EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

WLSB

Stand: 28.11.2017

DAS WICHTIGSTE ZUR DSGVO IM ÜBERBLICK

Allgemeines zur DSGVO

- Beschlossen im Frühjahr 2016 durch EU
- Anpassung BDSG-neu im Sommer 2017
- Gültig in allen EU-Staaten ab 25.05.2018
- Ausgesprochen komplex
- Auch für Vereine und Verbände verbindlich

Ziele der DSGVO

- Schutz persönlicher Daten als Grundrecht
- Gleiches Schutzniveau innerhalb der EU
- Vereinheitlichung der Datenschutzregeln
- Stärkere Zusammenarbeit der Aufsichtsbehörden
- Gleiche Wettbewerbsbedingungen
- Anpassung an technologische Entwicklung

Grundsätze

- Stärkung der Betroffenenrechte (Auskunft, Berichtigung, Löschung, Widerruf, etc.)
- Rechtmäßigkeit der Erhebung / Verarbeitung
- Datenminimierung / Datensparsamkeit
- Sicherheit / Vertraulichkeit
- Erhöhter Sanktionsrahmen / Meldepflicht

Einwilligung in die Erhebung und Verarbeitung

- Freiwillig, verständlich, leicht zugänglich, einfache Sprache, von anderen Sachverhalten klar unterscheidbar
- Widerruf muss einfach möglich sein
- Nachweis des Vorhandenseins einer Einwilligung
- Bereits erteilte Einwilligungen sollen weiter gelten
- Rechtsvoraussetzungen (s.o.) beachten

Bestandsaufnahme: Was haben wir bereits erfüllt und wo besteht Nachbesserungsbedarf?

- Können die Betroffenenrechte sichergestellt werden?
- Ist ein Datenschutzbeauftragter erforderlich?
- Haben wir eine Rechtsgrundlage zur Verarbeitung personen-bezogener Daten?
- Sind Einwilligungserklärungen auf dem neusten Stand?
- Sind Verträge zur Auftragsdatenverarbeitung mit Dritten erforderlich?
- Gibt es einen Ablaufprozess bei Datenpannen und Zuständigkeiten hierzu?
- Gibt es ein Verzeichnis von Verarbeitungstätigkeiten?
- Sind die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten ausreichend?

ALLGEMEINES ZUR DSGVO

- Beschlossen am 27.04.2016 durch das Europäische Parlament
- Übergangsfrist bis 25.05.2018
- DSGVO stellt die EU-weite übergeordnete Grundlage zum Datenschutz dar
- Oberstes Kontrollorgan: Der Europäische Datenschutzausschuss
- DSGVO enthält Öffnungsklauseln zur Umsetzung von datenschutzrechtlichen Bestimmungen auf nationaler Ebene
  - „Datenschutz-Anpassungs- und Umsetzungsgesetz“ am 30.06.2017 beschlossen (BDSG-neu)
- Bisheriges BDSG bleibt bis zum 25.05.2018 unverändert in Kraft
- DSGVO und BDSG-neu treten ab dem 25.05.2018 in Kraft (und müssen berücksichtigt werden)
- Auch für Vereine und Verbände verbindlich
- Erhöhter Sanktionsrahmen
- Ausgesprochen komplex - intensive Erörterung in den entsprechenden Datenschutzfachkreisen auf Bundesebene (Datenschutzkonferenz)

WLSB

ZIELE DER DSGVO

- EU-weite Vereinheitlichung der Regeln zum Datenschutz
- Sicherstellung des gleichen Schutzniveaus von personenbezogenen Daten innerhalb der EU (Zusammenarbeit der Aufsichtsbehörden)
- Sicherstellung der gleichen Betroffenenrechte innerhalb der EU (z.B. Einwilligung, Auskunft, Löschen, Datenübertragung, Widerspruch)
- Schaffung gleicher Wettbewerbsbedingungen für europäische und außereuropäische Unternehmen (Beispiel: Ein außereuropäischer App-Anbieter, der seine Dienstleistungen in deutscher Sprache anbietet, muss das Europäische Datenschutzrecht beachten)
- Anpassung an aktuelle technologische Entwicklungen (z.B. Social Media)
- Stärkung der Selbstregulierung durch Zertifizierung und Verhaltensregeln

WLSB

GRUNDSÄTZE

- Regelt das Recht auf Schutz persönlicher Daten als Grundrecht in der EU
- Vereinheitlicht weitestgehend die bestehenden länderspezifischen Gesetze in den EU-Staaten
- Erhöht den Sanktionsrahmen bei Verstößen und stärkt die Rechte der Betroffenen sowie der Aufsichtsbehörden (z.B. Beschwerdemöglichkeit vor Ort)
- Starke Betonung der Sicherheit der personenbezogenen Daten – Sicht des Betroffenen (z.B. Verschlüsselung, Zugriffskontrolle)
- Beinhaltet eine Meldepflicht (innerhalb von 72 Stunden) über Datenschutzverletzungen
- Schaffung geeigneter technischer (z.B. Datensicherung) und organisatorischer (z.B. Zugriffs-berechtigung) Maßnahmen zum Schutz personenbezogener Daten
- Dokumentationsanforderungen für die Verarbeitungstätigkeiten und die Abwägung der Risikosituation bei der Verarbeitung von personenbezogenen Daten

WLSB

GRUNDSÄTZE – RECHTE DER BETROFFENEN (KAP. III DSGVO)

- Recht auf Auskunft über die gespeicherten Daten (Transparenz)
- Recht auf Berichtigung von personenbezogenen Daten
- Recht auf Löschung von personenbezogenen Daten (wenn diese für den Zweck, für den sie erhoben werden, nicht mehr benötigt werden)
- Recht auf „Vergessenwerden“ (wenn die zu löschenden Daten öffentlich gemacht wurden – z.B. bei Internet-Suchmaschine)
- Recht auf Widerruf der Einwilligung in die Verarbeitung personenbezogener Daten
- Recht auf Datenübertragbarkeit (in einem gängigen Format)
- Datenvermeidung und Datensparsamkeit

WLSB

GRUNDSÄTZE – VERARBEITUNG (ART. 5 DSGVO)

- **Personenbezogene Daten müssen unter anderem …**
  - … auf rechtmäßige Weise erhoben und verarbeitet werden (Rechtmäßigkeit)
  - … für festgelegte, eindeutige Zwecke erhoben und verarbeitet werden (Zweckbindung)
  - … dem Zweck angemessen sowie auf das notwendige Maß beschränkt sein (Datenminimierung bzw. Datensparsamkeit)
  - … sachlich richtig und auf dem neusten Stand sein (Richtigkeit)
  - … in einer Art und Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet (Sicherheit und Vertraulichkeit)

WLSB

GRUNDSÄTZE – RECHTMÄßIGKEIT (ART. 6 DSGVO)

- **Die Verarbeitung von personenbezogenen Daten („Verbot mit Erlaubnisvorbehalt“) ist nur rechtmäßig, wenn z.B. mindestens eine der nachstehenden Bedingungen erfüllt ist:**
  - Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere Zwecke gegeben
  - Die Verarbeitung ist für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen
  - Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt)

WLSB

GRUNDSÄTZE – EINWILLIGUNG (ART. 7 DSGVO)

- **Bei Einwilligungen müssen unter anderem folgende Punkte beachtet werden:**
  - Auch in Zukunft sind Einwilligungen eine wesentliche Rechtmäßigkeitsvoraussetzung für den Umgang mit personenbezogenen Daten
  - Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche (Verein) nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten freiwillig eingewilligt hat
  - Erfolgt die Einwilligung durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft (z.B. Antrag auf Mitgliedschaft), so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist

GRUNDSÄTZE – EINWILLIGUNG (ART. 7 DSGVO)

- **Bei Einwilligungen müssen unter anderem folgende Punkte beachtet werden:**
  - Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen - der Widerruf muss so einfach wie die Erteilung der Einwilligung sein
  - Bisher bereits erteilte Einwilligungen gelten nach derzeitigem Stand nach dem Wirksamwerden der DSGVO (25.05.2018) fort
  - Es wird empfohlen alte Einwilligungen soweit wie möglich zu aktualisieren und bei neuen Einwilligungen die Rechtsvoraussetzungen (s.o.) zu beachten

PROBLEMBEREICHE KÖNNEN Z.B. SEIN …

- Verarbeitung von personenbezogenen Daten erfolgt ohne rechtliche Grundlage
- Es wurde kein Datenschutzbeauftragter bestellt
- Die personenbezogenen Daten sind nicht ausreichend technisch und organisatorisch geschützt
- Personen im Verein, die personenbezogene Daten verarbeiten, wurden nicht auf das Datengeheimnis verpflichtet
- Es liegt kein Verzeichnis von Verarbeitungstätigkeiten vor (Hinweis: Vorab Prüfung, ob ein solches Verzeichnis im Einzelfall erforderlich ist) – Erforderliche Angaben im Verzeichnis sind z.B.:
  - Name und Kontaktdaten der Verantwortlichen (Vorstand und ggf. Datenschutzbeauftragter)
  - Zweck der Verarbeitung (z.B. Lohnabrechnung, Mitgliederverwaltung, Antragsbearbeitung)
  - Rechtsgrundlage der Verarbeitung (z.B. Einwilligung, Arbeitsvertrag, Mitgliedschaft)
  - Beschreibung der Kategorien betroffener Personen (z.B. Mitarbeiter, Funktionsträger, Mitglieder) und der personenbezogenen Daten (z.B. Adressdaten, Geburtsdatum, Bankverbindung)
  - Ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (z.B. Banken, Auftragsverarbeiter)
  - Dauer der Speicherung (z.B. Hinweis auf steuerrechtliche Aufbewahrungsfristen)
  - Beschreibung der technischen (z.B. Datensicherung) und organisatorischen Maßnahmen (z.B. Zugangskontrolle)

WLSB

WAS SOLLTEN VEREINE BIS MAI 2018 UNTERNEHMEN?

- **Bestandsaufnahme: Was haben wir bereits erfüllt und wo besteht Nachbesserungsbedarf?**
  - Erfassung aller Prozesse im Verein, die mit der Erhebung, Speicherung, Verarbeitung, Sicherung und Löschung von personenbezogenen Daten zusammenhängen
  - Prüfung der Rechtmäßigkeit der derzeitigen Datenverarbeitung
  - Prüfung, ob ein Datenschutzbeauftragter (s. § 38 Abs. 1 BDSG-neu) im Verein benannt werden muss (Auflistung, wer Zugang und Zugriff auf personenbezogene Daten hat und zu welchem Zweck)
  - Prüfung vorhandener Einwilligungserklärungen auf die neuen Rechtsvoraussetzungen
  - Prüfung, ob Verträge zur Auftragsdatenverarbeitung mit Dritten (z.B. IT-Dienstleiter) erforderlich werden
  - Ablaufprozess bei Datenpannen (z.B. unberechtigter Zugriff durch Dritte) und Verantwortlichkeiten festlegen (z.B. Meldung an Aufsichtsbehörden)

WLSB

WAS SOLLTEN VEREINE BIS MAI 2018 UNTERNEHMEN?

- **Bestandsaufnahme: Was haben wir bereits erfüllt und wo besteht Nachbesserungsbedarf?**
  - Sicherstellung der Betroffenenrechte (z.B. Auskunft, Löschen, Datenübertragung, Widerspruch)
  - Bei Bedarf Durchführung einer Datenschutz-Folgeabschätzung (z.B. bei Verwendung neuer Technologien, die voraussichtlich ein höheres Risiko für die Betroffenen mit sich bringen können) um zu prüfen, welche Risiken den Betroffenen z.B. bei Verlust der Vertraulichkeit ihrer Daten entstehen können
  - Sicherstellung der technischen (z.B. Verschlüsselung) und organisatorischen Maßnahmen (z.B. Zugriffsrechte) zum Schutz personenbezogener Daten sowie Dokumentation der Maßnahmen (z.B. Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO)
    - → Eine detaillierte, saubere Dokumentation dieser Prozesse ist sicherlich die größte Herausforderung
  - → Umfang und Aufwand der bei Vereinen erforderlichen Anpassungsprozesse ist abhängig z.B. von Vereinsgröße, Vereinsstruktur, bisheriger Umgang mit personenbezogenen Daten

WLSB

WEITERE INFORMATIONEN ZUR DSGVO

- Bundesbeauftragte für Datenschutz und Informationsfreiheit (Broschüre)
- Landesbeauftragte für den Datenschutz in Niedersachsen (Datenschutz im Verein)
- Landesbeauftragter für Datenschutz und Informationsfreiheit in BW (Merkblätter)
  - Hinweis: Die Information „Datenschutz im Verein“ wird derzeit überarbeitet und soll nach Auskunft des LfDI BW Ende Januar 2018 in einer aktuellen, der DSGVO und dem BDSG-neu entsprechenden Fassung zum Download zur Verfügung stehen.
- Datenschutzportal der Führungsakademie des DOSB (kostenpflichtiges Angebot)
- Bayerisches Landesamt für Datenaufsicht (Fragebogen zur Umsetzung der DSGVO)
- Kurzpapiere der Datenschutzkonferenz
- Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. (Praxishilfen)
- Analyse und Handlungsempfehlung durch externe Datenschutzexperten

Hinweis:
Bitte beachten Sie, dass keinerlei Haftung für die korrekte Anwendung bim Einzelfall und Aktualität der Informationen zum Zeitpunkt der Verwendung übernommen werden kann. Die Informationen können insoweit nur Anregungen liefern und sind stets an die individuellen Bedürfnisse im Einzelfall anzupassen. Wir empfehlen ergänzend rechtlichen und steuerlichen Rat im Vorfeld einzuholen.

WLSB