Zu meiner Person

Michael Benz
(Sparkassen-Betriebswirt)

Funktion

Auditor und Berater für Qualitätsmanagementsysteme und Datenschutz

Externer Datenschutzbeauftragter

DR. FRANKE, NECKER BRITSCH LL.M. & WOLFSTEINER

Steuerberater - Rechtsanwälte - Fachanwälte - vereidigter Buchprüfer

DIE NEUE DATENSCHUTZ-GRUNDVERORDNUNG (EU-DSGVO)

Umsetzung in den Unternehmen

- Rechtsgrundlagen für die Verarbeitung (Einwilligung, Vertragserfüllung, berechtigtes Interesse)
- Voraussetzungen bei besonderen Kategorien personenbezogener Daten
- Datenschutzerklärung im Internet
- Wann ist ein Datenschutzbeauftragter zu benennen?
- Datenschutzverletzungen und Sanktionen
- Verzeichnis der Verarbeitungstätigkeiten

Rechtsgrundlagen für die Verarbeitung

- Grundsatz: Verbot mit Erlaubnisvorbehalt

- Rechtmäßige Verarbeitung, wenn
  - zur Vertragserfüllung
    - häufige Rechtsgrundlage in Unternehmen
  - zur Wahrung berechtigter Interessen des Verantwortlichen (z.B. bei Kontaktdaten von Vertriebsmitarbeitern)
    - Interessen der betroffenen Person dürfen nicht überwiegen
    - Definition des berechtigten Interesses muss Zweckbindung erläutern
  - eine Einwilligung vorliegt
    - Freiwillig / Bestimmt / Klar / Verständlich / Bestätigt

Rechtsgrundlage „Einwilligung“ (Beispiel - Vereinsmitglied)

Hiermit erklärt das Mitglied sein Einverständnis, dass die erhaltenen Kontakt- und Personendaten zur Abwicklung vereinsinterner Registrierung und Mitgliederverwaltung verarbeitet und genutzt werden dürfen. Im Rahmen der Mitgliederverwaltung und -pflege dürfen diese Daten auch an öffentliche Stellen und verbundene Vereine weitergeleitet werden.

Erweiterung der Einwilligung:

[ ] Die Daten des Mitglieds dürfen auch in Vereinsmitteilungen veröffentlicht werden.

[ ] Bilder des Mitglieds dürfen in Vereinsbroschüren und weiteren Veröffentlichungen (u.a. Presse) genutzt werden

(Zutreffendes – soweit gewünscht – bitte ankreuzen)

Die Einwilligungserklärung kann jederzeit für künftige Nutzungszwecke beim Vereinsvorstand widerrufen werden. Gesetzliche Erlaubnistatbestände bleiben von diesem Widerruf unberührt.

Voraussetzungen bei besonderen Kategorien personenbezogener Daten

- Das sind …
  - Angaben über rassische und ethnische Herkunft
  - Politische Meinungen
  - Religiöse Überzeugungen
  - Gewerkschaftszugehörigkeit
  - Gesundheitsdaten
  - Daten über das Sexualleben
  - Genetische und biometrische Daten

- Besonders schutzbedürftig gem. Art. 9 DS-GVO

Voraussetzungen bei besonderen Kategorien personenbezogener Daten

Grundsatz: Verarbeitungsverbot mit Ausnahmevorbehalt

Ausnahmen (in Auszügen):

- Rechte und Pflichten des Arbeits- und Sozialrechts
- Zum Schutz lebenswichtiger Interessen (z.B. Unfall/Notfall)
- Durch geeignete Organisationen ohne Gewinnerzielungsabsicht
- Wenn durch die betroffene Person offensichtlich öffentlich bekannt gemacht
- Zwecke der Gesundheitsvorsorge, Versorgung, Behandlung durch Berufsgeheimnisträger

Datenschutzerklärung im Internet (Form)

- Präzise
- Transparent
- Verständlich
- Leicht zugänglich
- Klare und einfache Sprache

Datenschutzerklärung im Internet (wesentlicher Inhalt)

- Name und Kontaktdaten des Verantwortlichen + ggf. Kontaktdaten des Datenschutzbeauftragten
- Welche Daten werden erhoben (z.B. IP-Adresse, Browser, Surfdauer, bei Formular: Kontaktdaten)
- Zwecke der Verarbeitung (z.B. Statistik, Seitenoptimierung, bei Formular: Kontaktaufnahme) und Rechtsgrundlage
- Wie lange werden die Daten gespeichert (ggf. Hoster fragen!)
- Wer ist Empfänger der Daten (Verantwortlicher, Hoster) und gehen diese außerhalb der EU
- Welche Rechte hat der Betroffene (Auskunft, Löschung, Einschränkung, Beschwerderecht)
- Nutzung automatisierter Entscheidungsfindungen (z.B. Cookies, Google Analytics)

Datenschutzbeauftragter (wann zu benennen)

- Mindestens 10 Personen mit personenbezogener Daten beschäftigt
- Verarbeitung von besonderen Kategorien pbD in erheblichem Umfang (z.B. Krankenhäuser, Banken, Versicherungen, auch: ärztliche Gemeinschaftspraxen)
- Regelmäßige und systematische Überwachung ist Kerntätigkeit des Unternehmens/Vereins

Grundlagen:

Art. 37 DS-GVO / § 38 BDSG-neu /
Art-29-Gruppe: Arbeitspapier WP243 „Leitlinien in Bezug auf Datenschutzbeauftragte“

Datenschutzbeauftragter (Aufgaben / Veröffentlichung)

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten
- Beratung betroffener Personen
- Überwachung der Einhaltung der Vorschriften
- Beratung bei Datenschutz-Folgeabschätzung
- Zusammenarbeit mit Aufsichtsbehörde
- Anlaufstelle für die Aufsichtsbehörde

- Veröffentlichung der Kontaktdaten des DSB (Name nicht notwendig)
- Meldung des DSB an Aufsichtsbehörde

Datenschutzverletzungen (Beispiele des Alltags)

- E-Mailversand an alle Vereinsmitglieder als direkte Empfänger (An..) oder Kopie (Cc..), so dass jeder alle persönlichen Mailadressen lesen kann
  (wurde schon mal mit Bußgeld von Aufsichtsbehörde belegt!)
- Versand einer Patientenüberweisung versehentlich an falsche Faxnummer
- Verlust eines Mobiltelefons oder Notebooks mit betrieblichen (Kunden-)Daten

Achtung:

- (meldepflichtige) Datenschutzverletzungen müssen **innerhalb 72 Stunden** an die Aufsichtsbehörde gemeldet werden

Sanktionen

- Art. 83 DS-GVO
  „Geldbuße muss in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein“

- Bei nicht vorhandenen Datenschutzregularien
  - Bis zu 10 Mio. EUR oder 2% des Jahresumsatzes (höherer Betrag)

- Bei Verletzung der Betroffenenrechte (einschl. nicht vorhandener Rechtsgrundlage
  - Bis zu 20 Mio. EUR oder 4% des Jahresumsatzes (höherer Betrag)

Verzeichnis der Verarbeitungstätigkeiten

Mindestinhalte (Art. 30 Abs. 1 DS-GVO)

- Name und Kontaktdaten des Verantwortlichen
- Zwecke der Verarbeitung
- Kategorien betroffener Personen
- Kategorien personenbezogener Daten
- Kategorien von Empfängern der Daten
- Übermittlung an Drittländer oder internationale Organisationen
- Vorgesehene Fristen der Löschung (und Aufbewahrung)
- Technische und organisatorische Maßnahmen

- Rechtsgrundlage (empfohlene Erweiterung)

Verantwortlicher:
TSV Waldermühl e.V.
Steinbauerstr. 45a
98123 Sonsthausen

Tel. 0981/123456-0
E-Mail: team@waldermuehler-tsv.de
Web: www.waldermuehler-tsv.de

Vorstand: Dieter Eckbauer-Düppels, geb. 03.12.1952

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	02.03.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name und Adressen der Beschäftigten • ggf. Religions-zugehörigkeit • Eindeutige Kennzahlen zur Steuer/ Sozialabgaben ...	Externer Dienstleister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Mitgliederverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	02.03.2018	Verwaltung der Vereinstätigkeiten	Mitglieder	• Name und Adressen • Eintrittsdatum • Sportbereiche ...	Keine	Keine	2 Jahre nach Beendigung der Vereinsmitgliedschaft	Siehe IT-Sicherheitskonzept
Betrieb der Webseite des Sportvereins (über Hosting-Dienstleister)	Max Meier 0981/123456-0 max@ waldmuehler-tsv.de	28.02.2018	Außendarstellung	• Mitglieder • Webseitenbesucher	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept + HTTPS-Verschlüsselung
Veröffentlichung von Fotos der Mitglieder auf der Webseite	Max Meier 0981/123456-0 max@ waldmuehler-tsv.de	20.02.2018	Außendarstellung	Mitglieder	Fotos von Vereinstätigkeiten	Keine	Keine	Wenn Einwilligung widerrufen - unverzüglich	Siehe IT-Sicherheitskonzept
Beitragsverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	22.02.2018	Vereinsfinanzierung	Mitglieder	Bankverbindung	Steuerberater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...	...	...	...	...	...	...	...	...	...

Quelle: Bayerisches Landesamt für Datenschutz-Aufsicht
(Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

Wenn sie bisher noch nichts gemacht haben …

Mindestens bis Ende Mai erledigen …

- Verzeichnis der Verarbeitungstätigkeiten erstellen (Mindestinhalt, rudimentär)
- Prüfung ob Datenschutzbeauftragter benötigt wird, wenn ja – bestellen und melden
- Website (Impressum, Datenschutzerklärung) aktualisieren
- Ablauf planen und festhalten für
  - Meldung einer Datenschutzverletzung
  - Auskunftsanfrage eines Betroffenen
- Mitarbeiter über Datenschutz aufklären und ggf. zur Einhaltung verpflichten
- Planung der Umsetzung weiterer Sachverhalte

Fragen?

Vielen Dank für Ihre Aufmerksamkeit