der-pfalz.de/wordpress/kontakt/datenschutz> gelesen. Ich erkläre mich mit dem Prozedere der Datenverarbeitung zum Zwecke der Seminaranmeldung/Seminar Durchführung einverstanden.“

5. Wenn Sie ein Kontaktformular/eine Newsletteranmeldung – kurz, Formulare in die personenbezogene Daten eingegeben werden – nutzen, ist es unabdingbar, dass Sie Ihre Seite SSL-verschlüsseln (<https://...>) Haben Sie keine Seitenverschlüsselung integriert, entfernen Sie die entsprechenden Formulare von der Seite, bis die Seite durch SSL-Verschlüsselung gesichert ist. Ihr Webhoster hat i.d.R. entsprechende Angebote.
6. Der CVdP wird eine Ansprechpartnerin für Datenschutzfragen benennen.

Zusammengefasst

Dies alles hört sich zunächst einmal schlimmer an, als es tatsächlich ist. Legen Sie aber vor allem besonderes Augenmerk auf Ihre Außendarstellung der Website, denn hier drohen die meisten

Abmahnfallen. Im Innenverhältnis sollten Sie nun nach und nach die genannten Punkte weiter abarbeiten.

Die Datenschutzgrundverordnung im Verein (Beispiel)

Ein Chorverein hat 200 Mitglieder, einen ersten Vorstand, einen Kassier sowie einen Schriftführer (Vorstand im Sinne des BGB) sowie drei Personen (Chorleiter), die nach der sog. Übungsleiterpauschale bezahlt werden. Die Mitgliederverwaltung erfolgt durch den Schriftführer selbst. Die Verwaltung der Mitgliedsbeiträge erfolgt dagegen durch den Kassierer. Der Verein betreibt zudem eine kleine Webseite, die bei einem Dienstleister gehostet ist, mit Mitgliederfotos.

Wesentliche Verarbeitungstätigkeiten sind z.B.:

- Lohnabrechnung (über einen externen Dienstleister)
- Mitgliederverwaltung
- Betrieb der Webseite des Sportvereins (über Hostingpaket eines externen Dienstleisters)
- Veröffentlichung von Mitglieder-/Vorstandsfotos auf der eigenen Webseite
- Beitragsverwaltung

Datenschutzbeauftragter (DSB)

Muss ein DSB vom Verein benannt werden?

NEIN (weniger als 10 Personen im regelmäßigen Umgang mit personenbezogenen Daten – dazu zählt auch das Versenden von E-Mails)

Verzeichnis (Liste) von Verarbeitungstätigkeiten

Ist ein solches Verzeichnis erforderlich?

JA (wegen der regelmäßigen Verarbeitung personenbezogener Daten)

Datenschutz-Verpflichtung von Beschäftigten

Ist eine solche Verpflichtung durchzuführen?

JA (da alle Mitarbeiter mit personenbezogenen Daten umgehen)

Informations- und Auskunftspflichten

Bestehen irgendwelche Informationspflichten?

JA (insb. in der Vereinssatzung sowie auf der Webseite in der Datenschutzerklärung)

Löschen von Daten

Gibt es eine Anforderung zur Datenlöschung?

JA (aber erst nach Ablauf gesetzlicher Aufbewahrungspflichten)

Sicherheit

Müssen die Daten besonders gesichert werden?

NEIN (etablierte Standardmaßnahmen sind ausreichend, um die Daten effektiv zu schützen)

Auftragsverarbeitung

Ist ein Vertrag zur Auftragsverarbeitung notwendig?

JA (sowohl mit dem Hosting-Anbieter als auch mit dem externen Lohnabrechner)

Bei Kreis-Chorverbänden mit den Chorvereinen, der Chorverband mit den Kreis-Chorverbänden.

Datenschutzverletzungen

Müssen bestimmte Vorfälle gemeldet werden?

JA (aber nur bei relevanten Risiken – eine einfache Online-Meldung beim Landes-Datenschutzbeauftragten RLP ist möglich)

Datenschutz-Folgeabschätzung (DSFA)

Muss eine DSFA vom Verein durchgeführt werden?

NEIN (da kein hohes Risiko bei der Datenverarbeitung im Verein besteht)

Videoüberwachung (VÜ)

Besteht eine Ausschilderungspflicht bezüglich VÜ?

NEIN (da keine Videoüberwachung im Verein durchgeführt wird. Es sei denn, Sie lassen z.B. Ihr Vereinsheim durch Videoaufzeichnungen überwachen.)

In einem zweiten Teil erläutern wir, was nun im Innenverhältnis weiter zu tun bleibt.