EU – Datenschutz-grundverordnung

Die „neue“ EU-DSGVO

- Inkrafttreten 25.05.2018
- EU-weite Gültigkeit
- Verordnung = nationales Recht
- Bundes- und Landesgesetze
- Große Teile galten schon früher

Schlechte Nachricht

- ALLE Vereine sind betroffen
  - Nicht für kirchliche Institutionen und Vereine (KDG)
- Datenschutz ist Chefsache (BGB-Vorstand)
- Datenschutzbeauftragter berät und unterstützt

Gute Nachricht:

- Alte Informationen gelten fort!
  - falls sie bereits einen Hinweis auf das Widerrufsrecht haben

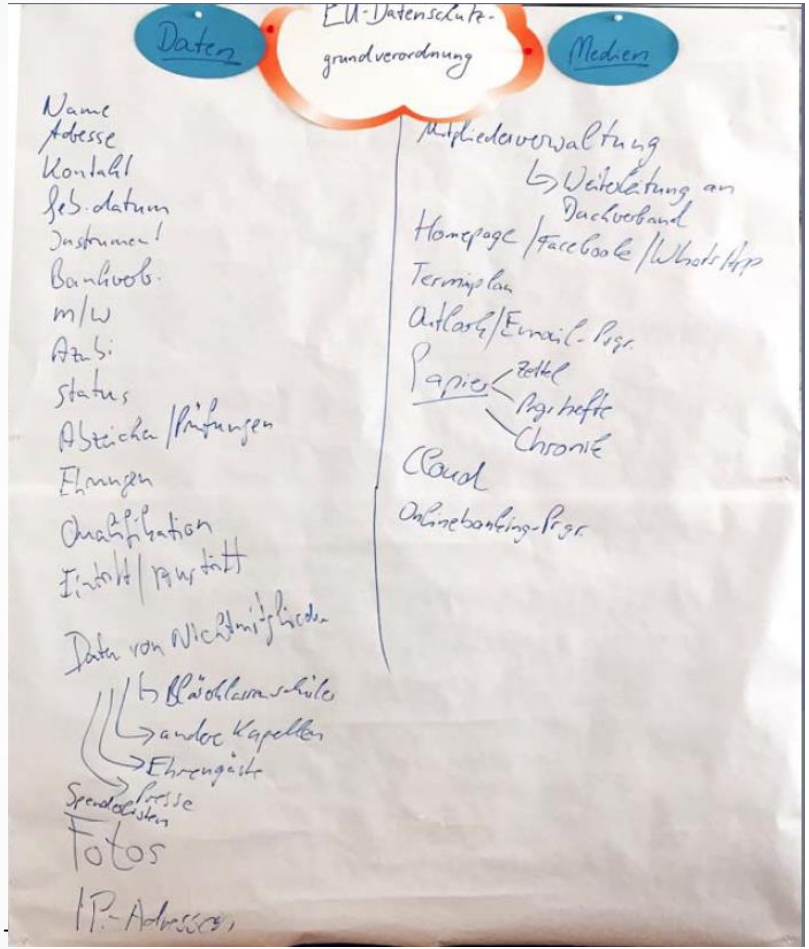
Prinzipien der Datenverarbeitung nach Art. 5 EU-DSGVO

- Rechtmäßigkeit, Verarbeitung nach Treu und Glaube, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Erste Schritte

- Bestandaufnahme: Wo werden Daten verarbeitet?
- Kritische Punkte nach außen prüfen:
  - Impressum und Datenschutz auf der Homepage
  - Impressum Social Media
- Erstellung Datenschutzordnung

Welche Daten werden verarbeitet?



Umsetzung

- Festlegung der Rechtsgrundlagen (Art. 6)
- Einwilligungen einholen
- Prüfungen Datenweitergabe nach außen (Auftragsdatenverarbeitung)
- Informationspflichten und Auskunftsrechte vorbereiten
- Vorsorge für Datenschutz durch Technik und Organisation treffen

Überblick der EU-DSGVO

- **Allgemeine Bestimmungen**
  - **Rechtmäßigkeit der Verarbeitung (Art. 6)**
  - **Einwilligung zur Verarbeitung (Art. 7)**
- **Rechte der betroffenen Personen**
  - **Informationspflicht bei Erhebung der Daten beim Betroffenen (Art. 13)**
  - Informationspflicht bei Erhebung der Daten bei Dritten (Art. 14)
  - **Auskunftsrecht des Betroffenen (Art. 15)**
  - Sonstige Rechte (Berichtigung, Löschung) (Art. 16, 17), (Einschränkung, Datenübertragung) (Art. 18, 20)
  - Recht auf Beschwerde bei der Aufsichtsbehörde (Art. 77).
- **Widerspruchsrecht im Einzelfall**
- **Handlungspflichten des Verantwortlichen**
  - Informationspflicht bei Erhebung der Daten (Art. 13)
  - Sicherheit der Verarbeitung (Risikoeinschätzung) (Art. 32)
  - Meldung bei Verletzungen an Aufsichtsbehörde (Art. 33)
- **Verantwortung für die Verarbeitung**
  - **Generelle Verantwortung des Verantwortlichen (Art. 24),**
  - **Datenschutz durch Technikgestaltung und Organisation (Art. 25, 26),**
  - Auftragsverarbeitung (Art. 28, 29)
  - **Verzeichnis der Verarbeitungstätigkeiten (Art. 30)**
  - Zusammenarbeit auf Anfrage der Aufsichtsbehörde (Art. 31)
- **Datenschutzbeauftragter**
  - **Benennung eines Datenschutzbeauftragten (Art. 37, § 38 BDSG),**
  - Stellung des Datenschutzbeauftragten (Art. 38),
  - Aufgaben des Datenschutzbeauftragten (Art. 39)
- **Aufsichtsbehörden**
  - Aufsichtsbehörde (Art. 51 ff)
  - **Sanktionen, Bußgelder** Art. 83, §§ 41, 43 BDSG

Welche Verein sind betroffen?

- ALLE Vereine, die personenbezogene Daten verarbeiten, unabhängig
  - wie groß der Verein ist
  - wie viele Personen mit Daten arbeiten
  - egal ob EDV oder über Karteikarten

→ also jeder Verein!

Datenverarbeitung

- Eine Verarbeitung liegt vor, wenn mit den personenbezogenen Daten etwas gemacht wird, also wenn
  - Daten erhoben, erfasst, gespeichert, verwendet, geordnet, angepasst, verändert, ausgelesen,
  - abgefragt, offengelegt, verbreitet, bereitgestellt, abgeglichen, verknüpft, eingeschränkt, gelöscht oder auch vernichtet werden.
- Es gleichgültig, ob die Verarbeitung automatisiert oder manuell erfolgt, beispielsweise in Form von Karteikarten oder ausgedruckten Listen, die verbreitet oder bereitgestellt unddann verwendet werden.

Beispiele für Datenverarbeitung

- Speicherung von Mitgliedsdaten
- Weitergabe von Daten an Dachverbände
- Veröffentlichung von Daten auf der Homepage oder Facebook
- Veröffentlichung von Daten in der Vereinszeitschrift
- Aushänge am schwarzen Brett

Was sind personenbezogene Daten?

- Name, Vorname, Adresse, Kontaktdaten, Bankverbindungen, …
- Daten von Kunden und Geschäftspartnern (sofern keine juristische Person)
- Daten von Ehrenamtlichen und Mitarbeitern
- IP-Adressen

Besondere Arten von pers.-bezogenen Daten

- Familienstand
- Religionszugehörigkeit, Ethnische Herkunft
- Politische Meinung
- Gesundheitsdaten

→ Pflicht Datenschutzbeauftragter

Datenschutzbeauftragter

- Bestellung wenn,
  - mehr als 9 Personen mit der Datenverarbeitung betraut, egal ob ehrenamtlich oder beruflich
  - Verarbeitung besonderer Daten
  - nicht Mitglieder des BGB-Vorstand
  - nicht Mitglieder, die EDV betreuen

Aufgaben Datenschutzbeauftragter

- Aufklärung über bestehende datenschutzrechtliche Pflichten und deren Einhaltung überwachen.
- Ansprechpartner für die Anfragen von Behörden und Betroffenen.
- führt das Verarbeitungsverzeichnis
- Ansprechpartner allen Fragen im Umgang mit Nutzer- und Kundendaten.
- Schulung zum Datenschutz
- Verantwortung liegt weiter beim Vorstand

Datenschutzbeauftragter Unterschied

Pflicht zur Bestellung des Datenschutzbeauftragen,

- wenn mehr als 9 Personen ständig Daten verarbeiten (z.B. Mitgliederverwaltung macht).
- Nicht dazu zählen, wer nicht ständig verarbeitet (z.B. Übungsleiter der kurz für 3 Minuten in sein Adressbuch schaut)

Datenschutzbeauftragter Unterschied

Pflicht zur Bestellung des Datenschutzbeauftragen,

- wenn mehr als 9 Personen Daten verarbeiten.
- Ein regelmäßiger, punktueller, kurzer Zugriff reicht aus um mitzuzählen. Es ist kein dauerhafter Zugriff nötig

Datenschutzbeauftragter

Nicht dazu zählen, wer nicht ständig verarbeitet (z.B. Übungsleiter der kurz für 3 Minuten in sein Adressbuch schaut)

Bayern

Ein regelmäßiger, punktueller, kurzer Zugriff reicht aus um mitzuzählen. Es ist kein dauerhafter Zugriff nötig

Baden-Württemberg

Homepage

- Pflicht zu Impressum (und) Datenschutzerklärung
- Korrekte und an DSGVO angepasste Form ist Pflicht, da von außen einsehbar
- Impressum-Generatoren im Internet nutzen
- Veröffentlichung von Adressdaten nur bei Einwilligung
- Ausnahme: gewählte Funktionsträger (dienstliche Daten)
- Verschlüssellung

Homepage Impressum

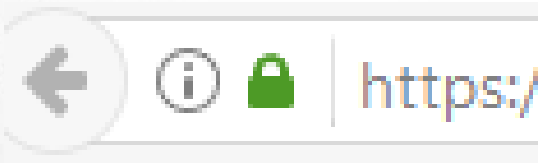
- Impressum muss Impressum heißen
- Impressum muss als Seite vorhanden sein (kein reiner pdf-Download)
- Impressum muss gut lesbar sein
- Zwei-Klick-Regel

Homepage Datenschutzerklärung

- Pflicht, wenn personenbezogene Daten verarbeitet werden:
  - Kontaktformular
  - Newsletteranmeldung
  - Analyse-Tools: Piwik, Google Analytics
  - Shop
  - Cookies

Homepage Verschlüsselung

- Verschlüsselung der Verbindung PC <-> Server
- Keine generelle Pflicht
- Pflicht bei Übertragung pers. Daten
  - Kontakt- und Anfrageformulare
  - Seiten, auf denen etwas bestellt werden kann
  - Downloadseiten auf denen der Nutzer seine E-Mail-Adresse angibt
  - Newsletter-Eintrage-Seiten
  - Log-In-Seiten
  - Seiten, auf denen Zahlungsprozesse ablaufen



Homepage Newsletter

- Kein Versand an Empfänger ohne Einwilligung
- Interessent muss sich aktiv in Newsletter
- Double-Opt-In-Verfahren ist zu nutzen
    - Interessent trägt seine Mailadresse in Formular ein
    - Interessent erhält eMail mit Bestätigungslink
    - Interessent muss Bestätigungslink folgen zum Erhalt Newsletter

Homepage Cookie

Wir benutzen Cookies um für Sie eine möglichst komfortable Bedienung und Funktionalität zu gewährleisten. Wenn Sie ohne Änderung Ihrer Einstellungen fortfahren, gehen wir davon aus, dass Sie damit einverstanden sind, alle Cookies von unserer Website zu empfangen. Diese Einstellungen können Sie jederzeit ändern. Weitere Informationen

OK

- Cookie-Richtlinie der EU ab 2019 (E-Privacy-Richtlinie)
- Nicht in deutsches Recht umgesetzt
- Laut EU-Kommission in D nicht nötig
- Hinweis in Datenschutzerklärung zu Cookies nötig

Wann dürfen Daten verarbeitet werden?

- Grundsatz:

  VERBOT mit Erlaubnisvorbehalt

- Erlaubnisvorbehalt:
  - Gesetzliche Grundlage
  - Einwilligung des Betroffenen

Gesetzliche Grundlage

- Rechtliche Pflicht
  - z.B. Aufbewahrung von Buchhaltungsdaten
- Zur Vertragserfüllung notwendig
  - Mitgliedschaft = Vertrag
- Interesse des Verein
  - Datenweitergabe an Dachverband, Versicherung, Buchhaltung

Einwilligung

- Freiwillige Einwilligung des Betroffenen:
  - Nutzung von Fotos
  - Weitergabe von Daten an Dritte
  - Empfang Werbung
- Möglichst im Aufnahmeantrag

Inhalt Einwilligung

- Freiwillige Entscheidung
- Welche Daten werden gespeichert
- Zu welchem Zweck
- Hinweis auf Widerrufsmöglichkeit
- möglichst schriftlich

Datenschutzordnung

- Anlage der Satzung
- Kann leichter geändert werden als Satzung
- Grundzüge der Datenverarbeitung definieren
  - Welche Daten werden erhoben
  - Welche Daten werden Weitergeben
  - Pressearbeit

Verarbeitungsverzeichnis

- Übersicht wie mit Daten gearbeitet wird
- Pflicht >250 Mitglieder, außer
  - Verarbeitung besonderer Daten
  - Kontinuierliche Datenverarbeitung
    - Beispiel: Mitgliederverwaltung

→Pflicht für so gut wie jeden Verein

→Kein Verzeichnis = Bußgeld

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten" gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für Datenschutzaufsicht

Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

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

Auftragsdatenverarbeitung

- Datenverarbeitung im Auftrag durch einen Dritten, bei der die Verantwortung beim Auftraggeber (Verein) bleibt
- Dienstleister nur unterstützend tätig (verlängerter Arm des Verein)
- Auftragsdatenverarbeitung ist keine Weitergabe von Daten, daher leichtere Voraussetzungen

Auftragsdatenverarbeitung

- Klassische Bereiche:
  - Externe Lohnabrechnung
  - Homepage-Hosting
  - Clouds
  - Mitgliederverwaltung im Internet

→ Verträge von Anbietern einfordern

Auftragsdatenverarbeitung

- Keine Auftragsdatenverarbeitung:
  - Berufsgeheimnisträger
    - Steuerberater, Rechtsanwälte
  - Kreditinstitute
  - Postdienste

Technischer & organisatorischer Datenschutz

- PC und Laptop mit Passwort schützen
- Sichere Passwörter / regelmäßig ändern
- Firewall / Virenscanner
- Datensicherung auf externe Festplatter
- Regelmäßige Updates
- Sperren von PC / Laptop bei Abwesenheit
- Verschlüsselte USB-Sticks

Technischer & organisatorischer Datenschutz

- Zugang zu Büro / PC beschränken
- Vertrauliche Daten in Papierform wegsperren
- Personenbezogene Daten auf Papier vernichten -> Aktenvernichter
- eMail-Versand: max 1 Adresse in An, bzw. CC, alle anderen in BCC

Technischer & organisatorischer Datenschutz

- Sicherheitskonzept für alle Mitarbeiter einschließlich Ehrenamtlichen
- Schulung aller Personen, die mit pers. Daten verarbeiten
- Verpflichtungserklärung aller Personen, die mit pers. Daten arbeiten

Betroffenenrechte

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung
- Widerspruchsrecht

Recht auf Auskunft

- Jeder Betroffene kann eine Auskunft verlangen, ob und welche Daten gespeichert sind
- Antwort innerhalb 1 Monat
- Maschinenlesbare Form

Recht auf Löschung

- Löschung muss durchgeführt werden:
  - Daten nicht mehr benötigt werden, weil Zweck entfallen
  - Daten unrechtmäßig verarbeitet wurden
  - Einwilligung widerrufen wurde

Verhalten bei Datenpannen

- Datenpannen:
  - Weitgefasster Begriff:
    - von Falschversand von eMails
    - bis Hackerangriff
  - Meldepflicht gegenüber Behörde und Betroffenen innerhalb von 72 Stunden
  - Online-Formular zu Meldung

Datenschutzbehörde

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit

Postfach 10 29 32
70025 Stuttgart
Tel.: 0711/615541-0
FAX: 0711/615541-15

poststelle@lfdi.bwl.de

Datenschutzbehörde Aufgaben

- Meldung Datenschutzbeauftragter
- Meldung von Datenpannen
- Beschwerden einreichen
- Informationen und Handlungsempfehlungen

Bußgelder

- **Bis 10 Mio. EUR / 2% d. weltweiten Jahresumsatz**
  nach Art. 83 Abs. 4 DSGVO
  - Einwilligung von Kindern (Art. 8 DSGVO)
  - ADV (auch gg. Auftragnehmer! - Art. 29 DSGVO)
  - Unzureichende Dokumentation (Art. 30 DSGVO)
  - Zusammenarbeit mit der Aufsichtsbehörde (Art. 31 DSGVO)
  - Unzureichende TOMs (bisher nicht bußgeldbewehrt - Art. 32 DSGVO)
  - Meldung von Datenschutzverstößen an Aufsicht und betroffene Personen (Art. 33,34 DSGVO)
  - Nicht durchgeführte DS-Folgenabschätzung bzw. Konsultation der Aufsicht (Art. 35, 36 DSGVO)
  - Benennung, Stellung und Aufgaben des DSB (Art. 37, 38, 39 DSGVO)
  - Pflichten der Überwachungs- und Zertifizierungsstellen (Art. 41,42,43 DSGVO)

- **Bis 20 Mio. / 4% d. weltweiten Jahresumsatzes**
  (je nachdem was höher ist)
  - Verstöße gegen Grundsätze nach Art. 5 DSGVO
  - Verstoß gegen Rechtmäßigkeit der Verarbeitung (Art. 6 DSGVO)
  - Verarbeitung ohne Einwilligung (Art. 7 DSGVO)
  - Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO)
  - Verstöße bei Beachtung der Rechte betroffener Personen (Art. 12-22 DSGVO)
  - Verstöße bei Drittlandsübermittlungen (z.B. in die USA - Art. 44-49 DSGVO)
  - Verstöße gegen Vorschriften der Mitgliedsstaaten in besonderen Verarbeitungssituationen nach Kapitel IX DSGVO
  - Verstöße bei der Zusammenarbeit mit der Aufsichtsbehörde
  - Verstöße gegen Anordnungen der Aufsichtsbehörde

Facebook

- Sowohl Facebook-Fanpage bzw. –Seite, als auch
- die Nutzung von Social-Media-Plugins auf der Homepage ist
- nach DSGVO problematisch und kaum sicher hinzubekommen
- Urteil EuGH C-210/16 vom 05.06.18
- Tipp: Shariff-/2-Klick-Lösung

WhatsApp

- alle Kontaktdaten aus dem Adressbuch werden an WhatsApp übertragen
- WhatsApp sammelt unkontrolliert Metadaten von Nutzern (wer mit wem, wie oft) zur Erstellung von Nutzerprofilen

→ Verstoß gegen EU-DSGVO

WhatsApp-Gruppe

- Entspricht nicht der EU-DSGVO, da Verein den Informationspflichten nicht nachkommen kann (Impressum, Datenschutzerklärung)
- Egal ob Betroffene eingewilligt haben oder nicht
- Nur private Gruppenbildung unter Mitgliedern möglich

Nutzung von Fotos

- Keine Änderung zu früher
- Nicht DSGVO, sondern KUG
- Fotos mit Personen enthalten personenbezogene Daten (auch ohne Namensangabe)
- Dürfen nur mit Einwilligung der Abgebildeten veröffentlicht werden
- Entlohnung = Einwilligung

Nutzung Fotos

- Grundsätzlich Einwilligung nötig
- Ausnahme:
  - Bildnisse Bereich Zeitgeschichte
  - Personen sind nur Beiwerk von Landschaften oder Örtlichkeiten
  - Bilder von Versammlungen, Aufzügen, o.ä. an denen die dargestellten Personen teilgenommen haben (Menschenansammlung)

Nutzung Fotos

Menschenansammlung:

Wer an öffentlichen Veranstaltungen teilnimmt, muss damit rechnen, abgebildet zu werden und muss dies in gewissen Grenzen akzeptieren. Die Vorschrift erfasst Veranstaltungen aller Art, wie öffentliche Demonstrationen, Karneval-Umzüge, Sportveranstaltungen, Konzerte und Kongresse

Nutzung Fotos

- Politiker-Besuch
  - Politiker sind Personen der Zeitgeschichte
  - Sonstige Personen sind Beiwerk

- Musikverein will Konzert dokumentieren
  - Auf Fotos können Gesichter einzelner Zuhörer erkennbar sein
  - Kein Zoomen auf einzelne Personen
  - Fotos ohne Zustimmung erlaubt (Versammlung)

Nutzung Fotos

- Frauenfußballspiel
  - Bei einem Zweikampf ist die nackte Brust zu sehen -> Einwilligung nötig
  - Frau reißen am Anfang Trikot hoch, als politisches Statement gegen Diskriminierung -> Einwilligung nicht nötig
- Mannschaftsfoto
  - Bewusste Entscheidung des Einzelnen sich aufzustellen -> keine Einwilligung nötig für Aufhängen im Vereinsheim, für Internet jedoch nötig
- Vereinschronik
  - Veranstaltungsbilder erlaubt, auch spätere Ausstellung
  - Einzelbilder (Vorstand), nur mit Einwilligung

Nutzung Fotos

- Besser Einwilligung
- Vorbeugende, allgemeine Einwilligung rechtlich nicht gültig
- Denkbar: konkrete Situation in Satzung oder Beitrittserklärung definieren
- Besonders Augenmerk auf Fotos von Jugendlichen

  → Zustimmung beider Erziehungsberechtigten !

Wenn das Bauchgefühl sagt, etwas ist nicht gut, ist es meistens auch nicht gut.

oder anders gesagt:

Fragen Sie vor einer Veröffentlichung eines Bildes einer anderen Person, ob Sie es auch im Internet veröffentlichen würden, wenn Sie selbst auf den Foto zu sehen wären.

Zusammenfassung

- Bestandsaufnahme machen
- Rechtsgrundlagen der Datenspeicherung prüfen/festlegen
- Homepage: Impressum / Datenschutzerklärung
- Dokumentation erstellen (Datenschutzordnung, Verarbeitungsverzeichnis)
- Einwilligungen neu formulieren (Hinweis auf Widerspruchsrecht)

Zusammenfassung

- Datenschutzbeauftragter
- Datenschutz durch Technik & Organisation
- Verträge zur Auftragsdatenverarbeitung
- Melde- und Kontrollpflichten gegenüber Behörden umsetzen
- Betroffenenrechte und Informationspflichten umsetzen


Erste Hilfe zur
Datenschutz-Grundverordnung
Herausgegeben vom
Bayerischen Landesamt für Datenschutzaufsicht
C.H.BECK
€ 5,50
Erste Hilfe zur
Datenschutz-
Grundverordnung
für Unternehmen
und Vereine
Das Sofortmaßnahmen-Paket

Auf die Plätze, fertig, los!

Es ist auf jeden Fall besser, mit dem Projekt DSGVO halb fertig zu sein, als – im Fall der Fälle - zugeben zu müssen, dass man noch nicht einmal begonnen hat.

Zeit für Austausch