Handlungsempfehlungen zur Umsetzung der DS-GVO für Vereine

Adressat:

Vereine und Verbände (unerheblich, ob Eintragung im Vereinsregister erfolgt ist)

Wer ist für die Umsetzung der DS-GVO verantwortlich?

Verantwortlicher für die Einhaltung des Datenschutzes ist der gesetzliche Vertreter des Vereins. Also in den meisten Fällen ein Vorstand oder mehrere Vorstände gemeinsam (§26 BGB).

Was ist zu tun?

Auch nach neuem Recht benötigen Vereine für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage. Dies kann wie bisher entweder eine gesetzliche Regelung oder eine Einwilligung der betroffenen Personen sein. Die Mitgliedschaft in einem Verein ist als Vertragsverhältnis zwischen den Mitgliedern und dem Verein anzusehen, dessen Inhalt im Wesentlichen durch die Vereinssatzung und sie ergänzende Regelungen vorgegeben ist. Alle Daten, die somit zur „Abwicklung dieses Verhältnisses erforderlich sind, dürfen gem. Art 6 Abs. 1 lit. b) DS-GVO verarbeitet werden. Im Folgenden finden Sie in Kurzform (nicht abschließende) Handlungsempfehlungen:

1. Internen **Datenschutzbeauftragten** benennen Eine Benennung ist wie bisher dann verpflichtend, wenn mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Es aber in jedem Fall ein Datenschutzbeauftragter zu benennen, wenn Angaben beispielsweise zur Gesundheit oder zur politischen Meinung oder zur Bewertung der Person durch den Verein erfasst werden (Art. 37 Abs. 1 lit. c DS-GVO). Genau wie bei Unternehmen wirkt ein Datenschutzbeauftragter im Verein auf die Einhaltung der datenschutzrechtlichen Vorschriften hin. Wie bisher ist es nicht möglich, dass der Vorstand im Sinne des § 26 BGB die Funktion des Datenschutzbeauftragten übernimmt. Muss ein Datenschutzbeauftragter benannt werden, so ist dieser dem Sächsischen Datenschutzbeauftragten zu melden.
    - Kurzpapier Nr. 12
2. **„Verzeichnis von Verarbeitungstätigkeiten“** vorbereiten. Gemäß Art. 30 DS-GVO hat jeder Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten zu führen. Zwar besteht bei Verantwortlichen, die weniger als 250 Mitarbeiter beschäftigt sind eine Ausnahme von der Verzeichnisführungspflicht. Diese Ausnahme gilt jedoch nicht, wenn die Verarbeitung nicht nur gelegentlich erfolgt, oder eine Verarbeitung sensibler Daten i.S. von Art 9 oder Art 10 DS-GVO erfolgt. Die Verwaltung der Mitgliedsbeiträge, die Veröffentlichung von Fotos der Mitglieder oder die regelmäßige Unterrichtung der Mitglieder mittels eines Newsletters per E-Mail stellt eine solche regelmäßige Verarbeitung dar
    - Kurzpapier Nr. 1
    - Muster Verarbeitungsverzeichnis Verantwortlicher
    - Muster Verarbeitungsverzeichnis Auftragsverarbeiter
3. „**Datenschutz – Folgenabschätzung**“ (Art. 35 DS-GVO) Ein Verein hat nur dann eine Datenschutz-Folgeabschätzung vorzunehmen, wenn die Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke ein hohes Risiko für die Rechte und Freiheiten für natürliche Personen zur Folge hat. Ein solches Risiko kann angenommen werden, wenn auf der Grundlage von personenbezogenen Daten systematische Bewertungen persönlicher Art (Rating, Scoring…) vorgenommen werden. Das Ziel einer

Datenschutz-Folgeabschätzung besteht darin, Kriterien für den Schutz der betroffenen Person zu definieren und die Folgen der Datenverarbeitung möglichst umfassend zu erfassen.

   - Kurzpapier Nr. 5

4. Zuständigkeiten für Informationen bei **Datenverlust** festlegen Art. 33, 34 DS-GVO verpflichten Verantwortliche dazu, Datenlecks und Schutzmaßnahmen unverzüglich - soweit möglich innerhalb von 72 Stunden - dem Sächsischen Datenschutzbeauftragten und den Betroffenen mitzuteilen.

5. Vorhandene **Einwilligungen** prüfen, um sicherzustellen, dass sie nach Wirksamwerden der Datenschutz-Grundverordnung fortgelten Gemäß Art. 7 Abs. 3 DS-GVO die betroffene Person vor Abgabe der Einwilligung darüber in Kenntnis gesetzt werden, dass der Widerruf einer Einwilligung nur die Datenverarbeitung ab diesem Zeitpunkt betrifft; weiterhin muss der Verantwortliche gemäß Art. 7 Abs. 1 DS-GVO die Einwilligung nachweisen können. Insbesondere die Veröffentlichung personenbezogener Daten im Internet bedarf einer ausdrücklichen Einwilligung des Betroffenen. Es ist daher anzuraten, von den Vereinsmitgliedern eine entsprechende Einwilligungserklärung unterzeichnen zu lassen.

6. Einhaltung der erweiterten **Informationspflichten** des Verantwortlichen gegenüber den betroffenen Personen nach den Artikeln 13 und 14 Datenschutz-Grundverordnung sicherstellen. Aus Gründen der Transparenz von Datenverarbeitungsvorgängen muss ein Verein bei einer Erhebung personenbezogener Daten eine datenschutzrechtliche Unterrichtung vornehmen. Diese Informationspflichten sind unabhängig von einer Kenntnis der betroffenen Person und umfassen u. a. neben der Dauer der Datenspeicherung auch das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde. Eine solche Information kann durch ein Merkblatt oder in der Satzung erfolgen.

   - Kurzpapier Nr. 10

7. Bestehende Verträge daraufhin überprüfen, ob Vorgaben für Vereinbarungen mit **Auftragsverarbeitern** gemäß der Artikel 28 und 29 Datenschutz-Grundverordnung eingehalten werden. Insbesondere kleine Vereine bedienen sich zur Adressverwaltung externer Dienstleister. Kennzeichnend für die Auftragsverarbeitung ist, dass der Auftragsverarbeiter über die bloße Beauftragung hinaus gegenüber dem Verantwortlichen weisungsabhängig ist. Seitens des Vereins dürfen nur Auftragsverarbeiter eingesetzt werden, die eine hinreichende Garantie für eine datenschutzkonforme Datenverarbeitung gewährleisten (vgl. Art. 28 Abs.1 DS-GVO). Für Verein wir in der Regel in Betracht kommen, dass die verbindliche Vereinbarung über die Auftragsverarbeitung auf der Grundlage eines Vertrages erfolgt.

   - Kurzpapier Nr. 13
   - Mustervertrag

8. **Sicherheit** personenbezogener Daten: Der Verein kann personenbezogene Daten mittels herkömmlicher Karteien oder automatisiert speichern (vgl. Art 2 Abs. 1 DS_GVO) Nach Art 32 DS-GVO sind bei der Verarbeitung personenbezogener Daten geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Welche Maßnahmen konkret umzusetzen sind, dazu macht Art 32 DS-GVO keine Vorgaben. Im Regelfall sind Standardmaßnahmen um die personenbezogenen Daten bei der Verarbeitung zu schützen, ausreichend. Dazu gehören u.a. aktuelle Betriebssysteme und Anwendungen, Passwortschutz, regelmäßige Backups und Virenscanner. Soweit private PCs genutzt werden, ist sicherzustellen, dass nur berechtigte Personen auf die Daten zugreifen können.

9. **Löschen** von Daten: Sobald keine gesetzliche Grundlage (steuerliche Aufbewahrungspflicht etc.) mehr für die Speicherung personenbezogener Daten besteht, sind diese zu löschen.

10. **Auskunftspflichten**: Die betroffenen Personen (z.B. Mitglieder des Vereins) haben das Recht Auskunft über die Verarbeitung ihrer personenbezogenen Daten zu erhalten. Dies kann formlos und ohne Begründung erfolgen. Werden seitens des Vereins personenbezogene Daten der betroffenen Person verarbeitet, hat diese ein Recht auf Auskunf tüber die personenbezogenen Daten. Zudem hat die betroffene Person, wenn personenbezogene Daten über sie verarbeitet werden, ein Recht auf die in Art. 15 Abs. 1 lit. a) bis h) DS-GVO aufgeführten Informationen.

    - Kurzpapier Nr. 6