



Datenschutzgrundverordnung der Europäischen Union (DSGVO)

Herbert Sattlecker

Obmann der Pongauer Computer-Freunde

obmann@pcf Freunde.org

Quelle und Haftungsausschluss

- Quelle:

Die Angaben dieser Präsentation bzw. dieses Vortrags beziehen auf das Amtsblatt der Europäischen Union L119.

- Haftungsausschluss:

Die Angaben dieser Präsentation bzw. dieses Vortrags wurden sorgfältig bearbeitet, erfolgen aber ohne Gewähr. Eine Haftung des Vortragenden oder Salzburger Bildungswerkes ist ausgeschlossen.

Allgemeines zum Vortrag

Dieser Vortrag enthält Auszüge aus dem EU-Amtsblatt und dient der Information, Sensibilisierung und zur allgemeinen Orientierung für Vereinsfunktionäre und interessierte Personen.

Die Inhalte wurden aus methodischen Gründen auf die wesentlichen Inhalte für Vereine gekürzt.

Achtung! Bei der Umsetzung der DSGVO müssen die Inhalte der entsprechenden Artikeln als gesamtes beurteilt werden.

Grundlagen (Gesetze)

- Verordnung (EU) 2016/679
- EU Amtsblatt (ABl) L 119/32
- BGBl Nr. 120/2017
- Leitfaden der Datenschutzbehörde Österreich
- Seit 25. Mai 2018 in Kraft

Gegenstand und Ziele (Artikel 1)

- Einheitliches Datenschutzrecht (EU)
- Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten
- Schutz der Grundrechte und Grundfreiheiten für die Betroffenen
- Eigenverantwortung für Unternehmen und Organisationen

Sachlicher Anwendungsbereich (Artikel 2)

- Absatz 1: Geltungsbereich für die ganz oder teilweise automatisierte oder nichtautomatisierte Verarbeitung von Daten.
- Absatz 2 c) Keine Anwendung bei natürlichen Personen im persönlichen oder familiären Bereich.

Räumlicher Anwendungsbereich (Artikel 3)

- Absatz 1: Verarbeitung personenbezogener Daten durch Verantwortliche oder Auftragsverarbeiter mit einer Niederlassung innerhalb der EU
- Absatz 2: Verarbeitung von personenbezogener Daten betroffener Personen der EU

Begriffsbestimmungen (Artikel 4) -1-

- **Personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.
Zu den personenbezogenen Daten zählen auch **Bild- und Filmaufnahmen**.
- **Verarbeitung von Daten** ist eine Verarbeitung von Daten mit oder ohne automatisierten Verfahren.
- **Pseudonymisierung** ist die Verarbeitung personenbezogener Daten, ohne Zuordnung einer bestimmten Person.
- **Verantwortlicher** ist eine natürliche oder juristische Person, die Entscheidungen über die Verarbeitung personenbezogener Daten trifft.

Begriffsbestimmungen

(Artikel 4) -2-

- **Auftragsverarbeiter** ist eine natürliche oder juristische Person, die im Auftrag eines Verantwortlichen personenbezogene Daten verarbeitet.
- **Einwilligung** ist eine ausdrückliche und unmissverständliche Willensbekundung in Form einer Erklärung einer betroffenen Person.
- **Verletzung des Schutzes** (Sicherheit) personenbezogener Daten durch z.B. Vernichtung, Verlust, Offenlegung oder unbefugter Zugang.
- **Gesundheitsdaten** sind Daten über die körperliche oder geistige Gesundheit einer natürlichen Person, die Aufschluss über den Gesundheitszustand geben. Mit eingeschlossen ist auch die Erbringung von Gesundheitsdienstleistungen.

Grundsätze (Artikel 5) -1-

- Absatz 1:
 - a) Rechtmäßigkeit (Ausdrückliche Einwilligung)
 - Verarbeitung nach Treu und Glauben
 - Transparenz
 - b) Zweckbindung
 - c) Datenminimierung
 - d) Richtigkeit

Grundsätze (Artikel 5) -2-

- Absatz 1:
 - e) Speicherbegrenzung
 - f) Integrität und Vertraulichkeit
- Absatz 2: Der Verantwortliche muss die Grundsätze gemäß Absatz nachweisen können (=Rechenschaftspflicht)

Personenbezogene Daten, besondere Kategorien (Absatz 9) -1-

- Rassistische und/oder ethnische Herkunft
- Daten über Gesundheit
- Genetische oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person
- Religiöse oder weltanschauliche Überzeugung
- Politische Meinung
- Gewerkschaftszugehörigkeit
- Sexualleben oder sexuelle Orientierung

Personenbezogene Daten, besondere Kategorien (Absatz 9) -2-

- Absatz 1: Die Verarbeitung dieser personenbezogenen Daten ist untersagt
- Absatz 2: Der Absatz 1 gilt in den Fällen lit a) bis j) nicht, wenn
 - a) Die betroffene Person hat ausdrücklich zur Verarbeitung eingewilligt und es kann der Zweck nachgewiesen werden
 - b) Aus Arbeits- und Sozialrecht oder soziale Sicherheit
 - Schutz lebenswichtiger Interessen
 - e) Personenbezogene Daten, die bereits durch die betroffene Person öffentlich gemacht wurden
 - f) Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüche
 - h) Verarbeitung zum Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin (nur durch Fachpersonal = Berufsgeheimnis)

Rechte der Betroffenen -1-

- Transparente Information (Artikel 12)
- Informationspflicht
 - Bei der Erhebung der Daten - Formular „Ausdrückliche Einwilligung“ - (Artikel 13)
 - Wenn die Daten bei der betroffenen Person **nicht** erhoben wurden (Artikel 14)
- Auskunftsrecht (Artikel 15)
- Recht auf Berichtigung (Artikel 16)
- Recht auf Löschung (Artikel 17)

Rechte der Betroffenen -2-

- Recht auf Einschränkung der Verarbeitung (Artikel 18)
- Mitteilungspflicht an die Empfänger (Artikel 19)
- Recht auf Datenübertragbarkeit (Artikel 20)
- Widerspruchsrecht (Artikel 21)

Verzeichnis von Verarbeitungstätigkeiten (Artikel 30)

- Verzeichnis über Verarbeitungstätigkeiten
 - Absatz 1: Führung durch Verantwortliche
 - Absatz 2: Führung durch Auftragsverarbeiter
 - Absatz 3: Ist schriftlich zu führen
 - Absatz 4: Vorlage der Aufsichtsbehörde (nach Aufforderung)
 - Absatz 5: Zusätzliche Regelung bezüglich der Führung eines Verzeichnisses. Ist nur unter bestimmten Voraussetzungen zu führen

Sicherheit der Verarbeitung (Artikel 32)

- Absatz 1: Gewährleistung eines angemessenen Schutzniveaus
 - Zugriffsschutz bei Computer oder mobilen Geräte
 - Verschlüsselte Datenübermittlung (E-Mail)
 - Sicherung der Daten (Backup)
- Absatz 2: Risikoabschätzung (nur bei bestimmten Voraussetzungen)
- Absatz 3: Einhaltung von Verhaltensregeln (Artikel 40)
- Absatz 4: Regeln für die Verarbeitung personenbezogener Daten für unterstellte natürliche Personen (z.B. Funktionäre)

Meldung einer Verletzung des Schutzes personenbezogener Daten (Artikel 33)

- Ansatz 1: Eine Verletzung des Schutzes personenbezogener Daten ist unverzüglich und binnen 72 Stunden (ab Bekanntwerden dieser) der Aufsichtsbehörde zu melden.
- Absatz 3: Informationen die in dieser Meldung beinhaltet sein sollten.

Datenschutzbeauftragter (Artikel 37)

- Artikel 1, Benennung:
 - Verarbeitung durch eine Behörde oder öffentliche Stelle
 - Kerntätigkeit ist die Durchführung von Verarbeitungsvorgängen
 - personenbezogene Daten über strafrechtliche Verurteilungen oder Strafdaten

Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecke (Artikel 89)

- Absatz 1: Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken und statistischen Zwecken.
 - Organisatorische und technische Garantien wie z.B. Einschränkung des Zugriffs, Datenminimierung, Pseudonymisierung

Achtung! Eine Verarbeitung personenbezogener Daten bedeutet eine Änderung der damals vereinbarten Zweckbindung. Von den betroffenen Personen ist dafür eine zusätzliche „Ausdrückliche Einwilligung“ einzuholen.



Umsetzung der DSGVO

Erhebung des IST-Zustands -1-

- Welche personenbezogenen Daten werden verarbeitet und wie wurden diese erhoben?
- Werden personenbezogenen Daten, die gemäß Art. 9 den besonderen Kategorien zuzuordnen sind, verarbeitet?
- Besteht bei den personenbezogenen Daten eine Zweckbindung?
- Haben die Mitglieder bereits ausdrücklich in die Verarbeitung ihrer personenbezogenen Daten eingewilligt (Form der Einwilligung)?

Erhebung des IST-Zustands -2-

- Kann eine Datenminimierung durchgeführt werden?
- Wer arbeitet mit personenbezogenen Daten und sind diese autorisiert?
- Wie und in welcher Art werden die personenbezogenen Daten verarbeitet?
- Werden die personenbezogenen Daten sicher aufbewahrt und sind diese vor unbefugten Zugriff geschützt?
- Werden die personenbezogenen Daten gesichert (Backup)?

Ausdrücklichen Einwilligung

- Berücksichtigung der Bedingungen gemäß Artikel 7 und Artikel 8
- Muss einfach, klar und deutlich formuliert sein
- Grundsatz der Transparenz, Treu und Glauben
- Information über die Art und den Zweck der Verarbeitung personenbezogener Daten (inkl. Foto- und Filmaufnahmen)
- Datenaustausch oder Weitergabe an Dritte
- Dauer der Speicherung der Daten bzw. die Löschung
- Erläuterung der Betroffenenrechte

Einwilligung auf dem Webauftritt (Homepage)

- Berücksichtigung der Bedingungen gemäß Artikel 7
- Muss einfach, klar und deutlich formuliert sein
- Grundsatz der Transparenz, Treu und Glauben
- Bestätigung durch einen „Klick“
- Information welche Daten beim Besuch gespeichert werden
 - IP-Adresse, Browsertyp, Cookies, ...
- Dauer der Speicherung

Achtung! Bei einem Webauftritt müssen auch andere Gesetze und Regelungen beachtet werden

Richtlinien für Funktionäre

- Autorisierung und Aufgabenzuweisung (gemäß den Statuten)
- Information über die Bestimmungen des Datenschutzes und der Geheimhaltung (=Verpflichtung)
- Keine Weitergabe personenbezogener Daten an Dritte (ausgenommen einer Autorisierung)
- Zugriffsschutz auf eigenen Datenverarbeitungsgerät (Computer und mobile Geräte)
- Ausdrücke müssen vor unbefugtem Zugriff geschützt sein
- Unverzügliche Information bei einer Verletzung des Schutzes personenbezogener Daten

Foto- und Filmaufnahmen

- Foto- und Filmaufnahmen sind personenbezogene Daten
- Ausdrückliche Einwilligung ist erforderlich
- Der Zweck und die weitere Verarbeitung ist anzuführen (z.B. Dokumentation oder Veröffentlichung)
- Bei öffentlichen Veranstaltungen sollte das Fotografieren oder Filmen angekündigt werden (z.B. Eintrittskarte, Einladung, Durchsage, ...)
- Es müssen noch zusätzliche Gesetze und Bestimmungen berücksichtigt werden (z.B. Bildnisschutz, Urheberrecht, ...)

Speicherbegrenzung

- Bei Beendigung einer Mitgliedschaft ist der Zweck der Verarbeitung grundsätzlich nicht mehr gegeben
- Die personenbezogenen Daten sind unter Berücksichtigung anderer Gesetze oder Bestimmungen (z.B. Nachweispflicht beim Finanzamt oder Förderer) zu löschen
- Personenbezogene Daten können für Archivzwecke (Artikel 89) weiterhin gespeichert werden.
- Für vereinsinterne statistische Zwecke darf die Identität der betroffenen Person nicht mehr feststellbar sein (Pseudonymisierung)

Wiederholung





Vielen Dank für Ihre
Aufmerksamkeit

Workshop Umsetzung der DSGVO

am Freitag, den 19.10.2018 von 15 bis 17 und 18 bis 20 Uhr
im Vereinslokal der Pongauer Computer-Freunde

Haus der Vereine
5620 Schwarzach im Pongau

Bitte anmelden: obmann@pcf Freunde.org