Die EU-Datenschutzgrundverordnung

Die Datenschutzgrundverordnung wird ab dem 25.05.2018 in jedem EU-Mitgliedsstaat unmittelbare Wirkung entfalten. Sie eröffnet dem nationalen Gesetzgeber Gestaltungsmöglichkeiten. Dies hat auch zu einer Änderung des Bundesdatenschutzgesetzes geführt.

Die Änderungen gelten für Unternehmen wozu auch gemeinnützige Vereine gehören und treten am 25.05.2018 in Kraft.

1.) Anwendungsbereich

Der Anwendungsbereich umfasst personenbezogene Daten, dh. alle Informationen, die sich auf eine entweder identifizierte oder identifizierbare natürliche Person beziehen.

Sofern personenbezogene Daten mittels eines Computerprogrammes zB. einer Personalverwaltungssoftware bearbeitet werden, müssen die Bestimmungen der EU-Verordnung beachtet werden.

Falls personenbezogene Daten nicht EDV gestützt verarbeitet werden, findet die EU Verordnung nur dann Anwendung, wenn die Daten in einem bestimmten System und nach bestimmten Kriterien geordnet sind. Darunter ist beispielsweise eine namensortierte Liste der Teilnehmer eines Vereinsausflugs zu verstehen.

2.) Grundsätze der Datenverarbeitung

Die Datenschutzgrundverordnung bringt zwar einige Neuerungen mit sich, behält aber die bisherigen bekannten Datenschutzgrundsätze im Wesentlichen bei. Neu ist, dass die Unternehmer die Einhaltung der datenrechtlichen Grundsätze auch nachweisen müssen.

Dies erfordert eine umfangreichere Datenschutzdokumentation als bisher.

3,) Grundsätze der EU Verordnung für die Verarbeitung personenbezogener Daten im Einzelnen (Art 5 DSGVO)

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn die Verarbeitung durch die Rechtsgrundlage gedeckt ist. Sie müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz)

Personenbezogene Daten dürfen auch weiterhin nur für festgelegte eindeutige und legitime Zwecke verarbeitet werden, soweit dies zur Erreichung des Zweckes angemessen und erheblich ist.

Darüber hinaus müssen personenbezogene Daten sachlich richtig sein und auf den aktuellen Stand gebracht werden.

Sie dürfen nur so lange gespeichert werden, wie dies zur Erreichung des Zweckes unbedingt notwendig ist.

Nach Zweckfortfall müssen die Daten entweder vollständig gelöscht werden oder es muss zumindest sichergestellt sein, dass die Identifizierung einer Person nicht mehr möglich ist.

Außerdem müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet.

Sie schließt den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung ein.

4.) Einwilligung in die Datenverarbeitung

Weiterhin muss eine Einwilligung nach Art 7 der EU Datenschutzgrundverordnung vorliegen. Eine Einwilligung kann nur dann wirksam erteilt werden, wenn der Betroffene in voller Kenntnis des Umfangs der geplanten Verarbeitung und freiwillig sein Einverständnis zur Verarbeitung erteilt.
Er muss bei Erteilung der Einwilligung auf sein Widerrufsrecht hingewiesen werden. Schriftform der Einwilligung ist nicht mehr vorgesehen. Einwilligungen können daher auch in mündlicher oder elektronischer Form wirksam erteilt werden. Die Einwilligung muss in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen. Einwilligungserklärungen von minderjährigen, die das 16. Lebensjahr vollendet haben, sollen grundsätzlich wirksam sein. Wenn ein Minderjähriger das 16. Lebensjahr noch nicht vollendet hat, bedarf es der Einwilligung des Erziehungsberechtigten.

Sofern bereits jetzt eingeholte Einwilligungserklärungen den Normen den EU-Verordnung entsprechen, gelten diese auch nach dem 25.05.2018 fort.
Eine weitere Einholung ist dann nicht mehr erforderlich.

5.) Bearbeitung besonderer Kategorien

Die Verarbeitung besonderer Kategorien personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgeht, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung dürfen zukünftig grundsätzlich nicht mehr verarbeitet werden, es sei denn, es liegt ein Ausnahmetatbestand vor.

6.) Dokumentationspflichten für Vereine

Neu sind die weiteren Dokumentationspflichten für Unternehmen (Vereine):

a.) Verzeichnis von Verarbeitungstätigkeiten

Jeder Verantwortliche ist zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten verpflichtet. Dieses Verzeichnis ist der zentrale Bestandteil der Datenschutzdokumentation, und listet alle Verarbeitungen von personenbezogenen Daten im Unternehmen (Verein) auf. Das Verzeichnis muss die folgenden Angaben enthalten :

- Name und Kontaktdaten des Verantwortlichen
- Zweck der Verarbeitung
- Beschreibung der Kategorien betreffender Personen
- Beschreibung der Kategorien personenbezogener Daten
- Aufzählung der Empfänger der personenbezogenen Daten
- Fristen für die Löschung der personenbezogenen Daten
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Das Verzeichnis ist eines der zentralen Dokumente für Prüfung durch die Datenschutzorganisation.

Innerhalb des Verzeichnisses können auch weitere Dokumentationspflichten, wie etwa durchgeführte Risikoanalysen oder Datenschutzfolgeabschätzungen erfüllt werden.

b.) Verzeichnis über Tätigkeiten als Auftragsverarbeiter (z.B. Verarbeitung personenbezogener Daten im Auftrag, etwa durch Callcenter, dessen Dienstleistungen im Rahmen einer separaten Vereinbarung von einem Unternehmen im Wege des Outsourcings in Anspruch genommen werden.)

Die Verpflichtung zur Führung eines Verzeichnisses zur Verarbeitungstätigkeit betrifft nicht nur die jeweiligen Verantwortlichen, sondern auch alle Auftragsverarbeiter.

c.) Dokumentation der Datenschutzprozesse

Die Beratung eines Datenschutzkonzeptes . Darin sollte geregelt werden , welche Personen verantwortlich sind, welche Schutzmaßnahmen bei der Verarbeitung der personenbezogenen Daten getroffen werden, wie mit Betroffenen Rechnung gelegt wird, wie das Löschen von personenbezogenen Daten gewährleistet wird, und wie mit Datenpannen umgegangen wird.

d.) Risikoanalyse

Es muss der drohende Schaden für die Rechte und Freiheiten natürlicher Personen durch die Datenverarbeitung klassifiziert werden.

Danach sich eine Prognose hinsichtlich der Eintrittswahrscheinlichkeit einer Rechtsverletzung zu erstellen. Abschließend muss analysiert werden, ob die Verarbeitung ein Risiko für die Rechte und Freiheit natürlicher Personen darstellt. Sofern diese Analyse dazu führt, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheit natürlicher Personen bedeutet, ist eine Datenschutzfolgeabschätzung durchzuführen und zu dokumentieren.

Diese Folgeabschätzung muss dabei folgendes beinhalten :

- Systematische Beschreibung der Verarbeitungsvorgänge
- Zweck der Verarbeitung
- Mit der Verarbeitung verfolgte Interessen
- Bewertung der Notwendigkeit der Verhältnismäßigkeit
- Bewertung der Risiken und die Rechte und Freiheiten der Betroffenen
- Getroffene und geplante Abhilfemaßnahmen durch die der Schutz der personenbezogenen Daten sicher gestellt wird.

7.) Rechte der Betroffenen.

Informationspflichten

Sofern die betroffenen Personen nicht bereits Kenntnis über die Informationen haben, müssen Unternehmen sie künftig zum Zeitpunkt der Datenerhebung über folgende Punkte informieren :

- Namen und Kontaktdaten des Verantwortlichen
- ggf.Kontaktdaten des Datenschutzbeauftragten
- Zwecke der Datenverarbeitung
- Berechtigte Interessen , falls die Verarbeitung aufgrund eines berechtigten Interesses durchgeführt wird
- Empfänger der Daten
- Ebenfalls die Absicht zur Übermittlung in ein Drittland
- Dauer der Speicherung
- Hinweis auf Betroffenenrechte
- Widerrufsrecht, falls die Verarbeitung auf einer Einwilligung basiert

Darüber hinaus hat jede betroffene Person auch weiterhin ein Recht auf Auskunft.

Recht auf Löschung personenbezogener Daten

Unternehmen müssen personenbezogene Daten löschen, wenn eine der folgenden Voraussetzungen erfüllt ist :

- Die Speicherung ist nicht länger erforderlich, weil der Zweck der Speicherung entfallen ist
- Die betroffene Person hat eine erteilte Einwilligung widerrufen.
- Die betroffene Person hat Widerspruch gegen die Verarbeitung eingelegt und es liegen keine berechtigten Gründe für die Weiterverarbeitung vor.
- Personenbezogene Daten werden unrechtmäßig verarbeitet

Insoweit hat sich am bisherigen Recht nichts geändert.

Es besteht aber auch für die Einhaltung der Löschungsverpflichtungen eine Rechenschaftspflicht.

Recht auf Datenübertragung und Widerspruchsrecht

Darüber hinaus haben die betroffenen Personen künftig das Recht, die bereitgestellten personenbezogenen Daten in einem strukturierten gängigen und maschinenlesbaren Format zu erhalten oder diese an einen Dritten zu übermitteln.

Die betroffenen Personen haben das Recht jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen.

8.) Fristen und Bußgelder

Neu ist auch, dass bei Datenpannen eine Meldung binnen 72 Stunden an die Aufsichtsbehörde zu erfolgen hat, selbst wenn hierfür der Auftragsverarbeitende verantwortlich ist.

Bestehende Verträge zur Auftragsdatenverarbeitung sollten frühzeitig an die Anforderungen des DS GVO angepasst werden.

Mit Inkrafttreten des DS GVO wird der Rahmen für Bußgelder erhöht.
Es können bis zu 4 % des erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres als Bußgeld fällig werden.

Bisher drohten Bußgelder von bis zu Euro 50.000.- bzw. Euro 300.000.-.
Zukünftig soll die Obergrenze Euro 10.000.000.- bzw. Euro 20.000.000.- betragen.

Die Erhöhung des Bußgeldrahmens soll für eine abschreckende Wirkung sorgen, damit sich Unternehmen, die das Thema Datenschutz in der Vergangenheit eher

stiefmütterlich behandelt haben, künftig an die Datenschutzrechtlichen Vorgaben halten.

9.)Tipps für die aktuelle Vereinsarbeit

Die Vereine sollten zunächst auf folgendes achten :

1 . Als ersten Schritt sollten die Dokumentationspflichten, insbesondere das Verzeichnis der Verarbeitungstätigkeiten erstellt, bzw. aktualisiert werden. Die erfassten Verarbeitungstätigkeiten sollten anschließend einer Risikobewertung unterzogen werden. Das Ergebnis dieser Bewertung sollte ebenfalls dokumentiert werden.

2 . Anschließend sollten alle datenschutzrelevanten Formulare , z.B. Einwilligungserklärungen oder Vereinbarungen zur Auftragsdatenverarbeitung auf Aktualität und Einhaltung der Anforderungen der DS GVO geprüft werden.

3 . Daran anknüpfend sollte das Datenschutzkonzept aktualisiert und überarbeitet werden.

4. In einem letzten Schritt sollten alle hierfür Verantwortlichen im Hinblick auf die Anforderungen des DS GVO sensibilisiert und geschult werden.

Im Hinblick darauf hat die Landesakademie für musisch kulturelle Bildung, der Verein Pro Ehrenamt, Schulungen für die im Verein Verantwortlichen durchführen.

Ein den Vereinen angepasstes Verarbeitungsverzeichnis und Checklisten ist von dem bayerischen Landesamt für Datenschutzaufsicht zusammengestellt worden. Dies ist unter dem Link www.lda.bayern.de/media/muster_1_verein-verzeichnis.pdf abrufbar.