KUNSTRAUM IN Churfranken e.V

VR 200 417

Vertreten durch: 1. Vorsitzender, Dieter Mocka, Bachgasse 18, 63920 Großheubach, Tel. 01512 1324309

Stand: 26.02.2019

Datenschutzkonzept

Grundsätze des Datenschutzes

Grundsätzlich ist es verboten, personenbezogene Daten zu verarbeiten. Es besteht jedoch ein Erlaubnisvorbehalt. Personenbezogenen Daten wie Name, Geburtsdatum, Eintrittsdatum, Bankverbindung u.ä. von Mitgliedern, Spendern usw. sind zu schützen. Der Datenschutz bezieht sich auf das Erheben, Verarbeiten (Speichern, Verändern, Übermitteln, Sperren und Löschen) und Nutzung (jede Verwendung) von Daten. Dies ist nur zulässig, wenn sie für die Erfüllung des Vereinszweckes erforderlich sind. Wir erheben, verarbeiten und nutzen personenbezogene Daten nur, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung des Rechtsverhältnisses erforderlich sind. Dies erfolgt auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO, der die Verarbeitung von Daten zur Erfüllung eines Vertrags oder vorvertraglicher Maßnahmen gestattet. Dies bedeutet, wenn Daten im Rahmen einer vertraglichen Beziehung, wie einer Mitgliedschaft, erhoben werden müssen, ist keine gesonderte Erlaubnis erforderlich. Diese Daten dürfen für die Mitglieds-Verwaltung in jedem Fall verwendet werden.

Der Vorstand des Vereins hat die Verantwortlichkeit hinsichtlich der Beschreibung der Datenschutzziele, ggf. der Benennung eines Datenschutzbeauftragten, der Sicherung der Betroffenenrechte, zu Regelungen zur Datensicherheit und zur Datenlöschung und des Umgangs mit eventuellen Risiken und Vorfällen (s. „Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 lit. B. EU-DS-GVO“). Er hat regelmäßig den aus dem Datenschutzrecht resultierenden Dokumentationspflichten in Form von z.B. Richtlinien, Beschreibungen und Dokumentation der Abläufe, nachzukommen.

Die Verantwortlichen, dies gilt auch für Mitglieder, haben darauf zu achten, mit welchen Personen sie über welche Inhalte sprechen. Dabei sind stets die besonderen Vorgaben zur Schweigepflicht einzuhalten.

Datenschutzbeauftragter

Lt. DS-GVO muss kein Datenschutzbeauftragter benannt werden, da weniger als 10 Personen regelmäßig Umgang mit personenbezogenen Daten des Vereins haben.

Einwilligung

Entsprechend den Transparenzvorgaben der EU-DS-GVO hat der Verein die Mitglieder umfassend und nachvollziehbar über den Vorgang der Datenverarbeitung zu informieren. Besteht für den Vorgang keine weitere Rechtsgrundlage, so muss im Rahmen einer Einwilligung die betroffene Person erklären, dass sie mit der Verarbeitung der betreffenden personenbezogenen Daten einverstanden ist. Dies kann schriftlich oder auch elektronisch (E-Mail) erfolgen.

Verzeichnis der Verarbeitungstätigkeiten

Die EU-DSGVO sieht vor, alle im Verein anfallenden konkreten Verarbeitungstätigkeiten, bei welchen personenbezogene Daten tangiert werden, zu dokumentieren. Jeder einzelne Prozess dazu ist zu identifizieren und entsprechend der Mustervorgabe (s. „Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen gem. Art. 30 Abs. 1 lit. B. EU-DSGVO“) zu beschreiben. Die einzelnen Dokumente sind im „Verzeichnis von Verarbeitungstätigkeiten“ zusammen zu führen.

Datenschutz-Folgeabschätzung (DSFA)

Es muss keine DSFA durchgeführt werden, da kein hohes Risiko bei der Datenverarbeitung im Verein besteht.

Auftragsdatenverarbeitung
Mit externen Dienstleistern, die Zugriff auf personenbezogene Daten erhalten, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann müssen nach Art. 28 EU-DS-GVO Verträge zur Auftragsdatenverarbeitung geschlossen werden. Dort ist die genaue Abgrenzung der Rechte und Pflichten festgelegt.

Sicherheit der Verarbeitung
Im Vordergrund steht eine Risikoanalyse, bei der die Eintrittswahrscheinlichkeit, einer Gefährdung für die Rechte und die Freiheiten der Betroffenen berücksichtigt werden soll. Lt. Bayer. Landesamt für Datenschutzaufsicht „Anforderungen der DS-GVO an Vereine“ sind etablierte Standardmaßnamen ausreichend, um die Daten zu schützen. Hier im Besonderen ist darauf zu achten, dass Computer mit Passwort und Firewall geschützt sind. Das Passwort muss für unbefugte Dritte unzugänglich aufbewahrt werden. Bei der Dokumentation in Schriftform ist darauf zu achten, dass der Zugriff für unbefugte Dritte nicht möglich ist (evtl. verschlossener Schrank, separater Raum – kein Zugang von Dritten möglich).
Der Verein weist darauf hin, dass die Datenübertragung im Internet (z.B. bei der Kommunikation per E-Mail) Sicherheitslücken aufweisen kann. Ein lückenloser Schutz der Daten vor dem Zugriff durch Dritte ist nicht möglich.
Der E-Mail-Verkehr erfolgt über ein g-mail-konto das mit einem Passwort geschützt ist (auf regelmäßige Änderung ist zu achten). Es besteht nur Zugriff durch den Vereinsvorstand bzw. durch ihn beauftragte Personen, bspw. für eine zeitlich begrenzte Aufgabenzuteilung. Es wird empfohlen, dies schriftlich zu dokumentieren, ebenfalls zur Verschwiegenheitspflicht (s. Anlage 2 „Verzeichnis von Verarbeitungstätigkeiten“ des Vereins).
Mehr Informationen zum Umgang mit Nutzerdaten des vereinsinternen Google-Kontos unter:
Datenschutzerklärung von Google: https://www.google.de/intl/de/policies/privacy/.
Für alle sonstigen digitalen Speicherungen ist darauf zu achten, dass keine Cloud-Speicher genutzt werden.

Betroffenenrechte
Die Rechte der Betroffenen umfassen
- Die Informationspflicht der Datenerhebung
- Das Recht auf Auskunft, Berichtigung und Löschung
- Das Recht auf Einschränkung der Verarbeitung
- Die Mitteilungspflicht bei Berichtigung, Löschung und Einschränkung der Verarbeitung
- Das Recht auf Datenübertragbarkeit
- Das Widerspruchsrecht
- Und das Profiling

Daten müssen gelöscht werden, wenn z.B. der Zweck entfällt (z.B. Ausstritt, Tod) oder der Betroffene seine Einwilligung zurückzieht. Das Recht auf Löschung wird beschränkt auf andere rechtliche Verpflichtungen und nur wenn keine übergeordneten Gesetze (Aufbewahrungsfristen, bspw. für Finanzamt u.ä.) einzuhalten sind.

Daten-Portabilität
Gemäß Art. 20 EU_DSGVO haben Betroffene das Recht, die sie betreffenden personenbezogenen Daten, die sie dem Verein bereitgestellt haben, in einem gängigen und maschinenlesbaren Format zu erhalten, ohne dass beim Empfänger irgendwelche Kompatibilitätsprobleme auftreten. Bei mündlicher oder elektronischer Auskunftserteilung muss sichergestellt werden, dass die Daten nicht unbefugten Dritten zur Verfügung gestellt werden. Ggf. ist eine Identitätsprüfung durchzuführen. Die Auskunftserteilung erfolgt unverzüglich, spätestens innerhalb eines Monats und ist für den Betroffenen unentgeltlich. Für weitere Kopien sowie lt. Art. 12 Abs. 5 Satz 2 ErwGr.63 kann bei offenkundig unbegründeten oder exzessiven Anträgen ein angemessenes Entgelt für die Auskunft verlangt werden.

Beschwerdestelle/Aufsichtsbehörde
Bayerisches Landesamt für Datenschutz (BayLDA)
Promenade 27
91522 Ansbach

Datenvernichtung,-löschung
Daten müssen bei berechtigtem Widerspruch sofort gelöscht werden und wenn Daten nicht mehr benötigt werden. Hierbei sind übergeordnete Aufbewahrungsfristen zu wahren. Siehe auch Löschkonzept und Verzeichnis für Verarbeitungstätigkeiten des Vereins.

Datenschutzverletzungen
Im Falle einer Verletzung des Schutzes personenbezogener Daten (bspw. bei Verlust von Datenträgern, Diebstahl eines unverschlüsselten Laptops mit gespeicherten personenbezogenen Daten, Vorhandensein von Trojanern in der IT-Infrastruktur oder Phishing-Attacken) meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde (hier: Bayerisches Landesamt für Datenschutzaufsicht, s. Meldung an die Aufsichtsbehörde bei Verlust der Kontrolle über Daten gem. Art. 33 EU-DS-GVO), es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. Bei der Meldung ist darauf zu achten, dass der Verantwortlich der Schweigepflicht unterliegt und somit nicht die konkreten personenbezogenen Daten melden darf.

Dokumentation
Die Vereinsleitung hat als Verantwortlicher im datenschutzrechtlichen Sinne eine sorgfältige Dokumentation zum Datenschutz zu führen. Diese wird gegenüber der Aufsichtsbehörde und im falle juristischer Auseinandersetzungen benötigt. Sie umfasst im Wesentlichen folgende Punkte:

- Beschreibung des Datenschutzkonzepts des Vereins
- Einwilligungen zu Verarbeitung von Daten
- Verzeichnis der Verarbeitungstätigkeiten
- Unterweisung von beauftragten Personen (auch temporärer Mitarbeiter) mit der Verpflichtung zur Verschwiegenheit und zum Datenschutz für jedes Mitglied und Vorstände im Besonderen
- Ggf. Verträge zur Auftragsverarbeitung
- Ggf. Datenschutzfolgeabschätzung, Risikoanalyse
- Ergriffene Sicherheitsmaßnahmen (technisch, organisatorisch)
- Meldungen an die Aufsichtsbehörde bei Datenpannen

Die Wirksamkeit der Datenschutz- und Datensicherheits-Maßnahmen sind bei Neuwahlen regelmäßig im 2Jahresrhythmus oder bei gravierenden Änderungen sofort zu überprüfen, zu bewerten und zu dokumentieren.