Neues Datenschutzrecht (5)

Rechtsanwalt Dr. Frank Weller aus Hohenahr begleitet die Arbeit des Freiwilligenzentrums Mittelhessen seit vielen Jahren. An dieser Stelle gibt er Tipps für Praktiker.

Ab 25.05.2018 wird der Datenschutz durch die Datenschutz-Grundverordnung (DS-GVO) in den Staaten der Europäischen Union neu geregelt. Dies hat auch Auswirkungen für Vereine. Mehrfach wurde hier darüber berichtet.

Heute geht es um die Datensicherheit in technischer und organisatorischer Hinsicht. Was hat man sich darunter vorzustellen? Welche Maßnahmen sind konkret gemeint?

Die DS-GVO regelt in Artikel 32 die Sicherheit der Datenverarbeitung. Gemeint ist damit die technische und organisatorische Sicherheit. Dies betrifft also die Frage, welche technischen und organisatorischen Maßnahmen ein Verein ergreifen muss, um die in seiner Obhut befindlichen Daten vor unbefugten Eingriffen oder Verlust zu schützen. Konkrete Maßnahmen werden allerdings nicht genannt; vielmehr beschränkt sich die Regelung auf Zielsetzungen und Rahmenbedingungen. Verlangt wird ein dem Risiko angemessenes Schutzniveau unter Berücksichtigung des Stands der Technik, der Kosten und der Verarbeitungszwecke sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos. Die Maßnahmen sollen u.a. folgendes einschließen: Verschlüsselung von Daten, Sicherung der Vertraulichkeit und Belastbarkeit der Systeme, Fähigkeit zur raschen Wiederherstellung der Daten nach einem physischen oder technischen Zwischenfall sowie Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Vor diesem Hintergrund muss jeder Verein selbst entscheiden, welche Maßnahmen für ihn in Betracht kommen. Das Neueste und Teuerste muss es nicht sein, wohl aber müssen die Daten so gut geschützt werden, dass Verstöße gegen die DS-GVO (vor allem Eingriffe durch unbefugte Personen oder Datenverluste) aller Wahrscheinlichkeit nach ausgeschlossen sind, wobei besonders sensible Daten (z.B. Gesundheitsdaten) den bestmöglichen Schutz verdienen. Im Folgenden einige Beispiele:

(1) Der Verein muss zunächst den Zugang zum PC sichern, und zwar in zweierlei Hinsicht: Verhinderung des körperlichen Zugangs durch Sichern und Abschließen von Räumlichkeiten sowie Verhinderung des technischen Zugangs durch passwortgeschützte Bereiche. Der Verein muss also festlegen, welche Personen Zugang zum PC und zu allen Daten haben dürfen. Das sollten möglichst wenige Personen sein. Allenfalls diese Personen sollten einen Schlüssel in zweifacher Bedeutung erhalten: Einen Schlüssel zu dem Raum, in dem der PC sich befindet, sowie ein Passwort für die Nutzung der Daten. Andere Personen dürfen nur von Fall zu Fall und im Zusammenhang mit ihrer jeweiligen Aufgabe Zugang zum PC und den jeweils benötigten Daten haben, z.B. mit gesondertem Passwort zu einem Teil der Daten. (2) Möglichst sichere Kommunikation wenigstens innerhalb des Vorstands (E-Mails nur über Vereins-Account, End-zu-End-Verschlüsselung). (3) Bei Webseiten mit Kommunikation mit dem Nutzer (Kontaktformular, Newsletterbestellung, Kommentarfunktion etc.) ist ab 25.05.2018 folgendes verpflichtend: Verwendung eines Hypertext Transfer Protocol Secure für die Webseite (https://..., Kommunikationsprotokoll im World Wide Web) (4) Regelmäßiges Aufspielen von Software-Updates (5) Zeitnahe Datensicherung, um ggf. auf Datenverlust reagieren zu können.

Noch Fragen? Bitte schreiben Sie an freiwilligenzentrum@mittelhessen.de