3rd Mind Business Consulting

Projektmanagement • Audit • Beratung • Training
IT-Compliance • Informationssicherheit • Datenschutz

„Nicht alles, was technisch machbar, ist auch juristisch erlaubt bzw. betriebswirtschaftlich sinnvoll“.

Kreisverwaltung Mayen-Koblenz (KV MYK) • DS-GVO für Vereine • 24.10.2018

Datenschutz im Lichte der **EU DS-GVO**

JUNGER LANDKREIS
MIT TRADITION

in Kooperation mit

3rd Mind
Business Consulting
IT • COMPLIANCE • DATENSCHUTZ

 • 65760 Eschborn / Ts. • www.3rd-mind.de • frank.giebel@3rd-mind.de • Tel.: +49 (0) 6173 322 527 Fax: +49 (0) 6173 322 528

JUNGER LANDKREIS MIT TRADITION

Ihr Referent

Frank Giebel
(Geschäftsführer)
3rd Mind Business Consulting GmbH

Ext. Datenschutzbeauftragter (HWK)
IT-Revisor (ISACA, IRCA)
ISO 27001 Lead Auditor (BSI.Group)
ISO 27001 Implementierer (BSI.Group)
Lead Auditor Datenschutz (azmCERT)

CISA Certified Information Systems Auditor – An ISACA® Certification

CISM Certified Information Security Manager – An ISACA® Certification

Cyber-Security Practitioner

- **3rd Mind Business Consulting GmbH**
  - Spezialisiertes Beratungsunternehmen (gegründet 2009)
  - Datenschutz + Informationssicherheit + rechtssichere Archivierung
  - Beratung + Projektgeschäft + Audit / Revision
- **Spezialisierung**
  - Externer Datenschutzbeauftragter
  - Datenschutzrecht – Vertragsrecht – Auftragsverarbeitung
  - Schulungen + Dozententätigkeit
- **(Über-)Regional aufgestellt**
  - Hessen – Rheinland-Pfalz – Nordrhein-Westfalen
  - Vor Ort + remote (Fernberatung)
  - Dort wo Sie uns brauchen!

Bundesverband der Wirtschaftsjuristen e.V. – seit 2000 – Mitglied – WJFH
ISACA – Trust in, and value from, information systems
GDD Mitglied – Gesellschaft für Datenschutz und Datensicherheit e.V.
Allianz für Cyber-Sicherheit
azm cert – Akkreditierte Zertifizierungsgesellschaft Mittelstand

JUNGER LANDKREIS MIT TRADITION

Datenschutz – *„na und?“*

„Tatsachen schafft man nicht dadurch aus der Welt, indem man sie ignoriert.“*

(Aldous Huxley)
Britischer Schriftsteller

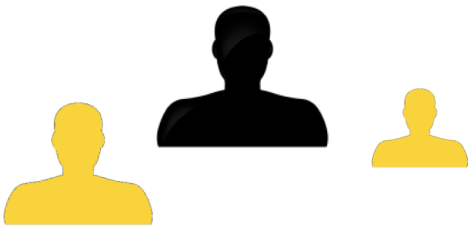
* Original: *„Facts do not cease to exist because they are ignored“* [1955: Speaker's Handbook of Epigrams and Witticisms, Seite 99, Verlag Harper]

Agenda

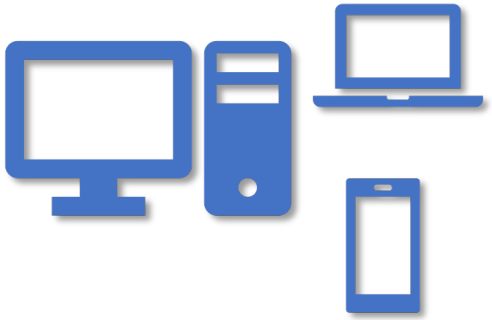
GEMEINSAMES VERSTÄNDNIS	→ Was ist „Datenschutz“?
ENTSCHLEIERT	→ Die EU Datenschutz-Grundverordnung (DS-GVO)
VERSCHÄRFTE WAHRNEHMUNG	→ Betroffenen-Rechte im Datenschutz
SCHADENSBEGRENZUNG	→ Datenpannen + Meldepflichten
ANGSTMACHER	→ Sanktionen + Abmahn-Industrie
DIGITALISIERUNG	→ Was ist „online“ zu beachten?
VERARBEITUNG + VEREINSLEBEN	→ Rechtsgrundlagen + Pflichten im Tagesgeschäft

GEMEINSAMES VERSTÄNDNIS – „Was ist Datenschutz?“

- **Datenschutz ist ein Grundrecht**
  - In der **EU**: Art. 8 der EU Grundrechte-Charta (2010/C 83/02)
  - In **Deutschland**: “Volkszählungsurteil“ v. BVerfG 1983 i.V.m. Artt. 1 (1), 2 (1) GG)
  - → Grundrechte sind unabdingbar!



Schutz der Person(en)
= **Datenschutz**



Schutz der Daten
= **Datensicherheit / IT-Sicherheit (TOM*)**

* TOM = Technisch-Organisatorische Maßnahmen (→ vgl. Art. 32 DS-GVO)

Datenschutz ist ein Grundrecht

Jeder Mensch

soll grundsätzlich **selbst** über die

Preisgabe und Verwendung

seiner persönlichen Daten **bestimmen.**

Volkszählungsurteil, 1983

Wer muss das Datenschutzrecht beachten („Scope“)?

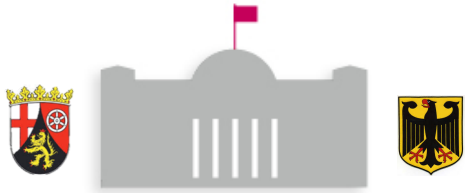
Öffentliche Stellen*

Kreiswehrersatzämter

Bundesagentur für Arbeit

Kreisverwaltungen

Sonstige Behörden



Nicht-öffentliche Stellen*

Privatrechtliche Organisationen

Firmen (auch Selbstständige)

Vereine

etc.

Alle Vereine sind im „Scope“:

- Eingetragen im Vereinsregister oder nicht
- Gemeinnützig oder nicht
- Nicht rechtsfähige Vereine

(Art. 2 (1) DS-GVO „Sachlicher Anwendungsbereich“)

* = die DS-GVO unterscheidet dies nicht mehr → „Verantwortlicher“

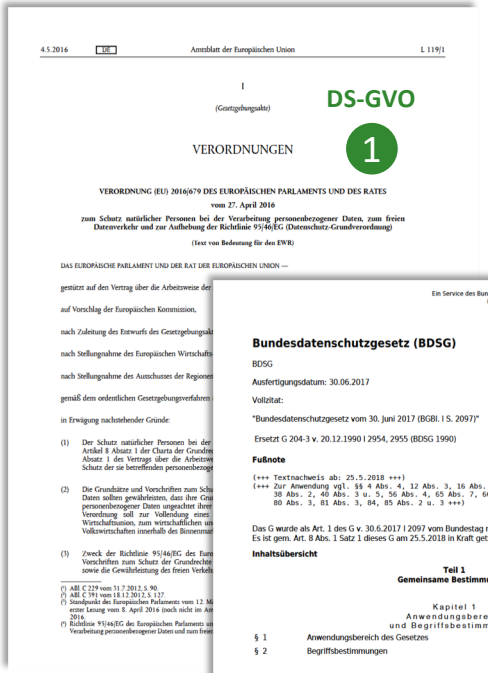
Geltungsbereich der DS-GVO für Vereine / Verbände

- **Sobald personenbezogene Daten verarbeitet werden**
  - ganz oder teilweise automatisiert oder
  - nichtautomatisiert

  die in einem *Dateisystem* gespeichert sind oder gespeichert werden sollen
  (vgl. Art. 2 Abs. 1 DS-GVO „Sachlicher Anwendungsbereich“).

- **Dateisystem**
  - jede strukturierte Sammlung pb Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig ob zentral, dezentral und wie geordnet
    (vgl. Art. 4 Nr. 6 DS-GVO „Begriffsbestimmungen“)

- **Geregelt in**
  - EU Datenschutz-Grundverordnung (DS-GVO)
  - Bundesdatenschutzgesetz (BDSG)


4.5.2016 DE Amtsblatt der Europäischen Union L 119/1

I
(Gesetzgebungsakte)

DS-GVO
1

VERORDNUNGEN

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 27. April 2016
zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakt

nach Stellungnahme des Europäischen Wirtschafts

nach Stellungnahme des Ausschusses der Regionen

gemäß dem ordentlichen Gesetzgebungsverfahren

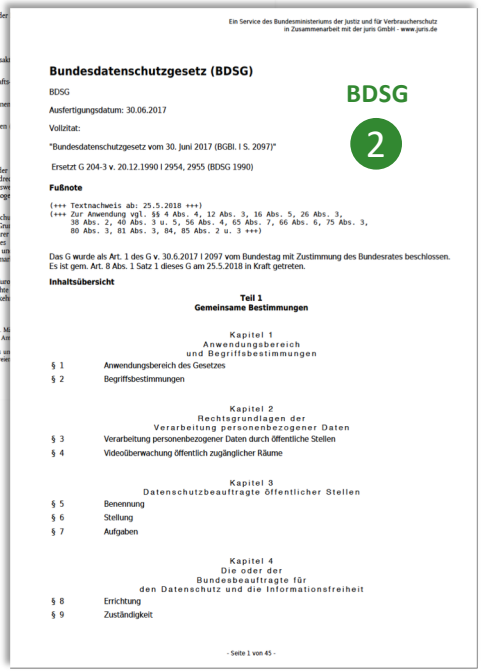
in Erwägung nachstehender Gründe:

(1) Der Schutz natürlicher Personen bei der Artikel 8 Absatz 1 der Charta der Grundrec Absatz 1 des Vertrags über die Arbeitsw Schutz der sie betreffenden personenbezog

(2) Die Grundsätze und Vorschriften zum Sch Daten sollten gewährleisten, dass ihre Gru personenbezogener Daten ungeachtet ihre Verordnung soll zur Vollendung eines Wirtschaftsunion, zum wirtschaftlichen un Volkswirtschaften innerhalb des Binnenmar

(3) Zweck der Richtlinie 95/46/EG des Euro Vorschriften zum Schutz der Grundrechte sowie die Gewährleistung des freien Verkehr

(1) ABl. C 229 vom 31.7.2012, S. 90.
(2) ABl. C 391 vom 18.12.2012, S. 127.
(3) Standpunkt des Europäischen Parlaments vom 12. M erste Lesung vom 8. April 2016 (noch nicht im Au 2016.
(4) Richtlinie 95/46/EG des Europäischen Parlaments un Verarbeitung personenbezogener Daten und zum freie


Ein Service des Bundesministeriums der Justiz und für Verbraucherschutz in Zusammenarbeit mit der juris GmbH - www.juris.de

Bundesdatenschutzgesetz (BDSG)

BDSG

BDSG
2

Ausfertigungsdatum: 30.06.2017

Vollzitat:

"Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097)"

Ersetzt G 204-3 v. 20.12.1990 I 2954, 2955 (BDSG 1990)

Fußnote

(+++ Textnachweis ab: 25.5.2018 +++)
(+++ Zur Anwendung vgl. §§ 4 Abs. 4, 12 Abs. 3, 16 Abs. 5, 26 Abs. 3, 38 Abs. 2, 40 Abs. 3 u. 5, 56 Abs. 4, 65 Abs. 7, 66 Abs. 6, 75 Abs. 3, 80 Abs. 3, 81 Abs. 3, 84, 85 Abs. 2 u. 3 +++)

Das G wurde als Art. 1 des G v. 30.6.2017 I 2097 vom Bundestag mit Zustimmung des Bundesrates beschlossen.
Es ist gem. Art. 8 Abs. 1 Satz 1 dieses G am 25.5.2018 in Kraft getreten.

Inhaltsübersicht

- Seite 1 von 45 -

Was sind „personenbezogene Daten“? – (Definition)

LEGAL-DEFINITION IN § 3 (1) BDSG a.F.

- Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

LEGAL-DEFINITION IN Art. 4 (1) DS-GVO (§ 27 LDSG RP 2018)

- (...) alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

ODER EINFACHER

- Alles womit ein Mensch **identifiziert** werden kann **(→ Personenbezug)**

„STAMMDATEN“ (BSP.)

- **NAME**
- **ADRESSE**
- **E-MAIL-ADRESSE**
- **TELEFONNUMMER**
- **GEBURTSDATUM**

- **PHOTO** (Biometrische Daten)

PLUS „PERSONALDATEN“ (BSP.)

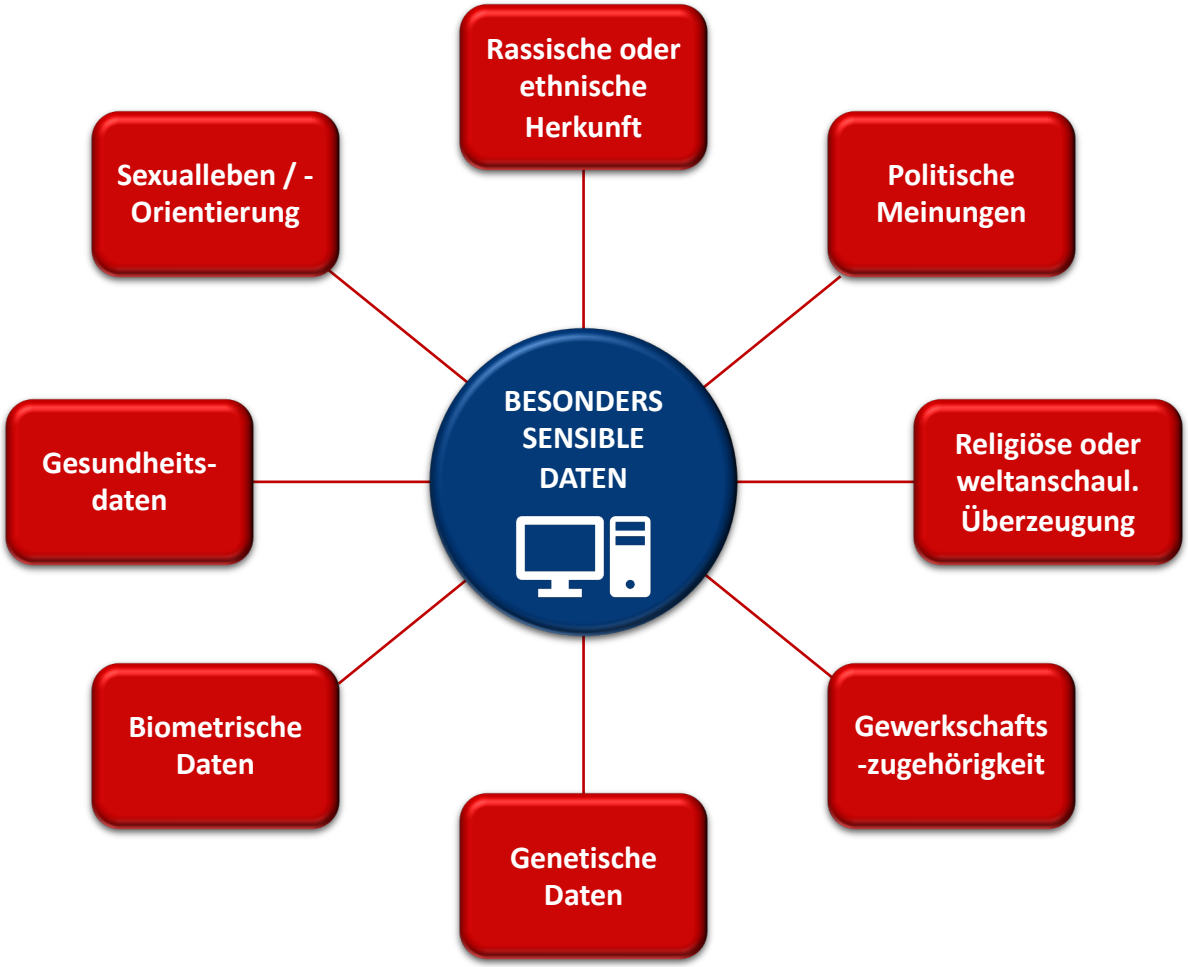
- **MITGLIEDSNUMMER**
- **MITGLIEDSBEITRAG**
- **ZAHLUNGSMORAL**

PLUS „IT – DATEN“ (BSP.)

- **BENUTZERKENNUNG**
- **DATENBANK-ID**
- **MASCHINENBEZOGENE NUTZUNGSZEITEN**

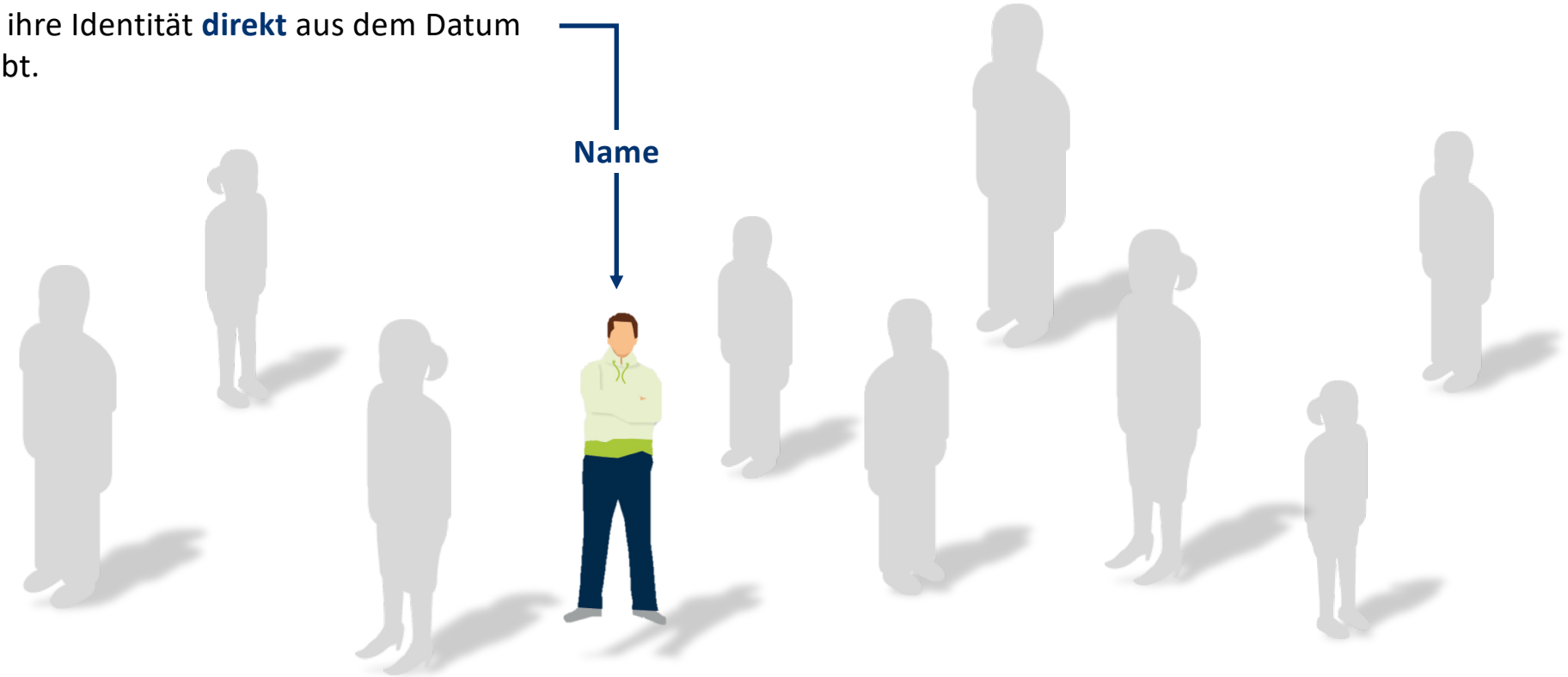
Besondere personenbezogene Daten

- Weitaus strengere Regeln gibt es für den Umgang mit sogenannten **besonderen** Kategorien personenbezogener Daten, da diese besonders schützenswert sind.



Identifizierung (direkte Zuordnung)

IDENTIFIZIERT ist eine Person,
wenn sich ihre Identität **direkt** aus dem Datum selbst ergibt.

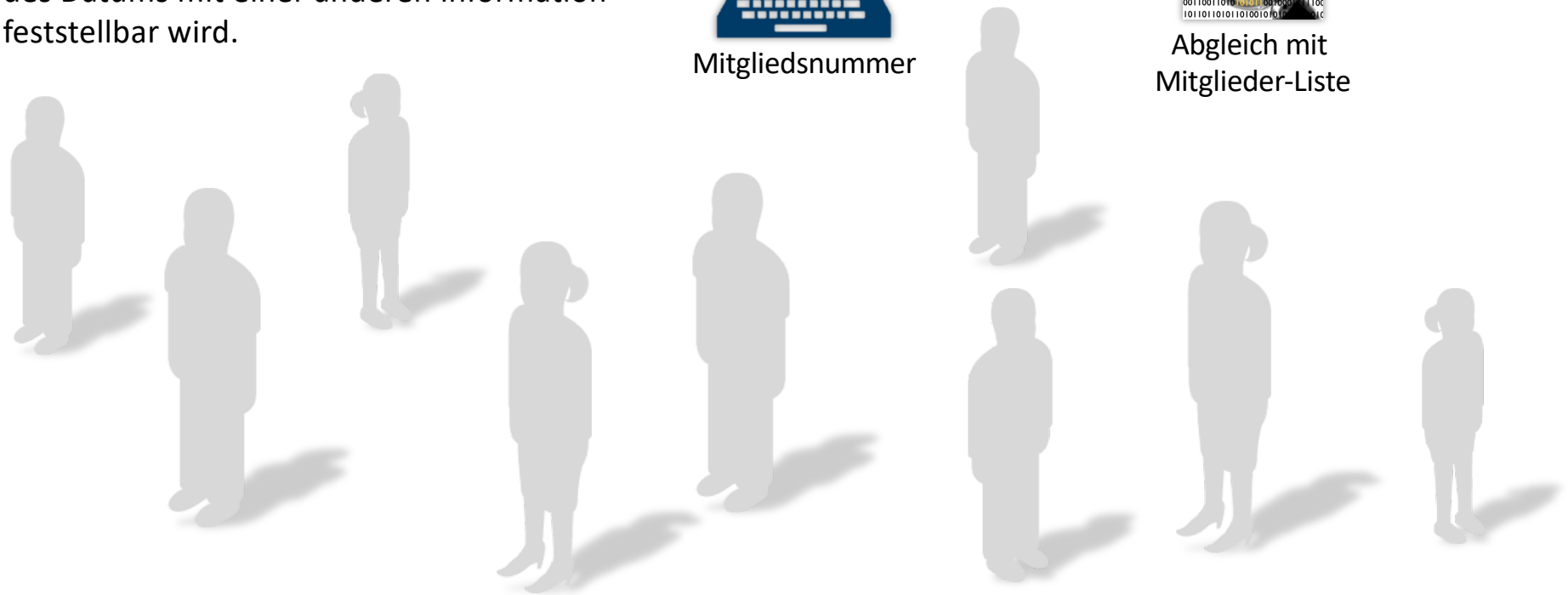


Identifizierung (indirekte Zuordnung)

IDENTIFIZIERBAR wird eine Person,
wenn ihre Identität durch die **Kombination** des Datums mit einer anderen Information feststellbar wird.

Mitgliedsnummer

Abgleich mit
Mitglieder-Liste



FAZIT – Die Information selbst ist entscheidend, nicht das Medium, auf dem sie steht!

Entsorgung

Briefpost

E-Mail

Datenbanken

Notizen

Vertrauliche oder **personenbezogene** Informationen können in / auf **jedem** Medium enthalten sein!

Netzwerk

Drucker

Telefax

Papier-Ablage

ENTSCHLEIERT – Die EU DS-GVO (Datenschutz-Grundverordnung)

→ Unmittelbare innerstaatliche Anwendung ab **25. MAI 2018**

HARMONISIERUNG	Unternehmen in allen EU Mitgliedsstaaten bekommen eine einheitliche Umgebung („Ein Gesetz für alle“)
TRANSPARENZ	EU Bürger erhalten mehr Kontrolle über ihre personen-bezogene Daten, die Betroffenen-Rechte wurden gestärkt.
ZWECKBINDUNG	Personenbezogene Daten dürfen nur in engen gesetzlichen Bahnen für eine rechtmäßige Verarbeitung erhoben werden.
RECHENSCHAFT	**Verantwortliche*** müssen die DS-GVO konforme Verarbeitung sicherstellen und nachweisen. (→ hohe Dokumentationspflichten)

* = natürliche o. juristische Person, (...), die über Zwecke und Mittel d. Verarbeitung entscheidet (→ Art. 4 Nr. 7 DS-GVO)

VERARBEITUNG – nur mit Rechtsgrundlage

- Das **Datenschutzrecht** verbietet grundsätzlich den Umgang mit personenbezogenen Daten, erlaubt diese aber unter bestimmten Voraussetzungen (→ „Verbot mit Erlaubnisvorbehalt“)
- Die **Verarbeitung** ist nur mit einer **Rechtsgrundlage** erlaubt

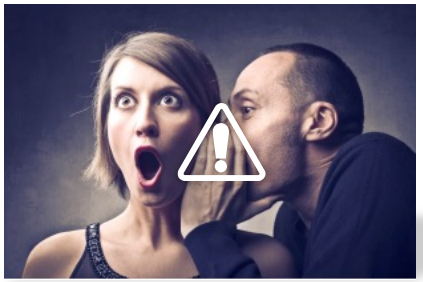
- Durch das Datenschutzrecht selbst (**Erlaubnistatbestand**)
  Beispiel: Zur Durchführung eines **Vertrages** (Mitgliedschaft)

- oder durch eine besondere **Rechtsvorschrift**
  Beispiel: Steuern, Abgaben

- oder durch die **Einwilligung** des Betroffenen ...
  Beispiel: Einverständniserklärung zur Datennutzung

VERARBEITUNG – nur gemäß der Aufgabenstellung

- Der Umgang mit personenbezogenen Daten darf nur zur **Aufgabenerfüllung** (Weisungen des Arbeitgebers / des Vorstandes) erfolgen – insbesondere konkretisiert durch Richtlinien und Arbeitsanweisungen.
- Über die Informationen und personenbezogene Daten ist – auch außerhalb des Arbeitsverhältnisses – **Vertraulichkeit** zu wahren.
- Dies gilt auch und insbesondere für **Social Media**!
- **FAUSTREGEL**
  - **Wofür** will ich pb Daten verarbeiten? (Zweck)
  - **Welche** Rechtsgrundlage habe ich dafür? (Rechtmäßigkeit)



„Goldene Regeln“ des Datenschutzes bleiben weiterhin bestehen

9 GOLDENE REGELN	Rechtsnormen aus BDSG a.F.	Rechtsnormen aus DS-GVO	Rechtsnormen aus BDSG n.F.
1. RECHTMÄSSIGKEIT (§§)	§ 4 BDSG a.F. (Zulässigkeit)	Art. 5 DS-GVO (Grundsätze), Art. 6 DS-GVO (Rechtmäßigkeit)	§§ 3, 4, 23 ff. (div.) BDSG-neu
2. R. EINWILLIGUNG / VERTRAG	§ 4a BDSG a.F. (Einwilligung)		n/a
3. ZWECKBINDUNG	u.a. §§ 4, 14, 28, 31 BDSG a.F.	u.a. Artt. 6, 7, 9 DS-GVO	s.o. bzw. n/a bzw. 22, 24, 26, 28 BDSG-neu
4. DATENSPARSAMKEIT	§ 3a BDSG a.F.	Art. 5 DS-GVO	n/a
5. TRANSPARENZ	§§ 6, 34 (Auskunft) BDSG a.F.	u.a. Artt. 12, 15 DS-GVO	u.a. § 27 ff. BDSG-neu
6. DATENSICHERHEIT IT	§§ 5, 9, BDSG a.F.	Artt. 5 (1) lit. f, 24, 25, 32, 35, 36	n/a (außer Teil 4, Justiz + Polizei)
7. KONTROLLE IT	§§ 5, 9, 11 BDSG a.F.	Artt. 5 (1) lit. f, 24, 25, 28, ff. 32, 35 ff.	n/a (außer Teil 4, Justiz + Polizei)
8. DOKUMENTATION	§§ 4d ff., 9 (Anlage), 11 BDSG a.F.	u.a. Art. 5 (2), 24 (Accountability), 28	n/a
9. (DSB-BESTELLPFLICHT)	§ 4f (2) BDSG a.F.	Art. 37 ff. DS-GVO	§§ 5, 38 BDSG-neu (öffentliche / nicht-öffentliche Stellen)

→ **Keine Änderungen an den Grundprinzipien des Datenschutzes!**

Die 7 wichtigsten Aspekte der DS-GVO im Überblick

Rechtsgrundlage

- *Klassisch: Vertrag, Gesetz, Einwilligungserklärung (EWE) zur Verarbeitung etc.*

Betroffenen-Rechte

- *Transparenz, Pro-aktive Benachrichtigung, Auskunft, Berichtigung, Löschung, Sperrung, Portabilität (neu), Widerspruch*
- *Unabdingbar, keine Einschränkung zulässig*

Nachweis + Dokumentation

- *Jede noch so kleine oder kurze Doku ist besser, als gar keine.*
- *Es muss der Nachweis geführt werden können, dass die DS-GVO umgesetzt wurde.*

IT-Sicherheit

- *Nicht nur gesetzlich verlangt, auch in eigener Sache nützlich.*
- ***TIPP:** für die Herangehensweise § 64 BDSG heranziehen – da steht das Wichtigste drin.*

Regelmäßig unter Ihrer Kontrolle

Outsourcing (Auftragsverarbeitung)

- *Die Arbeit kann delegiert werden – die Verantwortung jedoch nicht!*
- *Sorgen Sie für belastbare und professionelle Vertragsgrundlagen (AV-V).*

„Beschäftigten"-Datenschutz

- *Das bisherige Recht gilt im Wesentlichen weiter.*
- *Die Rechtsprechung bleibt erhalten.*

Haftung und Bußgelder

- *Schadensersatz + persönliche Haftung*
- *Bei DS-GVO Verstößen:*
  - *EUR **10.000.000** oder 2% d. Vorjahresumsatzes (höhere Zahl entscheidet)*
- *Bei DS-GVO Verstößen in bestimmten Fällen:*
  - *EUR **20.000.000** oder 4% des Vorjahresumsatzes (höhere Zahl entscheidet)*

Betroffenen-Rechte sind stets zu wahren (ansonsten wird es teuer)

ARTIKEL 12 DS-GVO

(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in ***präziser***, ***transparenter***, ***verständlicher*** *und* ***leicht zugänglicher*** *Form in einer* ***klaren*** *und* ***einfachen Sprache*** *zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten.*

Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch.

Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

Regelmäßig *nicht* unter Ihrer Kontrolle

Kenntnis der eigenen Verfahren

- *Belastbare Dokumentation (→ „Verzeichnis der Verarbeitungstätigkeiten“, vorm. „Verfahrensbeschreibungen“).*
- *Nur so können die Betroffenen-Rechte gefahrlos gewährt werden*

Kenntnis der Verfahrensweise

- *Bei der 1. Anfrage sicherheitshalber eine fachkundige Person fragen – danach selber umsetzen.*
- *Fristen und Formen beachten.*

NIEMALS IGNORIEREN!

VERSCHÄRFTE WAHRNEHMUNG – Transparenzpflichten + Betroffenen-Rechte

(§ 28 (4) BDSG a.F.)

WIDERSPRUCH
Unter bestimmten Umständen kann der Verarbeitung widersprochen werden. (Art. 21 DS-GVO)

INFORMATIONSPFLICHTEN
Bei oder vor der Datenerhebung muss die Organisation die betroffene Person über die Verarbeitung und alle ihre Rechte Informieren.
(Artt. 13, 14 DS-GVO)

DATENEXPORT
Auf Antrag sind pb Daten unter bestimmten Umständen elektronisch zur Verfügung zu stellen (Art. 20 DS-GVO).

„VERGESSENWERDEN“
Auf Antrag sind veröffentlichte pb Daten zu löschen (z.B. Web).
(Art. 17 (2) DS-GVO).

AUSKUNFT („aufgebohrt“)
Auf Antrag über die gespeicherten Daten, Quelle, Empfänger etc.
(Art. 15 DS-GVO)

(§ 34 BDSG a.F.)

BERICHTIGUNG
Unkorrekte pb Daten müssen stets berichtigt werden.
(Art. 16 DS-GVO)

LÖSCHUNG
Pb Daten sind auf Antrag unter best. Umständen zu löschen (Art. 17 (1) DS-GVO).

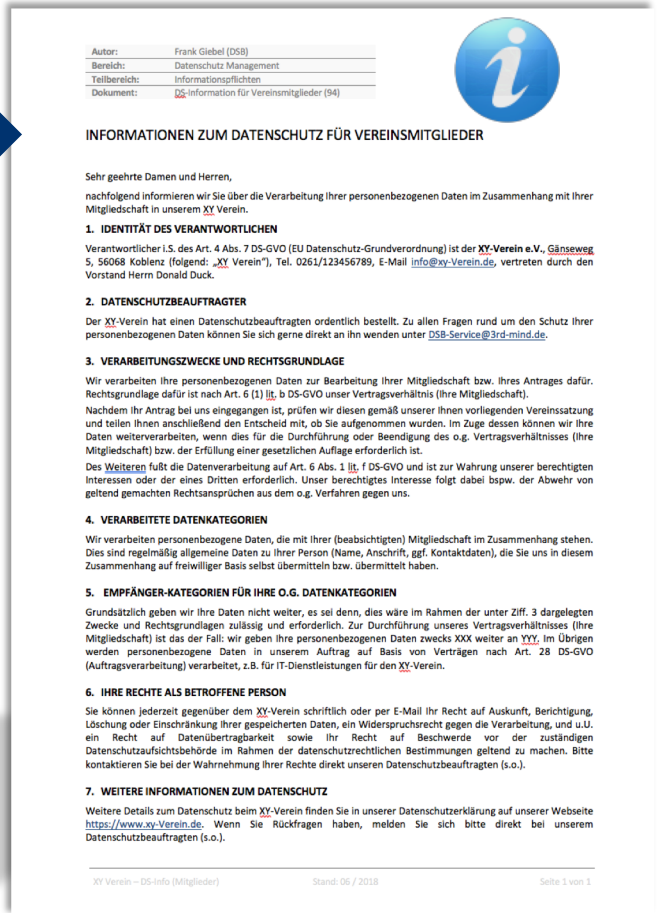
EINSCHRÄNKUNG (SPERRUNG)
Auf Antrag sind pb Daten unter bestimmten Umständen zu sperren (Art. 18 DS-GVO).

(§ 35 BDSG a.F.)

(Benachrichtigung aller Empfänger n. Art. 19 DS-GVO)

INFORMATIONSPFLICHTEN – (nicht nur) für Vereine

ART. 13 Abs. 1 DS-GVO	**„1st-Level-Infomationen (unmittelbar)**
Identität d. Verantwortlichen	Verein + Anschrift + Vorstand etc.
ggf. Kontaktdaten der / des DSB	Sofern Bestellpflicht n. § 38 BDSG besteht
Zwecke + Rechtsgrundlage d. Verarbeitung	Betroffenen-Rechte im Datenschutz
ggf. „Berechtigte Interessen“	schwierig, nur bei Bedarf (Prüfung!)
Empfängerkategorien	Sofern die Daten nach extern weitergehen
ggf. Absicht der Weitergabe in Drittländer	Weitergabe nach außerhalb der EU
	Rest (Abs.) auf Anforderung oder Web (s.u.)
ART. 13 Abs. 2 DS-GVO	**„2nd-Level-Infomationen (mittelbar)**
	→ Datenschutz-Erklärung auf Webseite



Autor:	Frank Giebel (DSB)
Bereich:	Datenschutz Management
Teilbereich:	Informationspflichten
Dokument:	DS-Information für Vereinsmitglieder (94)

INFORMATIONEN ZUM DATENSCHUTZ FÜR VEREINSMITGLIEDER

Sehr geehrte Damen und Herren,

nachfolgend informieren wir Sie über die Verarbeitung Ihrer personenbezogenen Daten im Zusammenhang mit Ihrer Mitgliedschaft in unserem XY Verein.

1. IDENTITÄT DES VERANTWORTLICHEN

Verantwortlicher i.S. des Art. 4 Abs. 7 DS-GVO (EU Datenschutz-Grundverordnung) ist der **XY-Verein e.V.**, Gänseweg 5, 56068 Koblenz (folgend: „XY Verein“), Tel. 0261/123456789, E-Mail info@xy-Verein.de, vertreten durch den Vorstand Herrn Donald Duck.

2. DATENSCHUTZBEAUFTRAGTER

Der XY-Verein hat einen Datenschutzbeauftragten ordentlich bestellt. Zu allen Fragen rund um den Schutz Ihrer personenbezogenen Daten können Sie sich gerne direkt an ihn wenden unter DSB-Service@3rd-mind.de.

3. VERARBEITUNGSZWECKE UND RECHTSGRUNDLAGE

Wir verarbeiten Ihre personenbezogenen Daten zur Bearbeitung Ihrer Mitgliedschaft bzw. Ihres Antrages dafür. Rechtsgrundlage dafür ist nach Art. 6 (1) lit. b DS-GVO unser Vertragsverhältnis (Ihre Mitgliedschaft).

Nachdem Ihr Antrag bei uns eingegangen ist, prüfen wir diesen gemäß unserer Ihnen vorliegenden Vereinssatzung und teilen Ihnen anschließend den Entscheid mit, ob Sie aufgenommen wurden. Im Zuge dessen können wir Ihre Daten weiterverarbeiten, wenn dies für die Durchführung oder Beendigung des o.g. Vertragsverhältnisses (Ihre Mitgliedschaft) bzw. der Erfüllung einer gesetzlichen Auflage erforderlich ist.

Des Weiteren fußt die Datenverarbeitung auf Art. 6 Abs. 1 lit. f DS-GVO und ist zur Wahrung unserer berechtigten Interessen oder der eines Dritten erforderlich. Unser berechtigtes Interesse folgt dabei bspw. der Abwehr von geltend gemachten Rechtsansprüchen aus dem o.g. Verfahren gegen uns.

4. VERARBEITETE DATENKATEGORIEN

Wir verarbeiten personenbezogene Daten, die mit Ihrer (beabsichtigten) Mitgliedschaft im Zusammenhang stehen. Dies sind regelmäßig allgemeine Daten zu Ihrer Person (Name, Anschrift, ggf. Kontaktdaten), die Sie uns in diesem Zusammenhang auf freiwilliger Basis selbst übermitteln bzw. übermittelt haben.

5. EMPFÄNGER-KATEGORIEN FÜR IHRE O.G. DATENKATEGORIEN

Grundsätzlich geben wir Ihre Daten nicht weiter, es sei denn, dies wäre im Rahmen der unter Ziff. 3 dargelegten Zwecke und Rechtsgrundlagen zulässig und erforderlich. Zur Durchführung unseres Vertragsverhältnisses (Ihre Mitgliedschaft) ist das der Fall: wir geben Ihre personenbezogenen Daten zwecks XXX weiter an YYY. Im Übrigen werden personenbezogene Daten in unserem Auftrag auf Basis von Verträgen nach Art. 28 DS-GVO (Auftragsverarbeitung) verarbeitet, z.B. für IT-Dienstleistungen für den XY-Verein.

6. IHRE RECHTE ALS BETROFFENE PERSON

Sie können jederzeit gegenüber dem XY-Verein schriftlich oder per E-Mail Ihr Recht auf Auskunft, Berichtigung, Löschung oder Einschränkung Ihrer gespeicherten Daten, ein Widerspruchsrecht gegen die Verarbeitung, und u.U. ein Recht auf Datenübertragbarkeit sowie Ihr Recht auf Beschwerde vor der zuständigen Datenschutzaufsichtsbehörde im Rahmen der datenschutzrechtlichen Bestimmungen geltend zu machen. Bitte kontaktieren Sie bei der Wahrnehmung Ihrer Rechte direkt unseren Datenschutzbeauftragten (s.o.).

7. WEITERE INFORMATIONEN ZUM DATENSCHUTZ

Weitere Details zum Datenschutz beim XY-Verein finden Sie in unserer Datenschutzerklärung auf unserer Webseite https://www.xy-Verein.de. Wenn Sie Rückfragen haben, melden Sie sich bitte direkt bei unserem Datenschutzbeauftragten (s.o.).

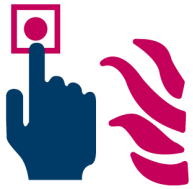
XY Verein – DS-Info (Mitglieder) Stand: 06 / 2018 Seite 1 von 1

SCHADENSBEGRENZUNG – Datenpannen sind meist ungewollt, aber leider sehr real

DATENPANNEN

- Vernichtung
- Verlust
- Veränderung
- „Unfreundlicher Informationsabfluss“

UNVERZÜGLICHE MELDUNG



Je nach Risiko für die Rechte und Freiheiten der Betroffenen

- **keine Meldepflicht**
- **Unverzügliche Meldung an Betroffene**
- **Meldung an Aufsichtsbehörden innerhalb von 72 Stunden**

Für den Verein:

- Vorstand / GF
- ggf. Datenschutz-beauftragte(r)

ANGSTMACHER – Mögliche Sanktionen bei Datenschutz-Verstößen

RECHTSWEGE

- Beschwerde bei **Aufsichtsbehörde**
- **Gerichtsverfahren** gegen Aufsichtsbehörde
- **Gerichtsverfahren** gegen Verantwortlichen / Auftragsverarbeiter

VERTRETUNG

- Vertretung des Betroffenen durch einen Verband
- Verbandsklagerecht
- UKlaG
- „Abmahn-Industrie“

SANKTIONEN

- **Schadensersatz**
- **Persönliche Haftung**
- **(Bußgeld** bis EUR 20.000.000 oder 4% des weltweiten Jahresumsatzes, je nach dem welcher Betrag höher ist)
- **Haftstrafen bis zu 3 Jahren**

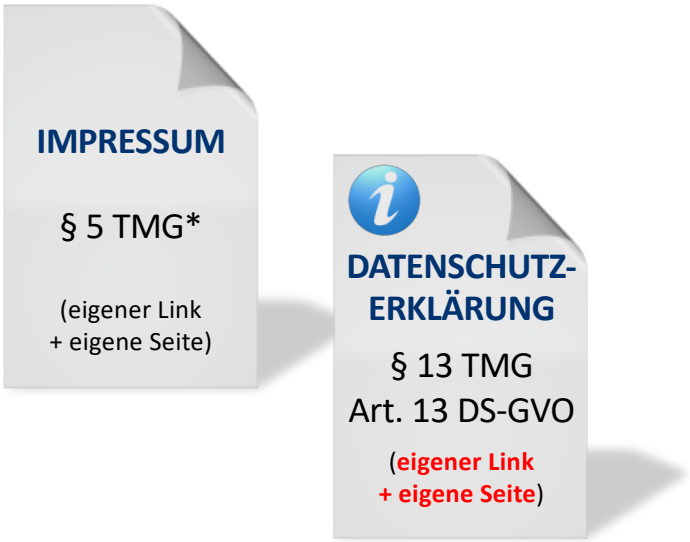
NEGATIV-PRESSE

- **Ungewollte Interviews**
- **Negativ-Schlagzeilen a la „Datenskandal beim XY-Verein“**
- **Negativ-PR / Social Media (!)**
- **Das Internet “vergiss nichts“**

SCHRITT 1: Alle Online-Auftritte DS-GVO-konform ausgestalten!

DIGITALISIERUNG – Was ist „online“ zu beachten?

- **IMPRESSUM**
  - aktualisieren, keine Rechtsnormen, nur Angaben machen
- **DATENSCHUTZERKLÄRUNG**
  - Bisherige Angaben + zusätzlich Tools, Social-Media etc.
  - „Web-Generatoren“ ggü. kritisch sein!
- **HTTPS** bei Web-Formularen
  - Zusätzlich zu § 13 (7) TMG nun Artt. 32 (1) lit. a i.V. mit 5 (1) lit. f DS-GVO
- **NEWSLETTER** (-Formular)
  - Nur 1 Pflichtfeld: @-Adresse (vgl. 2. Corrigendum, Art. 25 DS-GVO)
  - 2-Zeiler mit Verweis auf DS-Erklärung, ggf. verpflichtende Checkbox
  - Double-Opt-In wegen Beweiskraft
- **SOCIAL MEDIA** (Facebook & Co.)
  - Keine pb Daten über Social Media verarbeiten (vgl. EuGH-Urteil v. 05.06.2018)
  - Empfehlung: Verweis auf Webseite (Anmeldungen etc.)



* TMG = Telemediengesetz idF v. 28.09.2017

DIGITALISIERUNG – Update „Facebook-Fanpages“ / Tracking pb Daten („Insights“)

- **EuGH Urteil v. 05.06.2018**
  - „Gemeinsame Verantwortung“ für Facebook + Seitenbetreiber
  - Mögliches Haftungsrisiko für Datenschutz-Verstöße durch Facebook
- **DSK[1] Entscheidung v. 05.09.2018**
  - DSK[1]: „Fanpages sind illegal“
  - Facebook in der Pflicht → Betreiber??
- **Reaktion von Facebook am 11.09.2018**
  - „Page Controller Addendum“ im Administrationsbereich
  - Automatische Annahme bei Weiterbetrieb der Seite
- **ToDo für „risikofreudige“ Seitenbetreiber**
  - Datenschutzerklärung „Facebook“ anpassen (nicht mit Web-Erklärung vermischen!)
  - Auf Fanpage veröffentlichen oder auf sep. Unterseite im Web verlinken
  - Urteil des BVerwG abwarten, Aufsichtsbehörden – Meldung beobachten

[1] DSK = Datenschutzkonferenz, Gremium aller dt. Aufsichtsbehörden

JUNGER LANDKREIS MIT TRADITION

VERARBEITUNG – Datenschutz im Vereinsleben

- **FOTO / VIDEO** bei Vereinsfesten + Veranstaltungen
  - EWE einholen und / oder Hinweisschilder
  - „Recht auf Vergessenwerden“ und Widerrufs-Konsequenzen beachten
- **MITGLIEDERVERWALTUNG**
  - Analog Personalstelle im Betrieb (Mitgliedschaftsvertrag / Satzung / Zwecke)
  - Inhaltskontrolle aus § 307 BGB (Bestimmungen) beachten
- **AUFTRAGSVERARBEITUNG**
  - Dienstleisterverträge (IT, Werbung etc.) / „AV-V“ prüfen oder erstellen
- **E-MAIL-VERSCHLÜSSELUNG**
  - Keine Standards / „feste Stellen“ (SteBe) z.B. mit „Datev-Dongle“
  - Office + pdf-Dateien mit Kennwort schützen + per Telefon mitteilen
- **DSB-BESTELLPFLICHT**
  - Sobald die Vereinsorgane 10 Personen umfassen (§ 38 BDSG)
- **DOKUMENTATION** (DS-Handbuch)

TIPP

Der Landesbeauftragte für den DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz

Datenschutz im Verein

unter Berücksichtigung der Datenschutz-Grundverordnung

Die 10 wichtigsten Hinweise
für Vereinsvorstände und andere Personen,
die im Verein mit datenschutzrechtlichen
Belangen befasst sind

https://www.datenschutz.rlp.de/de/themenfelder-themen/vereine/

Stand: 03.05.2018

Herausgeber
Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit Rheinland-Pfalz
Hintere Bleiche 34
55116 Mainz

www.datenschutz.rlp.de
poststelle@datenschutz.rlp.de
Telefon: +49 (0) 6131 208-2449
Telefax: +49 (0) 6131 208-2497

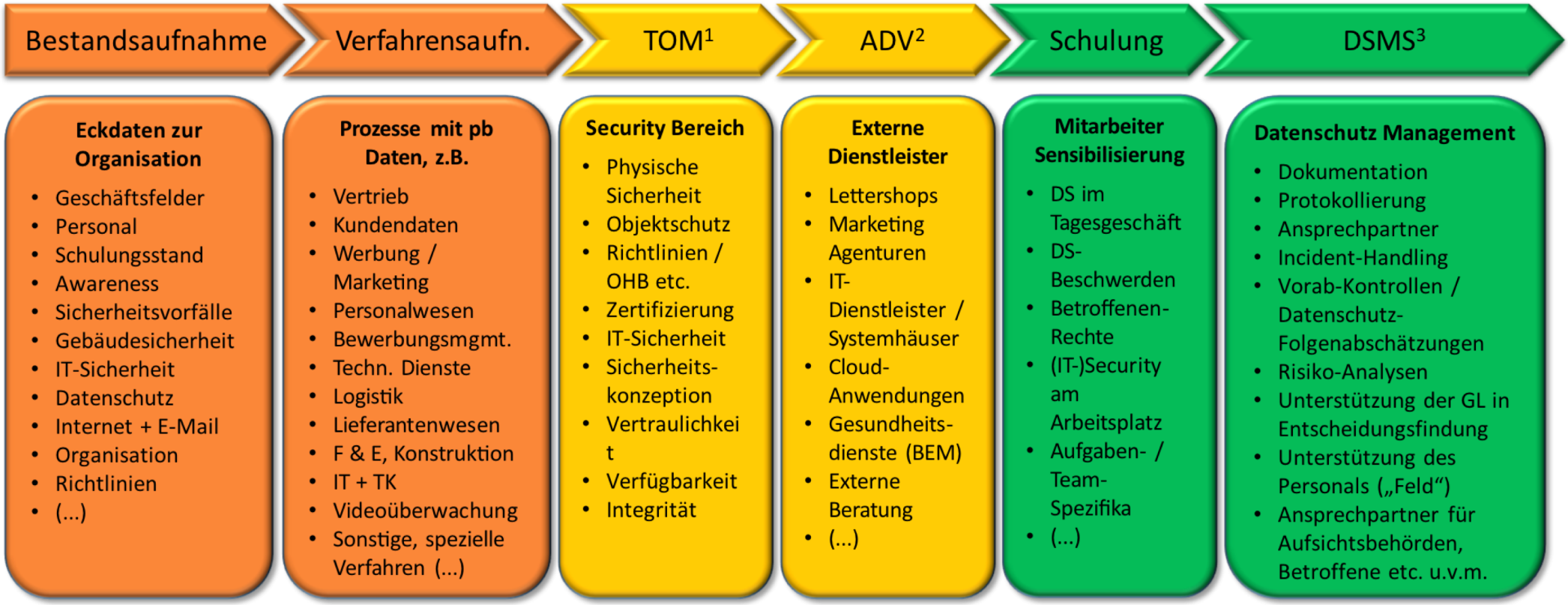
FÜHRUNGSEBENE – Schaffen der Voraussetzungen + Sensibilisierung + „Controlling“

VEREINSFÜHRUNG
stellt sicher, dass ...

- Eine **Rechtsgrundlage** für die Verarbeitung ist vorhanden und der rechtskonforme Verarbeitungsprozess ist dokumentiert (→ Verz. f. Verarbeitungstätigkeiten, VVT).
- Die Verarbeitung wird / wurde auf besondere **Risiken** für die Betroffenen hin untersucht und im Hinblick auf die Minimierung dieser Risiken gestaltet (→ TOM, ggf. Datenschutz-Folgenabschätzung).
- Die Verarbeitung kann den Betroffenen gegenüber **transparent** dargestellt werden (→ Dokumentation, VVT).
- Die **Daten-Nutzungsdauer** ist bestimmt und Aufbewahrungs- sowie Löschkonzepte (inkl. Papier- und Datenträger-Entsorgung) werden eingehalten (→ Dokumentation, VVT, MA-Sensibilisierung, TOMs).
- Bei der Einbindung von **Dienstleistern** werden diese sorgfältig ausgewählt, vertraglich gebunden und kontrolliert (→ Auftragsverarbeitung).
- Bei der Einführung / Änderung einer Verarbeitung wird die/der **DSB** stets einbezogen (→ Unterstützung, Wiederholung d. Punkte 1-5).

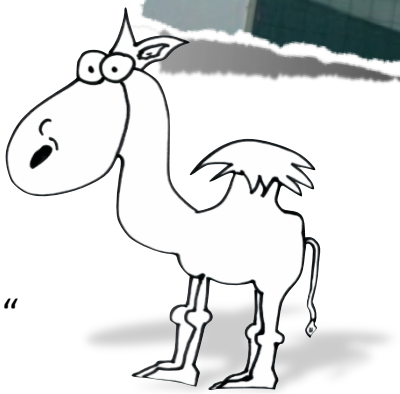
DATENSCHUTZBEAUFTRAGTE(R)
unterstützt und berät

UMSETZUNG – Bestandteile eines Datenschutz-Management-Systems (Auszüge)



Das Letzte

- **Ein DS / IS Konzept ist NIE fertig**
  - Bedrohungen entwickeln sich weiter
- **Richtlinien + Rechtsnormen sind wichtig**
  - Aber manchmal nicht so ganz eindeutig
- **Technologie ist nützlich**
  - Aber nicht immer zuverlässig
- **Vertrauen ist gut**
  - Aber (Selbst-)Kontrolle ist besser
- **Ein arabisches Sprichwort sagt ...**
  - „... vertraue auf Allah - aber binde Dein Kamel (trotzdem) an“



3rd Mind Business Consulting

Projektmanagement • Audit • Beratung • Training
IT-Compliance • Informationssicherheit • Datenschutz

„Nicht alles, was technisch machbar, ist auch juristisch erlaubt bzw. betriebswirtschaftlich sinnvoll“.

Kreisverwaltung Mayen-Koblenz (KV MYK) • DS-GVO für Vereine • 24.10.2018

Datenschutz im Lichte der **EU DS-GVO**

JUNGER LANDKREIS
MIT TRADITION

in Kooperation mit

3rd Mind
Business Consulting
IT • COMPLIANCE • DATENSCHUTZ

© 2009 - 2018 3rd Mind Business Consulting GmbH • 65760 Eschborn / Ts. • www.3rd-mind.de • frank.giebel@3rd-mind.de • Tel.: +49 (0) 6173 322 527 Fax: +49 (0) 6173 322 528