Datenschutzgrundverordnung 2018 - Anwendung im Einkaufsstraßenverein

Checkliste

Entsprechende Muster finden Sie in der Beilage.

1. **Erstellen Sie ein Datenverarbeitungsverzeichnis**
   Hier wird der Beweislastumkehr (= der Verantwortliche muss beweisen, dass er alle notwendigen Schritte gesetzt hat) Rechnung getragen.
   Ein vollständig ausgefülltes Datenverarbeitungsverzeichnis enthält im Normfall Namen und Kontaktdaten des Verantwortlichen, den Verarbeitungszweck (z.B. Mitgliederverwaltung, Werbeaktionsverwaltung, Gewinnspielverwaltung), die Gruppe der betroffenen Personen (z.B. Mitglieder, Teilnehmer an Gewinnspielen), die Art der Daten (Name, Adresse, etc.), Art und Ort der Datenerhebung (z.B. Beitrittserklärung), Grundlage der Verarbeitung (z.B. Einwilligung, Vertragserfüllung), Ort der Speicherung (z.B. Datenbank, Excel-sheet), technische/organisatorische Sicherheitsmaßnahmen (z.B. Back up, Berechtigungen, Datenverschlüsselung), Zugriffsberechtigungen (= berechtigte Personen), Datenweitergabe an Drittempfänger (z.B. Fördergeber) und Löschfristen (z.B. Vertragsdauer + 7 Jahre).

2. **Erstellen oder überprüfen Sie Verträge mit Auftragsdienstleistern**
   Hier werden die Pflichten des Auftragsdienstleisters genau festgelegt:
   Vertragspartner, Vertragsgegenstand (Beschreibung des Zwecks, der Verarbeitungstätigkeit und der Art der Daten), Vertragsdauer, Pflichten des Auftragsverarbeiters, Ort der Datenverarbeitung (EU oder Drittländer)

3. **Erstellen oder überprüfen Sie Verträge mit Betroffenen – Datenschutzvereinbarungen**
   Um Daten von Personen, in Ihrem Fall Mitgliedsbetrieben verarbeiten zu können bedarf es der ausdrücklichen Einwilligung aller betroffenen Personen, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden sind. Dies muss eine aktive und belegbare Handlung sein. Eine Ergänzung der Statuten reicht hier nicht aus. Im Idealfall ist diese Einwilligung Teil des Beitrittsformulars oder der Anmeldung zu einer Aktion/Veranstaltung/ Gewinnspiel. Online ist das aktive Ankreuzen einer check-box und das aktive Bestätigen dieser Auswahl ausreichend.

4. **Kommen Sie Ihrer Informationspflicht nach**
   Für bereits vorhandene Daten muss im Rahmen der Informationspflicht eine nachträgliche Information über die derzeit gespeicherten Daten erfolgen. Es wird empfohlen die Information über die am 25.5.2018 vorhandenen Daten zeitnah an die Betroffenen zu übermitteln.

5. **Treffen Sie Vorkehrungen zu Anträgen auf Auskunftserteilung**
   Erfolgt ein Antrag auf Auskunft über gespeicherte Daten ist wie folgt vorzugehen:
   Identifizierung des Antragstellers (persönlich bekannt, elektronisch signiert oder über Ausweisleistung)
   Die Auskunft ist innerhalb eines Monats ab Eingang schriftlich zu erteilen. Die Kopien der Daten, die konkret verarbeiteten Daten, der Verarbeitungszweck, Empfänger, an die die Daten weitergegeben worden sind und die geplante Speicherfirst sind mitzuteilen.

6. **Stellen Sie den technischen Standard der IT-Anlage sicher**
   Das verwendete Computersystem muss „state oft the art“ sein, das heißt dem aktuellen Stand der Technik entsprechen. Die Daten sind regelmäßig zu sichern und gegen Angriffe von außen zu schützen. Praktisch bedeutet das eine Firewall und ein Anti-Viren-System, sowie ein Back-up-System zu verwenden.

   Weitere Maßnahmen zur technischen Sicherheit sind die Verschlüsselung der Daten, die Einschränkung der Personen, die Zugang zum System haben, die Verhinderung von unberechtigter Manipulation der Daten, sowie die Möglichkeit der Wiederherstellung / Backup.

   Um nach einem Schadensfall (z.B. technisches Gebrechen oder Cyberangriff) Systeme und die dazugehörenden Informationen wiederherstellen zu können braucht es ein Backup-Konzept – zeitlich (wann werden Backups erstellt), räumlich (wo werden diese gespeichert, damit diese im Schadensfall erhalten bleiben z.B. Brand, Einbruch), sachlich (welche Daten werden gesichert), sowie ein Wiederherstellungskonzept – wer (autorisierte und verfügbare Person), kann was (technische Infrastruktur) wie (Systemkonfiguration) mit welchen Informationen (Backups) wiederherstellen. Die Wiederherstellung sollte entsprechend getestet werden um sicherzustellen, dass Backup, Prozesse und Dokumentation ausreichend sind.

   Die technisch-organisatorischen Maßnahmen sind nicht nur auf Aktualität, sondern auch in Bezug auf den Stand der Technik hin kontinuierlich zu evaluieren.

Lassen Sie Ihre Mitarbeiter und andere betroffene Personen jedoch eine Verpflichtungserklärung unterschreiben
Alle Personen, die mit den personenbezogenen Daten zu tun haben (z.B. Mitarbeiter) sollten eine Verpflichtungserklärung zum Datengeheimnis unterschreiben.

Sie brauchen keinen Datenschutzbeauftragten
Aufgrund der Datenmenge, der Art der Datenverarbeitung und der Kerntätigkeit ist die Bestellung eines Datenschutzbeauftragten nicht notwendig.

Sie brauchen keine Datenschutzfolgeabschätzung:
Da im Standardverein keine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen (Profiling), keine systematische und umfangreiche Videoüberwachung durchgeführt wird, sowie keine sensiblen Daten verarbeitet werden ist davon auszugehen, daß eine Datenschutzfolgeabschätzung nicht notwendig ist.