dcif Bundesverband Wettbewerbs- und Marktanalyse

Vereinsrichtlinie zur Datenschutz-Organisation

Die Umsetzung der DSGVO und weiterer datenschutzrechtlicher Vorgaben macht es erforderlich, von Seiten des Vorstands klare Anweisungen zu erteilen. Wie ist mit personenbezogenen Daten zu verfahren, welches Selbstbild hat der Verein bei der Datenverarbeitung und welche konkreten Ziele werden bei der Datenschutz-Organisation verfolgt?

Um diese Fragen zu klären, hat der Vorstand im Juni 2018 die folgende Datenschutzrichtlinie beschlossen:

Richtlinie zur Datenschutzorganisation im dcif e.V. – Bundesverband Wettbewerbs- und Marktanalyse

1. Grundsätze

Der Schutz personenbezogener Daten ist uns ein wichtiges Anliegen. Deshalb verarbeiten wir die personenbezogenen Daten unserer Mitglieder, Kunden sowie Geschäftspartner in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit.

In dieser Datenschutzrichtlinie wird beschrieben, welche Arten von personenbezogenen Daten wir erheben, wie diese Daten genutzt werden, an wen sie übermittelt werden und welche Wahlmöglichkeiten und Rechte betroffene Personen im Zusammenhang mit unserer Verarbeitung der Daten haben. Außerdem beschreiben wir, mit welchen Maßnahmen wir die Sicherheit der Daten gewährleisten und wie betroffene Personen Kontakt mit uns aufnehmen können, wenn Sie Fragen zu unserer Datenschutzpraxis haben.

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die insoweit beim dcif e.V. bestehenden Verantwortlichkeiten. Alle Mitglieder sind zur Einhaltung der Richtlinie verpflichtet.

Sie richtet sich an

• die Personen oder Abteilungen, die über den Einsatz/die Bereitstellung eines Anwendungssystems entscheiden (Vorstand);

• die Personen oder Abteilungen, die über die Nutzung des Systems für ihre Aufgaben entscheiden (Vorstand);

• Benutzer, d.h. diejenigen, die das zur Verfügung gestellte System für die Erledigung ihrer vereinsbetrieblichen Aufgaben nutzen (Mitglieder und Mitarbeiter).

Dabei gelten folgende Grundsätze:

• Die für Vereinszwecke eingesetzte DV-Hard- und Software ist gegen Verlust und Manipulation zu sichern.

• Jedes Mitglied und jeder Mitarbeiter ist in seinem Verantwortungsbereich für die Umsetzung der Richtlinie verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden.

• Die für die Verarbeitungen der eingesetzten Systeme Verantwortlichen stellen sicher, dass die Mitglieder und Mitarbeiter über diese Richtlinie informiert werden; das gilt auch für temporär Beschäftigte.

2. Datenschutzkoordination

2.1 Das dcif e.V. hat *keinen* nach Maßgabe des Artikels 37 DS-GVO betrieblichen Datenschutzbeauftragten (DSB) bestellt. Die Verantwortung für den Datenschutz im Verein trägt der Vorstand. Die Kontaktdaten des Vorstandes sind auf der Webseite des dcif veröffentlicht.

2.2 Der Vorstand unterrichtet die Mitglieder hinsichtlich ihrer Datenschutzpflichten. Ihm obliegt die Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, und der Sensibilisierung der Mitglieder.

2.3 Der Vorstand wird frühzeitig in alle Datenschutzfragen eingebunden und wird von den Mitarbeitern der Geschäftsstelle bei der Erfüllung seiner Aufgaben unterstützt.

2.4 Der Verein hat kein Verzeichnis über alle Verarbeitungsvorgänge zu führen, strebt aber die Einführung eines solchen an. Die dafür notwendigen Informationen zu den Verfahren zusammenzutragen und diese entsprechend den

Vorstand: Dr. Joachim Buck (buck@dcif.de), Alexander Haudan (haudan@dcif.de), Matthias Knapp (knapp@dcif.de), Rainer Michaeli (michaeli@dcif.de)
Vorsitzende: Alexandra Nelles (nelles@dcif.de)

Anforderungen des Art. 30 DS-GVO zu dokumentieren übernimmt die Leitung der Geschäftsstelle. Bei Unklarheiten hinsichtlich der gesetzlich geforderten Informationen kann ein Datenschutzbeauftragter beratend hinzugezogen werden.

Auf Anfrage stellt das dcif e.V. der Aufsichtsbehörde das Verzeichnis zur Verfügung. Im Einvernehmen mit dem Vorstand ist hierfür die Leitung der Geschäftsstelle zuständig und arbeitet mit der Aufsichtsbehörde zusammen.

2.5 Jedes Mitglied und jeder Mitarbeiter kann sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an den Vorstand wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

2.6 Der Vorstand berichtet jährlich im Rahmen des Geschäftsberichts über stattgefundene Prüfungen, Beanstandungen und ggf. noch zu beseitigende Organisationsmängel.

3. Beschaffung/Hard- und Software

3.1 Über die Beschaffung von Hard- und Software entscheidet der Vorstand. Bereits bei der Auswahl von Hard- und Software wird das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet.

3.2 Private Hard- und Software dürfen nur dann zur Verarbeitung personenbezogener Daten Verwendung finden, wenn sie entsprechend der Vorgaben des dcif e.V. geschützt sind.

3.3 Die Geschäftsstelle führt ein Verzeichnis der eingesetzten Hardware und der verwendeten Anwendungsprogramme. Der Vorstand kann auf das Verzeichnis jederzeit zugreifen.

3.4 Bei Verdacht des Diebstahls von Hard- und Software, des unbefugten Zugriffs auf personenbezogene Daten, von Sabotage etc. sind der Vorstand und die Leitung der Geschäftsstelle unverzüglich zu informieren.

4. Verpflichtung der Mitglieder und Mitarbeiter

4.1 Jeder Mitarbeiter und jedes Mitglied, das Umgang mit personenbezogenen Daten hat, ist auf einen vertraulichen Umgang mit personenbezogenen Daten und die Einhaltung dieser Richtlinie zu verpflichten.

4.2 Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars.

5. Transparenz der Datenverarbeitung

5.1 Über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, führt die Geschäftsstelle *freiwillig* ein Verzeichnis von Verarbeitungen gem. Art. 30 DSGVO. Der für ein Verfahren Verantwortliche meldet dieses zeitnah der Geschäftsstelle. Gleiches gilt für Veränderungen (Change Request).

5.2 Macht ein Betroffener von seinem Auskunftsrecht nach Art. 15 DSGVO oder seinem Korrektur- oder Widerspruchsrecht nach Art. 16 und Art. 21 DSGVO Gebrauch, so erfolgt die zentrale Bearbeitung durch die Leitung der Geschäftsstelle. Dies betrifft auch Auskunfts- und Einsichtsrechte von Mitarbeitern und Mitgliedern. Es ist sicherzustellen, dass dem Betroffenen seine Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden können.

6. Erhebung/Verarbeitung von personenbezogenen Daten

6.1 Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen. Hierbei sind auch die besonderen Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gemäß Art. 9 Abs. 1 DSGVO zu beachten. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur vereinsbetrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen.

6.2 Es wird sichergestellt, dass Betroffene keiner Entscheidung unterworfen werden, die ausschließlich auf einer automatisierten Verarbeitung beruhen und zugleich den Betroffenen gegenüber eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (bspw. Profiling).

6.3 Vor Einführung neuer Arten von Erhebungen ist die, die Zulässigkeit bestimmende Zweckbestimmung der Daten, durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Die im Rahmen

Vorstand: Dr. Joachim Buck (buck@dcif.de), Alexander Haudan (haudan@dcif.de), Matthias Knapp (knapp@dcif.de), Rainer Michaeli (michaeli@dcif.de)
Vorsitzende: Alexandra Nelles (nelles@dcif.de)

der Zweckänderung genutzten Abwägungs-Kriterien sind einzeln zu prüfen.

Eine Zweckänderung ist auch zulässig, wenn eine Einwilligung der betroffenen Person durch den Verantwortlichen eingeholt wird. Gleichzeitig hat der für die Verarbeitung Verantwortliche vor der Erhebung bzw. der Speicherung von Daten schriftlich festzulegen, ob und in welcher Art und Weise der gesetzlichen Benachrichtigungspflicht des Betroffenen zu genügen ist.

6.4 Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse des Vereins besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der Vorstand zu kontaktieren.

7. Datenhaltung/Versand/Löschung

7.1 Die Speicherung von Daten erfolgt grundsätzlich auf den hierzu vom dcif e.V. zur Verfügung gestellten Speichermedien. Eine Speicherung auf privaten (z.B. mobilen) Datenträgern oder Cloudspeicher (z.B. Flashspeicher, Streamer-Bändern) bedarf der Genehmigung durch den Vorstand und der Registrierung durch die den Träger einsetzende Stelle.

7.2 Soweit technisch bedingt ein anderer Speicherort erforderlich ist (z.B. Notebook, Desktop-PC) ist der jeweilige Benutzer für die Durchführung der Datensicherung selbst verantwortlich. Ist ein Netzzugang möglich (z.B. bei Notebook mit WLAN, Tablet), ist zumindest einmal wöchentlich der aktuelle Datenbestand zu sichern.

7.3 Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über die Verarbeitung der Daten Entscheidenden in seiner Verantwortung zu beachten.

7.4 Bei der Weitergabe nicht mehr benötigter IT-Komponenten ist der Benutzer verpflichtet, dafür zu sorgen, dass zuvor sämtliche Daten wirksam gelöscht wurden.

8. Externe Dienstleister/Auftragsverarbeitung/Wartung

8.1 Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten (z.B. Erhebung, Löschung = Entsorgung) bzw. mit Tätigkeiten (z.B. Wartung, Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, so hat der Vorstand einen den Anforderungen des Art. 28 DS-GVO genügenden Vertrag zu schließen.

8.2 Entsprechendes gilt, falls das dcif e.V. entsprechende Tätigkeiten im Auftrag Dritter wahrnehmen will.

9. Sicherheit der Verarbeitung

9.1 Für jedes Verfahren ist eine dokumentierte Schutzbedarfsfeststellung sowie eine Analyse bzgl. der für den Betroffenen möglichen Risiken zu erstellen. Diese richten sich an der Art, dem Umfang, der Umstände und Zwecke der Verarbeitung sowie der Wahrscheinlichkeit des Eintritts einer solchen Gefahr.

9.2 Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten sowie der Belastbarkeit der Daten verarbeitenden Systeme ist ein allgemeines Sicherheitskonzept zu erstellen. Das Konzept orientiert sich an der zuvor erstellten Schutzbedarfsfeststellung und der Risikoanalyse. Dieses Konzept ist maßgeblich für alle weiteren Verfahren.

10. Rechenschafts- und Dokumentationspflicht

Die Einhaltung der Vorgaben, die sich aus dieser Richtlinie ergeben, muss jederzeit nachweisbar sein („Accountability“). Eine Nachweisbarkeit hat insbesondere durch eine schlüssige und nachvollziehbare schriftliche Dokumentation hinsichtlich getroffener Maßnahmen und dazugehöriger Abwägungen zu erfolgen.