bvve
Bundesverband der Vereine
und des Ehrenamtes e.V.

DSGVO | Das ungeliebte Thema in Verein und Ehrenamt

Workshop Kompetent im Ehrenamt | Studienstiftung des deutschen Volkes Bonn e.V.

03. Bis 05. Mai 2019 Köln

Fit-im-Ehrenamt.de
Eine Initiative im Bundesverband
der Vereine und des Ehrenamtes e.V.

CAROLINE SCHWARZ

Bildungsmanagerin und Betriebswirtin (IWW)
Vize-Präsident – Bildung des bvve e.V.

Themenfelder

- Prozessbegleitung, Struktur- und Organisationsentwicklung
- Kommunikation & Kooperation; Konfliktklärung und Mediation

Projektbeispiele

- Konzeption und Durchführung von Seminaren und Bildungsprojekten
- Begleitung von Führungskräften aus unterschiedlichen Bereichen (Unternehmen/Schule/soziale Einrichtungen/Gemeinden)
- Begleitung von Veränderungsprozessen in Non-Profit-Organisationen – Schwerpunkt: Führung
- Freiwilligenmanagement
- Nachfolgemanagement
- Datenschutz als Chance zur Neustrukturierung
- Teamentwicklung und Supervision sozialer Einrichtungen
- Leitbild- und Teamentwicklung insbesondere in Non-Profit-Organisationen
- Dozententätigkeit an der Steinbeis Hochschule Berlin, der DHBW Stuttgart sowie Lehrauftrag an der PH Ludwigsburg

HANS-JÜRGEN SCHWARZ

Hans-Jürgen Schwarz

Betriebswirt, Datenschutzbeauftragter (IHK)
Initiator und Präsident des bvve e.V.

Kompetenzen

- Unternehmer mit über 30-jähriger Erfahrung im IT-Bereich
- Schwerpunkte: IT-Systeme und ERP-Softwareentwicklung,
- Gründungs- und Vorstandsmitglied verschiedener Vereine
- 2013 Initiator und Gründer des
  Bundesverbandes der Vereine und des Ehrenamtes e.V. | bvve
- Geschäftsführungsverantwortlicher für die Bereiche Datenschutz
  in der **GADE GmbH Gesellschaft für angewandten Datenschutz in Europa**

Schwerpunktthemen seit 2016

- Europäische Datenschutzgrundverordnung im praktischen Einsatz
- Beratung für Datenschutz in Non-Profit-Organisation – NPO und KMU
- Konzeptionen zu betrieblichen Datenschutzprozessen
- Externer Datenschutzbeauftragter für verschieden Organisationen
- Datenschutzexperte in der GADE mbH –
  Gesellschaft für angewandten Datenschutz in Europa mbH

Vorträge und Workshops zur DSGVO

- im Bundesverband der Vereine und des Ehrenamtes e.V. | bvve
- für Fach- und Dachverbände, Unternehmen und Organisationen
- Dozent für Bildungseinrichtungen und -träger
- Keynotes bei Foren, Symposien, Messen

GADE
Gesellschaft für angewandten
Datenschutz in Europa

bvve
Bundesverband der Vereine und des Ehrenamtes e.V.

SPORT | KUNST | KULTUR | FREIZEIT | SOZIALES

Der Bundesverband der Vereine und des Ehrenamtes e.V. | bvve engagiert sich **spartenübergreifend für Vereine und die ehrenamtlich Engagierten.**

Der bvve fördert und unterstützt damit das größte und älteste soziale Netzwerk – **die Vereine.**

Fünf Bereiche für die Vereine …

Fit-im-Ehrenamt.de
Eine Initiative im Bundesverband der Vereine und des Ehrenamtes e.V.

- **Akademie** | für Bildung und Wissen
- **Benefits** | Rahmenvereinbarungen für Vergünstigungen und Vorteile der Ehrenamtlichen
- **Community** | Austausch und Vernetzung der Vereine
- **Lobby** | als Sprachrohr in Politik und Wirtschaft
- **News** | Berichterstattung und Neues aus wichtigen Themenbereichen für die Vereine

3 SCHRITTE ZUM DATENSCHUTZKONFORMEN VEREIN

Einheitliches Konzept und Handlungsleitfaden für Vereine und Ehrenamt!

IMPULS-VORTRAG

Was die neue Datenschutzgrundverordnung von Vereinen verlangt

GRUNDLAGEN

- DSGVO und BDSG – die gesetzlichen Verpflichtungen
- in Verein, Verband und Non-Profit-Organisationen

Fit-im-Ehrenamt.de
Eine Initiative im Bundesverband der Vereine und des Ehrenamtes e.V.

TAGESSEMINAR

Das Aktiv-Tagesseminar zur Einführung der DSGVO

EINFÜHRUNG

- Das Aktiv-Tagesseminar zur Einführung der DSGVO
- Ermittlung des Soll-Ist Zustandes im Verein
- Erstellung des Fahrplans zur Einführung der DSGVO
- Umfangreiche Checklisten und Muster
- TOM – Technisch Organisatorische Maßnahmen
- Verfahrensverzeichnisse

WORKSHOPS

zur Umsetzung und Anwendung der DSGVO

UMSETZUNG, AUSBILDUNG UND WEITERBILDUNGEN

- Datenschutzkoordinator
- Datenschutzbeauftragter für Vereine | DSBIV
- Ausbildung zum betrieblichen Datenschutzkoordinator u. -beauftragten
- Verpflichtung und Schulung zur Datengeheimnisverpflichtung
- Datenschutz-Managementsystem

Sicherheit und Datenschutz in Verein • Verband • Organisationen | bvve e.V.
bvve
Bundesverband der Vereine und des Ehrenamtes e.V.

DAS SIND WIR – DIE VEREINE IN DEUTSCHLAND

620.000 Vereine in Deutschland – 50 Millionen Mitglieder

27,2 Millionen Mitglieder in Sportvereinen (DOSB)

22,8 Millionen Mitglieder in Kultur, Freizeit, Sozialem …

Fakten Zivilgesellschaft – Verein [1)]

- 620.000 Vereine mit über 50 Millionen Mitgliedern in Deutschland
- Bruttowertschöpfung 4,1 % des Bruttoinlandsproduktes (90 Mrd. Euro) [1)]
- 2,3 Millionen sozialversicherungspflichtige Arbeitsplätze [1)]
- 300.000 in 450-Euro-Jobs Tätige [1)]

Ehrenamtliches Engagement

- Im Regelfall werden über 90 % der Veranstaltungen in Städten und Kommunen durch die Vereine und Ehrenamtlichen initiiert und abgedeckt.
- **20 bis 30 Millionen Menschen engagieren** sich in Vereinen und im Ehrenamt in Deutschland.
- Der Wert der Leistung ihres Engagements liegt bei rund **40 Mrd. Euro pro Jahr**.

1) Fakten aus FAZ erstellt im Auftrag der Stiftungen Bertelsmann und Thyssen. Studie aus 2013

VEREINE | GELDWERT

*) 178 h pro ehrenamtlich Aktiver per anno – ergibt bei einem Stundenlohn von 9,- Euro einen Gesamtwert von ca. 40 Mrd. Euro p.a.

**) 40.000.000 dividiert durch 620.000 Vereine = 64.516 Euro,- / Verein

DER 25.MAI 2018 | DIE HERAUSFORDERUNG

DER ÜBERBLICK DER TAGE

DIE HERAUSFORDERUNG

Informationspflichten
bei Veröffentlichungen und Ergebnisdiensten

RECHT AM BILD - EINE DER GRÖßTEN HERAUSFORDERUNGEN

DIE HERAUSFORDERUNG

Informationspflichten, Einwilligungen und Widerrufe

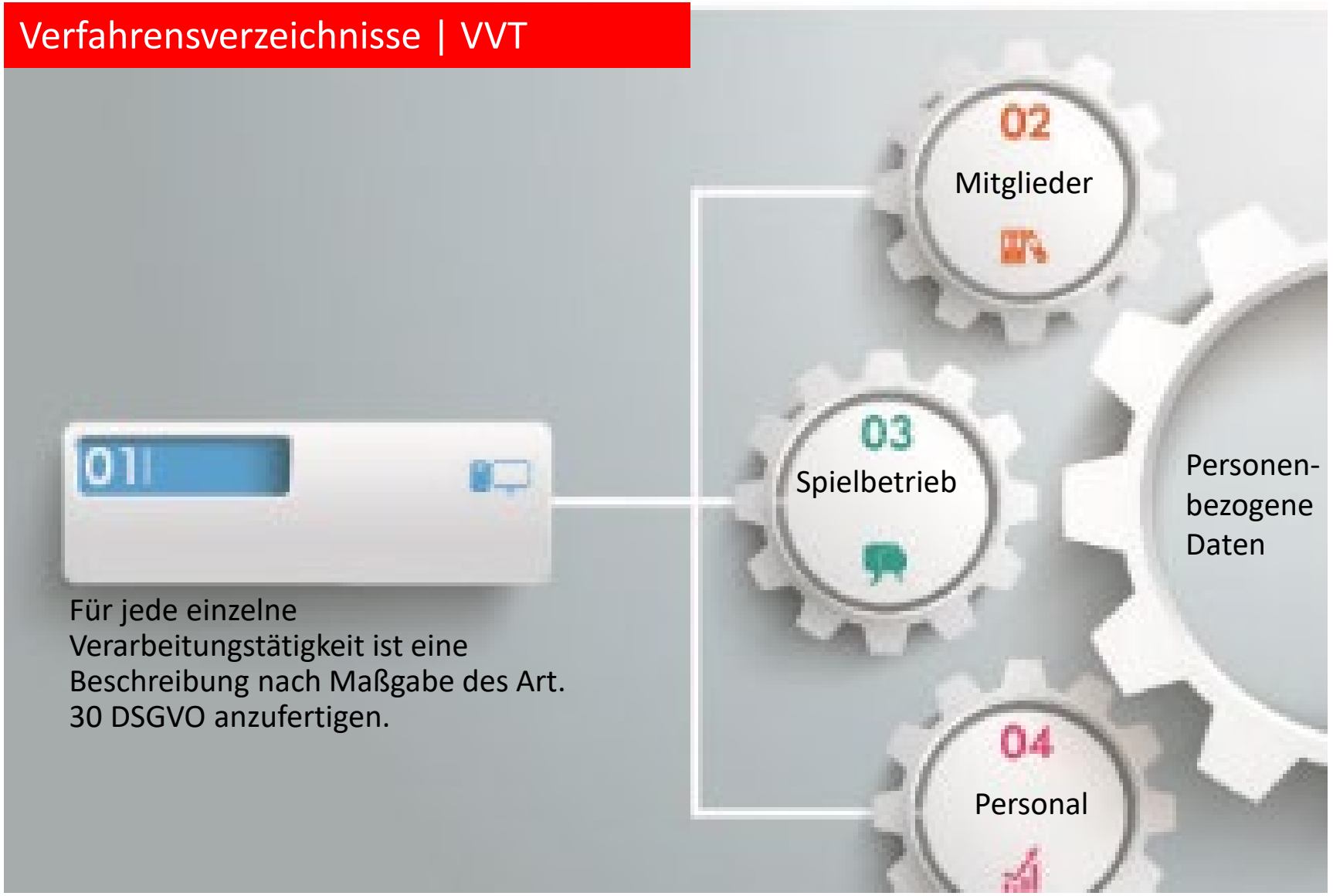
SOZIALE MEDIEN – DATENSCHUTZKONFORME NUTZUNG

UNTERRICHTUNG DER BESCHÄFTIGTEN

Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DSGVO

VERFAHRENSVERZEICHNISSE

Verfahrensverzeichnisse | VVT



Für jede einzelne Verarbeitungstätigkeit ist eine Beschreibung nach Maßgabe des Art. 30 DSGVO anzufertigen.

AUFTRAGSVERARBEITUNG | AV ART. 28 DSGVO

Ein Unternehmen / Verein (Auftraggeber) beauftragt externe Dienstleister (Auftragnehmer) weisungsgebunden personenbezogene Daten zu verarbeiten.

IT-SICHERHEITSKONZEPT

IT-Sicherheitskonzepte |
BackUp-Konzept für Verfügbarkeit

TECHNISCH ORGANISATORISCHE MAßNAHMEN – TOM

Technisch Organisatorische Maßnahmen – TOM

- Berechtigungskonzepte
- Beachtung des Trennungsgebots in der Verarbeitung/Datenminimierung
- Löschkonzepte
- Auskunftskonzept
- Kontrollkonzept
- Datenpannen Meldekonzept
- Backup-Konzept für Verfügbarkeit

DATENSCHUTZBEAUFTRAGTE

Der Datenschutzbeauftragte

WEBSITE | ONLINE | VIRTUELL

- Impressum
- Datenschutzerklärung
- E-Mail-Verkehr

E-MAIL VERKEHR

DASHBOARD

Grundlagen	Rechtmäßigkeit der Verarbeitung	Veröffentlichungen	Dokumentationen	Aussenwirkung
InCome Anforderungen Fragen	Satzung	Pressearbeit	VVT	Website
Überblick der Themen	Verträge Mitglieder	Social Media	TOM	E-Mail Cloud
Rechtsgrundlagen	Einwilligung	Fotorechte	AVAuftragsverarbeitung | AV Art. 28 DSGVO	Fragenrunde
Personenbezogene Daten	Datenschutz-beauftragte	Datengeheimnis Beschäftigte	Das Datenschutz-handbuch	Feedbackrunde
Haftung Sanktionen	**Datenpannen**	**Auskunfs-ersuchen**	Datenschutz-management-system	**Fallbeispiele**

Über den <Klick> auf das „bvve-Logo“ kommen Sie von jeder Folie aus auf das DASHBOARD zurück

FRAGE

… und wo stehen Sie?

WARUM DATENSCHUTZRECHT? – DER ZWECK

- **der Schutz der personenbezogenen Daten**
- **der Schutz des Persönlichkeitsrechts**

DIE GESETZLICHEN GRUNDLAGEN

Vorteile der Datenschutz-Grundverordnung

- **Ein Regelwerk für ganz Europa**
- **Einheitliche Regeln für alle** Unternehmen, **Vereine**, **Verbände**, die in der EU Dienstleistungen anbieten
- **Neue, gestärkte Rechte für Bürgerinnen und Bürger**
- **Besserer Schutz vor Datenschutzverletzungen**
- **Effektive Regeln und Geldbußen mit Abschreckungswirkung**

EU-Datenschutz-Grundverordnung | EU-DSGVO seit 25. MAI 2018

DIE 7 GRUNDPRINZIPIEN DER DSGVO |

Artikel 5 | Erwägungsgrund 39

1. Rechtmäßigkeit | Artikel 5

- Verarbeitung nach Treu und Glauben
- Transparenz

2. Zweckbindung | Artikel 5

- Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und
- dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden […] („Zweckbindung“)

3. Datenminimierung | Artikel 5

- Personenbezogene Daten müssen dem Zweck angemessen und
- erheblich
- sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“)

4. Richtigkeit | Artikel 5

- Personenbezogene Daten müssen sachlich richtig
- und erforderlichenfalls auf dem neuesten Stand sein
- Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“)

5. Speicherbegrenzung | Artikel 5

- Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist
- Personenbezogene Daten dürfen länger gespeichert werden, soweit diese vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, […] verarbeitet werden („Speicherbegrenzung“)

6. Integrität und Vertraulichkeit | Artikel 5

- Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit dieser Daten gewährleistet,
- einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung
- durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“)

7. Rechenschaftspflicht „Accountability“ | Artikel 5

- Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich
- und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

WAS SIND PERSONENBEZOGENE DATEN?

WO WERDEN DIE VEREINE TANGIERT?

EXTERN

- Internet
- E-Mail
- Presse
- Veranstaltungen
- Öffentlicher Raum
- …

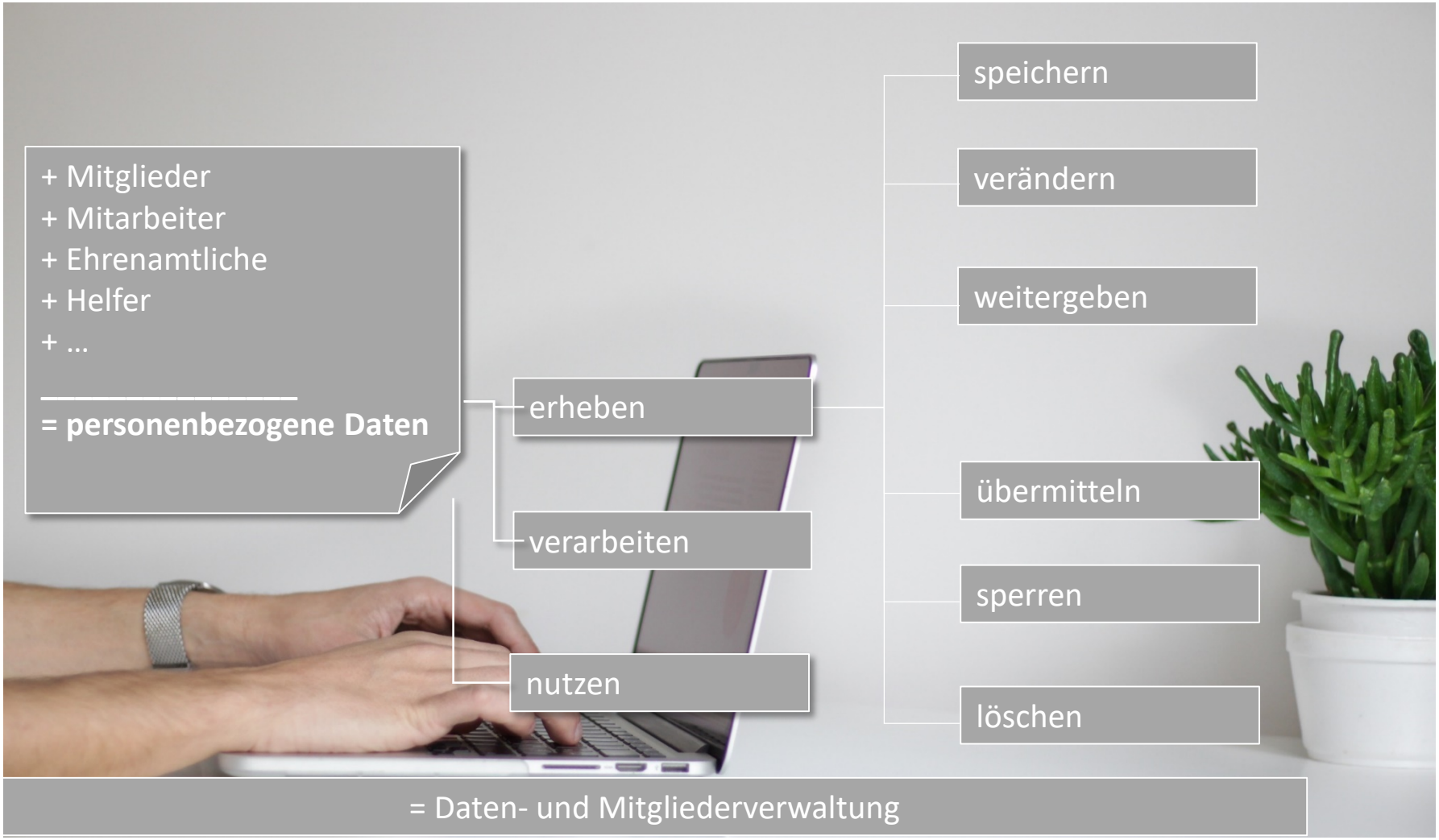
INTERN

Bei der Nutzung und Verarbeitung der personenbezogenen Daten

von

- Mitgliedern
- Mitarbeitern
- Helfern
- Lieferanten
- Sponsoren
- Gästen ...

PERSONENBEZOGENE DATEN IM VEREIN



PERSONENBEZOGENE DATEN | BETROFFENER

Personenbezogene Daten sind alle Informationen, die sich auf eine

- identifizierte oder
- identifizierbare natürliche Person […]

beziehen. (Art. 4 Nr. 1 DSGVO)

Darüber hinaus zählen dazu sämtliche Informationen, die etwas über

- die persönlichen oder
- sachlichen Verhältnisse

einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)

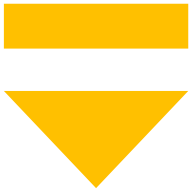
aussagen.

BEISPIELE PERSONENBEZOGENER DATEN

- Name und Anschrift
- Familienstand
- Zahl der Kinder
- Beruf
- Telefonnummer
- E-Mail-Adresse

- Eigentums- oder Besitzverhältnisse
- persönliche Interessen
- Mitgliedschaft in Organisationen
- Datum des Vereinsbeitritts
- sportliche Leistungen
- Platzierung bei einem Wettbewerb

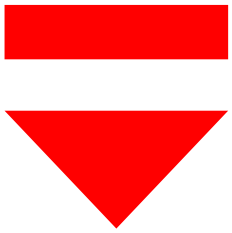
....



BEISPIELE PERSONENBEZOGENER DATEN

Spezielle Beispiele personenbezogener Daten

- Kfz-Kennzeichen
- das Aussehen
- der Gang
- Aufzeichnungen über die Arbeitszeiten
- Bewegt-Bilder und Fotografien von Personen
- IP-Adressen



BESONDERE PERSONENBEZOGENE DATEN

Besondere Arten personenbezogener Daten nach Art. 9 DSGVO

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Verarbeitung von genetischen und
- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person
- Gesundheitsdaten
- Daten zum Sexualleben bzw.
- der sexuellen Orientierung

Wenn Sie diese Daten erheben, brauchen Sie immer einen Datenschutzbeauftragten!

BEISPIELE PERSONENBEZOGENER DATEN

WICHTIG: Nicht vom BDSG geschützt werden Angaben über Verstorbene.

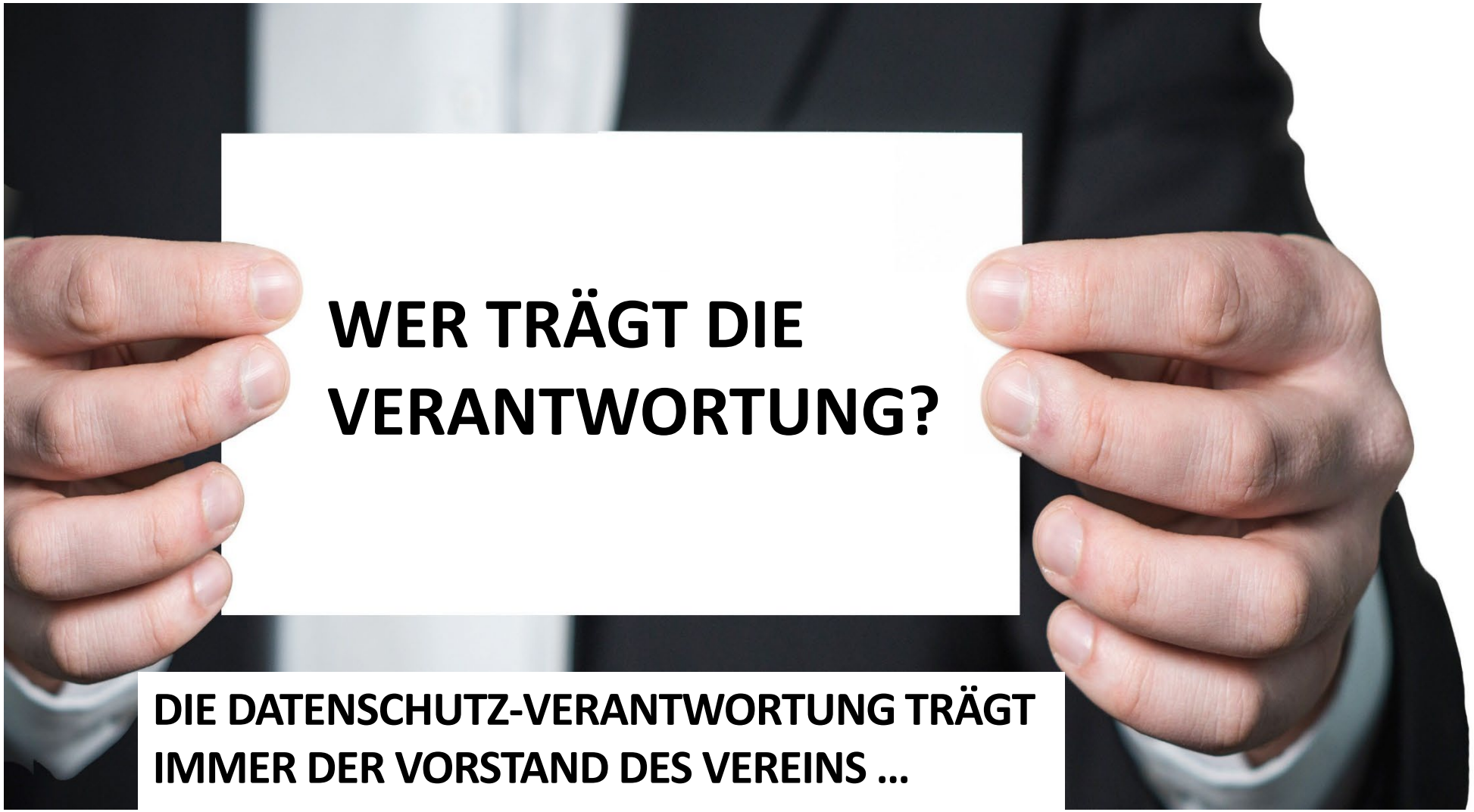
Beispielsweise

- in einem Nachruf für ein verstorbenes Vereinsmitglied
- im Vereinsblatt oder
- In Form einer Nennung auf einer Liste der Verstorbenen

WER ARBEITET REGELMÄßIG MIT PERSONENBEZOGENEN DATEN?

- Vorstand
- Erweiterter Vorstand
- Geschäftsstelle/Sekretariat
- Abteilungsleiter
- Trainer
- Übungsleiter
- Webmaster
- Mitarbeiter/Beschäftigte
  - FSJ – Freiwilliges Soziales Jahr
  - Teilzeitkräfte
  - alle Mitarbeiter, auch die ohne Bezahlung
- …

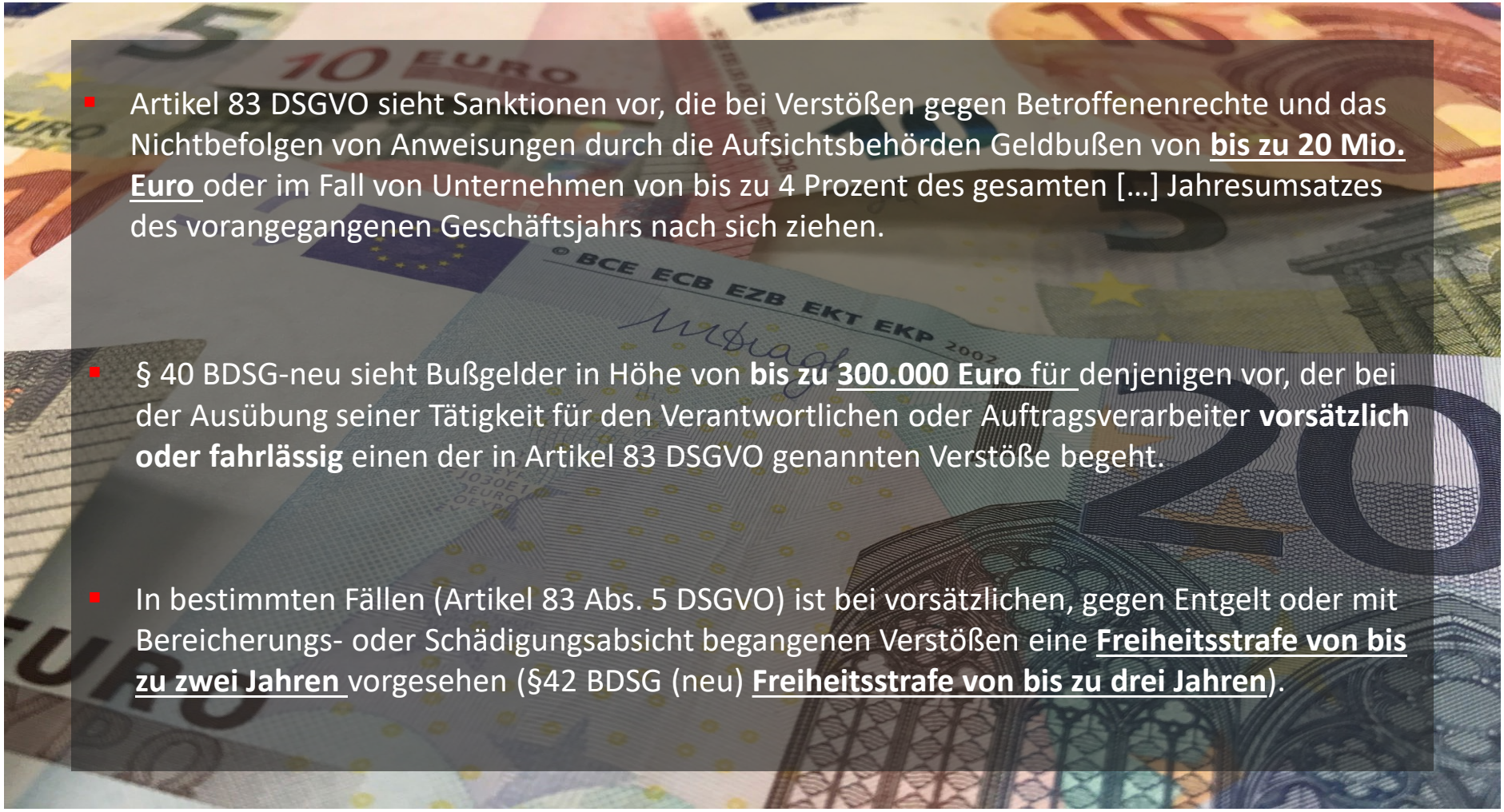
Alle die, die regelmäßig mit personenbezogenen Daten in Berührung kommen …



„Als Verantwortlicher im Verein benötigt man für die Anforderungen in Verwaltung und Datenschutz immer zwei Beine, denn mit dem einen ist man im Gefängnis und mit dem anderen steht man auf einer Bananenschale…“

SANKTIONEN IN DER VERANTWORTLICHKEIT

Sanktionen



- Artikel 83 DSGVO sieht Sanktionen vor, die bei Verstößen gegen Betroffenenrechte und das Nichtbefolgen von Anweisungen durch die Aufsichtsbehörden Geldbußen von **bis zu 20 Mio. Euro** oder im Fall von Unternehmen von bis zu 4 Prozent des gesamten […] Jahresumsatzes des vorangegangenen Geschäftsjahrs nach sich ziehen.

- § 40 BDSG-neu sieht Bußgelder in Höhe von **bis zu 300.000 Euro** für denjenigen vor, der bei der Ausübung seiner Tätigkeit für den Verantwortlichen oder Auftragsverarbeiter **vorsätzlich oder fahrlässig** einen der in Artikel 83 DSGVO genannten Verstöße begeht.

- In bestimmten Fällen (Artikel 83 Abs. 5 DSGVO) ist bei vorsätzlichen, gegen Entgelt oder mit Bereicherungs- oder Schädigungsabsicht begangenen Verstößen eine **Freiheitsstrafe von bis zu zwei Jahren** vorgesehen (§42 BDSG (neu) **Freiheitsstrafe von bis zu drei Jahren**).

RECHTMÄßIGKEIT DER VERARBEITUNG

DAS VERBOTSPRINZIP | ART. 6 DSGVO

Der Verein darf **keine personen-bezogenen Daten erheben –**

es sei denn, es liegt eine Erlaubnis der Datenverarbeitung gemäß **BDSG und DSGVO** vor …

WELCHE DATEN DARF DER VEREIN ERHEBEN?

Rechtsgrundlage

Der Verein darf alle Daten erheben,

- die zur Verfolgung der Vereinsziele und für
- die Betreuung und Verwaltung der Mitglieder erforderlich sind

Wo erhebt der Verein die Daten?

- Beispielhaft im Aufnahmeantrag oder
- in der Beitrittserklärung

DIE SATZUNG IM VEREIN

Der Verein darf alle Daten erheben,

- die zur Verfolgung der Vereinsziele und für
- die Betreuung und Verwaltung der Mitglieder erforderlich sind.

Wichtige Neuerung –

- die DATENSCHUTZRICHTLINIE/DATENSCHUTZINFORMATION

  in der Satzung **oder besser als gesondertes Regelwerk**

Der Kernpunkt für die Verarbeitung ist die Satzung.
Die Satzung ist die Verfassung des Vereins!

SATZUNG 4.0

Neue Regelungen in der Satzung – einfachere Strukturen

Satzungsänderungen, insbesondere Änderungen des Vereinszweckes, sind aufwändig und schwer handhabbar – siehe Einreichung Registergericht bzw. Finanzamt.

Möglichkeiten zur schlankeren Satzung nutzen – „Satzung 4.0“

Einzelne Teile in Vereins- und Geschäftsordnungen auslagern und somit die Satzung verschlanken, z.B.

- Beitrags- und Gebührenordnung
- Finanzordnung
- Geschäftsordnung
- Datenschutzrichtlinien | Datenschutzordnung

DIE „LEAN“-SATZUNG

Warum brauchen wir schlankere Strukturen?

- schnellere Aktions- und Reaktionsmöglichkeiten im Verein und Ehrenamt
- Online-Teilnahmen/virtuelle Teilnahmen im Vereinsleben
- Veröffentlichungen auf der Homepage –
  die Website als offizielles Mitteilungsorgans des Vereins
- Ehrenamt – projektorientiert statt „lebenslang“
- Mitglieder müssen „Fans“ werden!
- Der Verein muss sexy sein

Das Ziel muss sein:

- die jungen Menschen für das Ehrenamt in der Nachfolge zu gewinnen
- Ehrenamt attraktiv gestalten

Der Wurm muss dem Fisch schmecken …

… nicht dem Angler!

Neue und einfachere Strukturen

Auslagerung aller nicht gesetzlich vorgeschrieben Bestandteile in Ordnungen, neue Möglichkeiten erschaffen für:

- Externe, virtuelle Teilnahme an Vorstandssitzungen
- Partiell mögliche Verantwortung
- Virtuelle Mitgliederversammlungen
- Die Website als offizielles Mitteilungsorgan

Vorteil: Änderungen, die kurzfristig erfolgen sollen oder stetigem Wandel unterliegen (z.B. Datenschutz), kann der Vorstand beschließen. Dies muss nicht über die ordentliche Mitgliederversammlung oder eine außerordentliche Mitgliederversammlung erfolgen.

LEISTUNGEN, DIE DER VEREIN ERFÜLLEN MUSS

Informationspflichten, Betroffenenrechte

INFORMATIONSPFLICHTEN

Keine rückwirkende Informationspflicht

Gegenüber betroffenen Personen, **die vor dem 25. Mai 2018 ihren Status als Beschäftigte, Bestandskunden oder Vereinsmitglied** erworben haben, **entstehen rückwirkend keine Informationspflichten** nach Art. 13 Abs. 1 und 2 der DSGVO, da die ursprüngliche Erhebung von deren personenbezogenen Daten abgeschlossen ist und im Erhebungszeitraum die entsprechenden rechtlichen Vorgaben zur Einhaltung von Informationspflichten noch nicht galten.

WICHTIG: Die Informationspflichten entfallen dann, wenn die betroffene Person bereits über die Informationen verfügt (Art. 13 Abs. 4 und Art. 14 Abs. 5 Buchst. a DSGVO).

INFORMATIONSPFLICHTEN

Pflichten als Verantwortlicher, um die Informationspflichten aus Art. 13 und 14 Datenschutz-Grundverordnung (DSGVO) zu erfüllen:

Bestandteile der Informationspflichten | Art. 13 Abs. 1 und 2 DSGVO

- **Verantwortliche Stelle**
  Name und Kontaktdaten der verantwortliche Stelle
- **Zwecke, für welche die personenbezogenen Daten verarbeitet werden**
  (Verarbeitungszwecke und Rechtsgrundlagen)
- **Notwendigkeit der Angabe der persönlichen Daten** – Beschreibung der berechtigten Interessen bei Verarbeitungen nach Art. 6 Abs. 1 Buchst. f DSGVO; gesetzliche oder vertragliche Verpflichtungen der betroffenen Person zur Bereitstellung bestimmter Daten
- **Direkterhebung** der personenbezogenen Daten bei der betroffenen Person selbst (Art. 13 DS-GVO); **Dritterhebung**: Die personenbezogenen Daten werden bei einem Dritten erhoben (Art. 14 DS-GVO).
- **Personen, die Zugriff auf die Daten haben**
- **Welche Daten werden im Einzelnen erhoben?**

INFORMATIONSPFLICHTEN

- **Mögliche Empfänger** der personenbezogenen Daten
- **Welche Daten werden im Einzelnen übermittelt?**
- Wahrnehmung **berechtigter eigener Interessen** des Vereins
- **Speicherdauer** – wie lange werden die Daten der Betroffenen gespeichert?
- **Recht auf Auskunft**, Berichtigung, Löschung usw.
- Hinweis auf **Widerrufsmöglichkeit** einer erteilten Einwilligung
- **Beschwerderecht** bei der Datenschutzaufsichtsbehörde wegen Datenschutzverstößen
- **Datenschutzbeauftragter** des Vereins (sofern notwendig) –
  Name und Kontaktdaten, mindestens E-Mail-Adresse
- **externe Auftragsverarbeitung** von Daten – AVD (Schreibarbeiten, Digitalisierung, Verwaltung)
- Absicht zur **Verarbeitung in Drittländern**, also Staaten außerhalb der EU
- nähere Angaben im Falle **automatisierter Entscheidungsfindungen** einschließlich **Profiling**


Wird die Kamera zur DSGVO-Falle?
KuG vs. DSGVO?

FOTO | RECHTLICHE ANFORDERUNGEN UNTER DER DSGVO

Beispiel der Informationsmöglichkeit in Form von Bannern oder Plakaten

Der Verantwortliche

Welche Daten werden erhoben?

Der Zweck der Verarbeitung

Wo finden sich weitere Informationen, die zur Verfügung zu stellen sind, um eine faire und transparente Verarbeitung zu gewährleisten?

Wo erfolgt die Veröffentlichung?

An wen kann man sich wenden?

QR-Code (optional)

SOZIALE MEDIEN – DATENSCHUTZKONFORME NUTZUNG

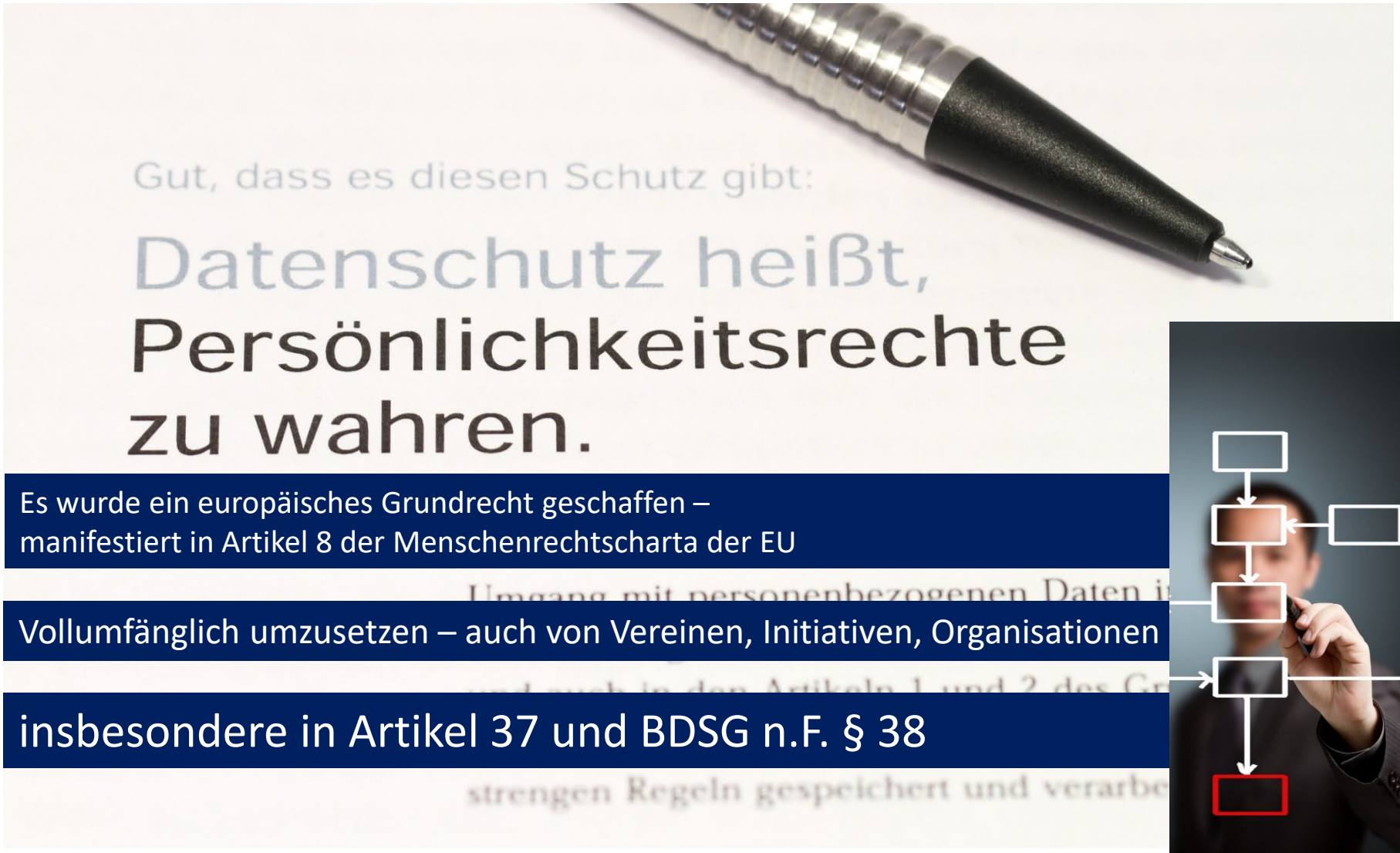
- Facebook
- WhatsApp
- Instagram
- Snapshot
- ….

Wie überprüfe ich einen Anbieter auf DSGVO-Konformität?

- Impressum
- Datenschutzerklärung
- Wo steht der Server?

Facebook Urteil

FRAGERUNDE



Es wurde ein europäisches Grundrecht geschaffen –
manifestiert in Artikel 8 der Menschenrechtscharta der EU

Vollumfänglich umzusetzen – auch von Vereinen, Initiativen, Organisationen

insbesondere in Artikel 37 und BDSG n.F. § 38

DER DATENSCHUTZBEAUFTRAGTE | ART. 37 UND BDSG n.F. § 38

- **Datenschutz-Folgenabschätzung** | relativ unerheblich in Vereinen

- **Bei Verarbeitung besonderer Kategorien** von **personenbezogenen Daten gemäß Artikel 9 DSGVO – besonderes erheblich bei Gesundheitssport und Therapieangeboten | - Gruppen**

Nach Anzahl der Personen, die mit personenbezogenen Daten umgehen – Art. 37 DSGVO – § 38 BDSG.

- **Die Benennungspflicht eines Datenschutzbeauftragten (DBS) besteht für Vereine, soweit sie in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen.**

- **Dabei zielt der Wortlaut nicht darauf ab, ob die zehn Personen in einem bezahlten Arbeitsverhältnis stehen. Auch Ehrenamtliche zählen dazu. Die Aufgabe muss auch nicht die Hauptaufgabe der Personen sein.**

- **Maßgeblich ist zudem die Zahl der Köpfe, nicht die Zahl der Stellen.**

Quellen: Datenschutzkonferenz der Länder DSK | Stellungnahmen der Landesbeauftragten für den Datenschutz | DSGVO | BDSG

DER DATENSCHUTZBEAUFTRAGTE | ART. 9

- **Bei Verarbeitung besonderer Kategorien** von **personenbezogenen Daten gemäß Artikel 9 DSGVO**

- **Datenschutz-Folgenabschätzung**

Außerdem besteht die Pflicht zur Benennung eines Datenschutzbeauftragten für Vereine, die einer **Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO unterliegen** oder wenn **geschäftsmäßig Daten – anonymisiert oder nicht – zum Zwecke der Markt- oder Meinungsforschung** übermittelt werden.

Wichtig: Sind die Rechte und Freiheiten von Personen durch eine Datenverarbeitung einem **hohen Risiko ausgesetzt**, so ist vor der Datenverarbeitung eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen. Dies regelt Art. 35 DSGVO (früher Vorabkontrolle).

DER DATENSCHUTZBEAUFTRAGTE | WANN IST ER NÖTIG?

Nach Anzahl der Personen, die mit personenbezogenen Daten umgehen –
Art. 37 DSGVO – § 38 BDSG.

- Die Benennungspflicht eines Datenschutzbeauftragten (DBS) besteht für Vereine, soweit sie in der Regel **mindestens zehn Personen ständig** mit der Verarbeitung personenbezogener Daten beschäftigen.

- Dabei zielt der Wortlaut nicht darauf ab, ob die zehn Personen in einem bezahlten Arbeitsverhältnis stehen. **Auch Ehrenamtliche zählen dazu.**

- Maßgeblich ist zudem die **Zahl der Köpfe**, nicht die Zahl der Stellen.

Wichtig: Es besteht die Meldepflicht des Datenschutzbeauftragten bei der Datenschutzbehörde!

Ständig – Definition der Begrifflichkeit

längerer Zeitraum:

- Ist eine Person für eine Aufgabe über einen längeren Zeitraum vorgesehen und nimmt diese Aufgabe auch war, dann ist diese ständig mit der Verarbeitung beschäftigt.

Wahrnehmung der Tätigkeiten

- D. h. ständig ist auch dann als Tatbestandsmerkmal erfüllt, wenn die Aufgabe selbst nur gelegentlich anfällt, die betroffene Person sie aber stets (immer) wahrzunehmen hat.

Es gilt die Anzahl der Köpfe – nicht die Anzahl der Stellen.

Wichtig: Dies gilt natürlich auch dann, wenn sich diese Person diese Tätigkeit mit einer anderen Person oder mehreren anderen Personen teilt.

DSB | DEFINITION DER BEGRIFFLICHKEITEN

Nicht ständig – Definition der Begrifflichkeit

Nicht ständig:

- ist derjenige beschäftigt, der nur **gelegentlich andere obliegende Aufgaben** übernimmt oder
- nur vorübergehend in diesem Bereich tätig ist.

Wichtig: Es ist unerheblich, ob eine Person hauptamtlich oder ehrenamtlich, also ohne oder mit Entlohnung tätig ist. Die Aufgabe muss auch nicht die Hauptaufgabe der Personen sein.

Begriffsbestimmungen sind zu finden in § 46 BDSG

DSB | AUFGABEN

- Kontrolle für die Einhaltung der **datenschutzrechtlichen Bestimmungen bezüglich des Umgangs mit personenbezogenen Daten** bei der verantwortlichen Stelle
- Der DSB ist **unabhängiges Kontrollorgan**
- **Pflicht zur Kontrolle und Überwachung** der Abläufe auf die **Einhaltung der Datenschutzbestimmungen**
- zuständig für Aufbau einer Datenschutzorganisation
- informiert regelmäßig intern über Datenschutzrichtlinien, Bekanntmachungen
- **Ansprechpartner** bei Bedenken und Fragen zum Datenschutz im Verein | Unternehmen für
  - Mitglieder
  - Betroffene
  - Behörde
  - Unternehmens-/Vereinsführung

DSB | AUFGABEN

- Einbeziehen in **alle relevanten betrieblichen Planungs- und Entscheidungsabläufe**
- regelmäßige Schulung der Beschäftigten **hinsichtlich des Datenschutzes**
- **Gesamtüberblick über sämtliche Verfahrensverzeichnisse**
- **Überwachung der rechtmäßigen Entsorgung und Löschung**
- Der DSB unterliegt aufgrund seiner besonderen Stellung
  - ✓ der **Verschwiegenheitspflicht** und
  - ✓ hat zudem ein **Zeugnisverweigerungsrecht sowie**
  - ✓ einen **besonderen Kündigungsschutz**

Der Datenschutzbeauftragte ist der Geschäftsleitung/Vereinsführung direkt unterstellt.

Er wird nicht gewählt sondern benannt/bestellt.

DSB | QUALIFIKATIONEN

Der Datenschutzbeauftragte wird benannt auf der Grundlage seiner

- **beruflichen Qualifikation und**
- **insbesondere des Fachwissens.**

Qualifikationen | allgemein

- Datenschutzrecht allgemein –
  unabhängig von der Branche und der Größe der verantwortlichen Stelle
- Persönlichkeitsrechte der Betroffenen und Mitarbeiter
- umfassende Kenntnisse des Datenschutzrechts
  einschließlich technischer und organisatorischer Art
- Kenntnisse des Anwendungsbereiches datenschutzrechtlicher und einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen
- ...

Weiterführende Info
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/03/Beschluss-des-D%C3%BCsseldorfer-Kreises-2010-Mindestanforderungen_an_DSB_nach_4f_II_und_III_BDSG.pdf

DER DATENSCHUTZBEAUFTRAGTE | WICHTIG

- Sofern in einem Verein also zehn Übungsleitende oder Lehrkräfte die personenbezogenen Daten ihrer Trainierenden bzw. Schüler in einer Datei auf dem PC verarbeiten, ist ein Datenschutzbeauftragter zu bestellen.

- **Gesetzliche Grundlagen:**
  - ✓ **Art. 37 DSGVO** Benennung eines Datenschutzbeauftragten
  - ✓ **Art. 38 DSGVO** Stellung des Datenschutzbeauftragten
  - ✓ **Art. 39 DSGVO** Aufgaben des Datenschutzbeauftragten
  - ✓ **§ 38 BDSG** Bundesdatenschutzgesetz

- **Weitere Quellen**
  - Kurzpapier-Nr. 12 DSK Datenschutzkonferenz der Länder
  - Ergänzend | DSK | Düsseldorfer Kreis | bisherige Art. 29 Gruppe

- **ACHTUNG:** Erhebliche Sanktionen, wenn kein DSB benannt wird, obwohl die Verpflichtung dazu bestünde (bis zu 10 Mio. Euro oder 2 % des Jahresumsatzes, vgl. Art. 83 Abs. 4 lit. A DSGVO)

PRÜFUNGSSCHEMA ZUR NOTWENDIGKEIT EINES DSB

Anzahl der Personen > 9, die ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind?

JA → **DSB zu benennen**

Wichtig: Es ist unerheblich, ob eine Person hauptamtlich oder ehrenamtlich, also ohne oder mit Entlohnung, tätig ist. Die Aufgabe muss auch nicht die Hauptaufgabe der Person sein.

Nein ↓

Verarbeitungsprozesse, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche, regelmäßige und systematische Überwachung der betroffenen Person erforderlich macht?

JA → **DSB zu benennen**

Anmerkung: Im Regelfall kann davon ausgegeben werden, dass die Kerntätigkeit eines Vereines nicht in den Verarbeitungsprozessen der personenbezogenen Daten liegt, welche eine umfangreiche, regelmäßige und systematische Überwachung der betroffenen Personen erforderlich macht (z.B. Videoüberwachung im Stadion).

Nein ↓

Werden im Verein Verarbeitungen vorgenommen, die einer Datenschutz-folgeabschätzung nach Art. 35 unterliegen?

JA → **DSB zu benennen**

Anmerkung: Eine Datenschutzfolgeabschätzung ist nur dann erforderlich, wenn die Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen hat. Ein solch hohes Risiko ist jedoch die Ausnahme und besteht in aller Regel bei kleinen Vereinen nicht.

Nein ↓

NOTWENIGKEIT ZUM DSB

Werden im Verein Verarbeitungen „besonderer Kategorien von Daten gemäß Art. 9“ vorgenommen?

JA → **DSB zu benennen**

Nein ↓

Anmerkung: Besondere Kategorien von Daten sind personenbezogene Daten, aus denen die rassische bzw. ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben und der sexuellen Orientierung.
Beispiele: Religionszugehörigkeit, Parteizugehörigkeit, Angaben über Krankheiten, Koronarsportgruppen …
Hinzukommen muss jedoch auch hier, dass die Kerntätigkeit des Vereins in der Verarbeitung vorgenannter Daten liegt. Dies ist immer dann der Fall, wenn ohne die Verarbeitung dieser Daten der Zweck des Vereins nicht erreicht werden könnte. **Denkbar ist dies etwa bei Selbsthilfegruppen oder Vereinen mit politischer Zielrichtung.**

Werden im Verein Verarbeitungen über strafrechtliche Verurteilungen und Straftaten vorgenommen?

JA → **DSB zu benennen**

Nein ↓

Wichtig: Die Kontaktdaten des DSB sind nach Art. 37 Abs. 7 DSGVO zu veröffentlichen und der Aufsichtsbehörde mitzuteilen. Die Aufsichtsbehörden werden den mitteilungspflichtigen Stellen ein Formular zur Mitteilung der Kontaktdaten des DSB zur Verfügung stellen.
Anmerkung: Inwieweit es hier ausreichend ist, ausschließlich die E-Mail-Adresse des Datenschutzbeauftragten auf der Vereinshomepage zu benennen und frei zugänglich zu machen, ist noch abschließend zu klären.

Kein Datenschutzbeauftragter zu benennen!

WER DARF NICHT DATENSCHUTZBEAUFTRAGTER WERDEN?

Vermeidung von Interessenskonflikten | Interessenkollisionen

Es soll kein Umstand, in dem eine Person sich quasi selbst kontrolliert, vorhanden sein. Deshalb dürfen keine Interessenkollisionen in oder bei der Person vorliegen

Beispiele, wer es NICHT sein darf:

- Geschäftsführer
- Vorstände
- Leitung der Personalabteilung
- IT-Leiter (Passwortverwaltung, Webhosting)

Hinweis: Der Datenschutzbeauftragte muss nicht Mitglied des Vereins sein (Art. 37 Abs. 6 DS-GVO).

DSB | AUFGABEN

- Kontrolle für die Einhaltung der **datenschutzrechtlichen Bestimmungen bezüglich des Umgangs mit personenbezogenen Daten** bei der verantwortlichen Stelle
- der DSB ist **unabhängiges Kontrollorgan**
- **Pflicht zur Kontrolle und Überwachung** der Abläufe auf die **Einhaltung der Datenschutzbestimmungen**
- zuständig für Aufbau einer Datenschutzorganisation
- informiert regelmäßig intern über Datenschutzrichtlinien, Bekanntmachungen
- **Ansprechpartner** bei Bedenken und Fragen zum Datenschutz im Verein/Unternehmen

DSB | AUFGABEN

- Einbeziehen in **alle relevanten betrieblichen Planungs- und Entscheidungsabläufe**
- regelmäßige Schulung der Beschäftigten **hinsichtlich des Datenschutzes**
- **Gesamtüberblick über sämtliche Verfahrensverzeichnisse**
- **Überwachung der rechtmäßigen Entsorgung und Löschung**

- Der DSB unterliegt aufgrund seiner besonderen Stellung
  - der **Verschwiegenheitspflicht** und
  - hat zudem ein **Zeugnisverweigerungsrecht sowie**
  - einen **besonderen Kündigungsschutz**

Der Datenschutzbeauftragte ist der Geschäftsleitung/Vereinsführung direkt unterstellt. Er wird nicht gewählt sondern benannt/bestellt.

PROBLEMSTELLUNG

- **Wie sollen Vereine die DSGVO-Anforderungen leisten?**
- **Woher soll ein Datenschutzbeauftragter kommen?**
- **Mit welchen Mitteln soll er bezahlt werden?**

LÖSUNG: Die Vereine brauchen einen Ansprechpartner für Anwendungs- und Umsetzungsfragen zur DSGVO

➔ **einen zentralen Datenschutzbeauftragten**

bvve
Bundesverband der Vereine
und des Ehrenamtes e.V.

DATENSCHUTZBEAUFTRAGTE(R) IN VEREIN UND EHRENAMT | DSBIV

Dauer: Fünf Tage + Prüfungstag

Abschluss: Teilnahmebescheinigung und nach erfolgreich abgelegter Prüfung „Datenschutzbeauftragte(r) im Verein – DSBIV“ mit bvve Zertifikat

DATENPANNE

Nicht vergessen! Meldepflicht bei Datenpannen

Nach Art. 4 Abs.12 + Art. 33 DSGVO

DER DATENSCHUTZKOORDINATOR

Der Datenschutzkoordinator (DSK) bildet die Schnittstelle zwischen dem Verein intern und z.B. einem externen Datenschutzbeauftragten.

Datenschutzkoordinatoren unterstützen die verantwortliche Stelle und vor allem den/die Datenschutzbeauftragten im Bereich des Datenschutzes:

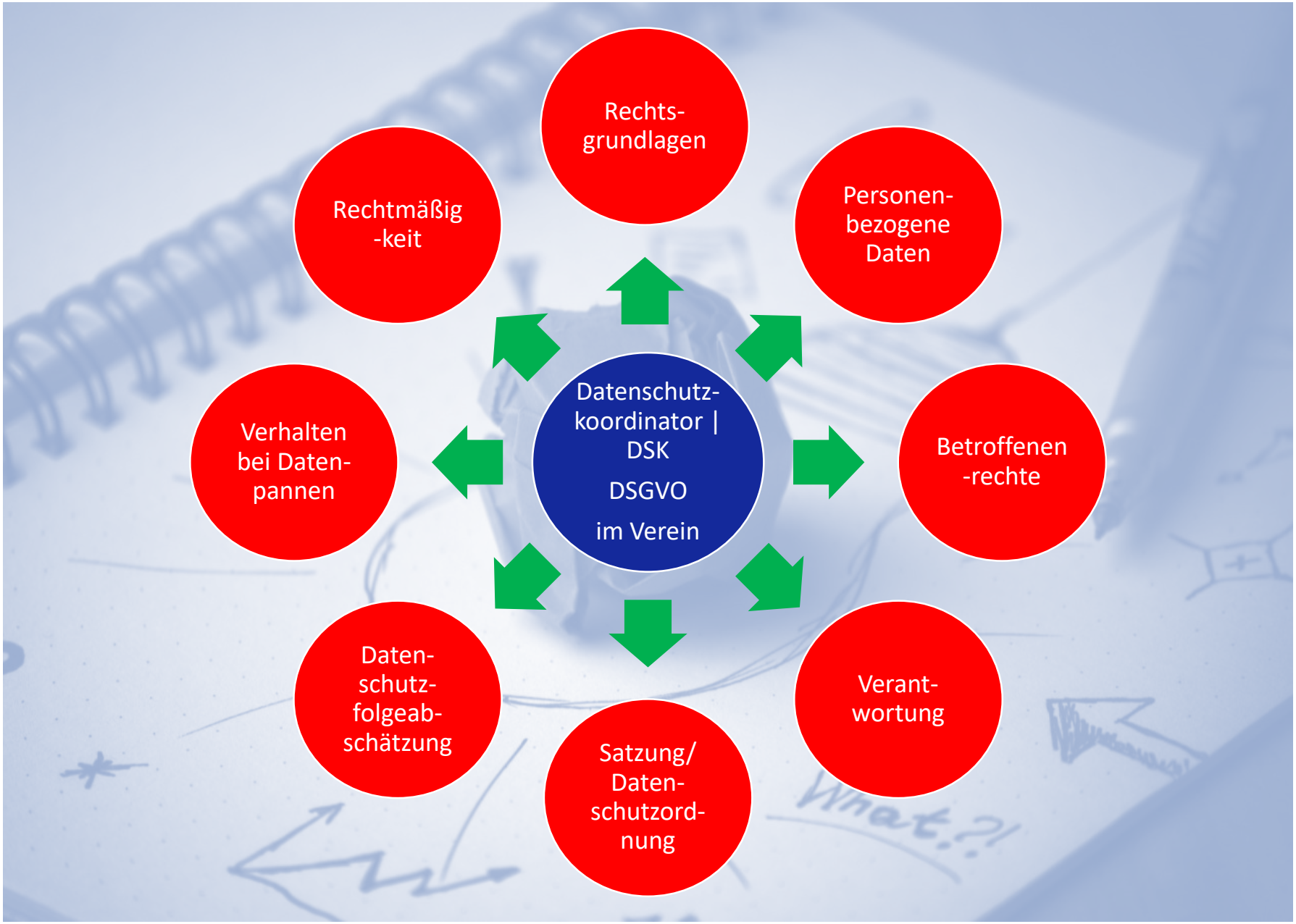
- Integration der Anforderungen der DSGVO in die vereinsinternen Abläufe
- notwendige neue Strukturen und Abläufe erarbeiten und vorschlagen
- datenschutzkonforme Entscheidungen treffen
- fundierte Einschätzungen vornehmen
- Zusammenhänge und Folgen abschätzen

Dauer: Die Weiterbildung umfasst eineinhalb Tage.

Voraussetzungen: DSK verfügen über ein gewisses Maß an Fachkunde.
Der Datenschutzkoordinator muss mit den jeweiligen Vereinen/Unternehmen und seinen Prozessen, Abläufen und seiner Infrastruktur eingehend vertraut sein.

Abschluss: bvve-Zertifikat

DER DATENSCHUTZKOORDINATOR | DSK



DIE BVVE INITIATIVE ZUM ZWEIGLIEDRIGEN SYSTEM

MUSTER-
VEREIN e.V.

Der Verein definiert den Aufgabenbereich des Datenschutzkoordinators | DSK

Der DSK erstellt die Dokumentationen und übernimmt die datenschutzspezifischen Aufgaben im Verein.

Der DSK ist zentraler Ansprechpartner für die Mitglieder, die Vereinsführung etc.

Das Fundament des Vereins …

Der DSK

- erstellt das Verzeichnis der Verarbeitungstätigkeiten VVT
- dokumentiert und überprüft die TOM | Technisch Organisatorische Maßnahmen
- erstellt die AV-Verträge
- führt im Verein die Auskunftsersuchen und Löschkonzepte
- prüft die Datenübermittlung – Datenweitergabe
- schützt die Betroffenenrechte
- führt die Dokumentationen
- …

Der DSK im Verein, ist zentrales Bindeglied zum externen DSB

Der Datenschutzkoordinator ist die neue Stabstelle im Verein!

DER ZENTRALE DATENSCHUTZBEAUFTRAGTE | DSB

Die D.S.I.Z. der VEREINE im Enzkreis

Datenschutzinformationszentrale für Vereine im Enzkreis
Externer Datenschutzbeauftragte des bvve e.V.
als zentraler externer DSB für die Vereine

Der Datenschutzbeauftragte | DSB

- informiert
- schätzt ein, analysiert
- beantwortet Fragen und
- unterstützt den Datenschutzkoordinator im Verein
- prüft auf Anforderung die Umsetzungen der Dokumentationen der Vereine

… er ist zentraler offizieller Ansprechpartner

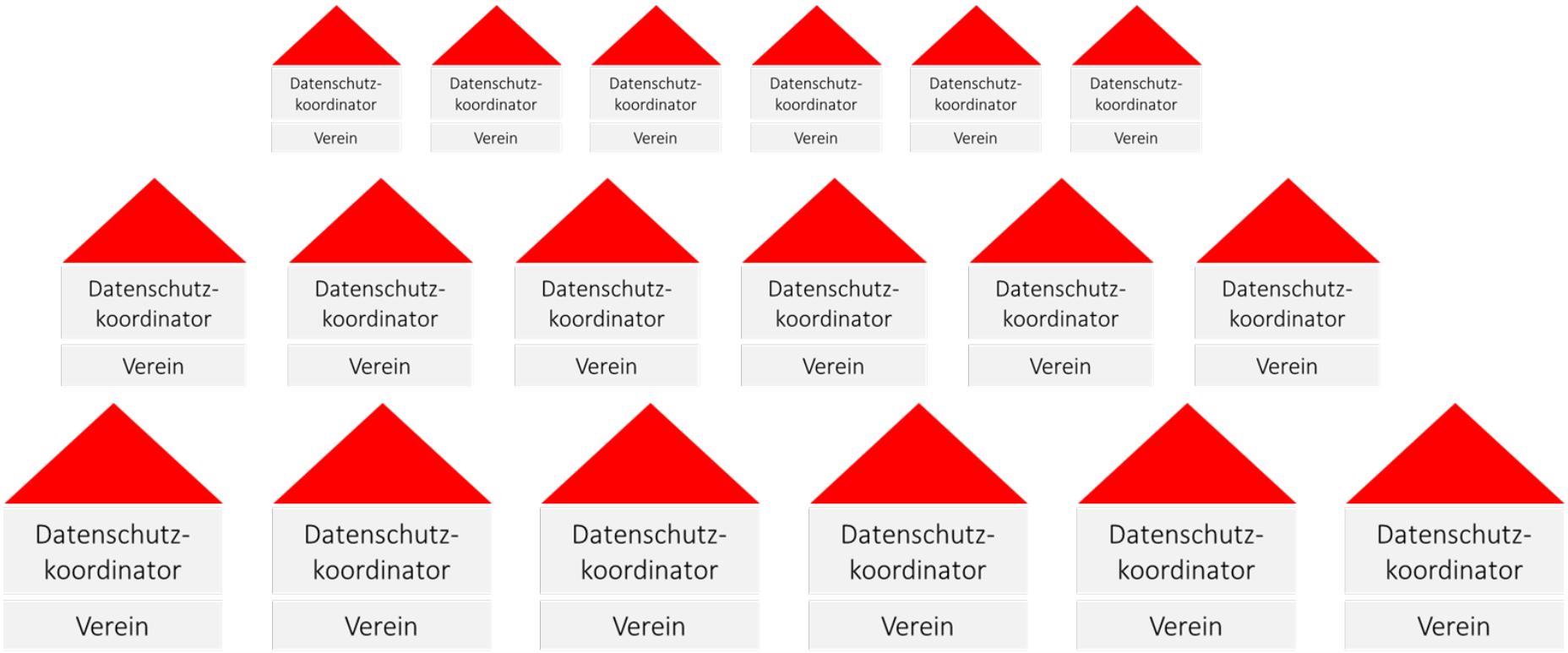
- zu Betroffenen
- zu Verantwortlichen
- zu Behörden
- er berät die Datenschutzkoordinatoren in den Vereinen
  - online und virtuell
  - in der Datenschutzsprechstunde in der Geschäftsstelle

Das Fundament für die Vereine …

IM ERGEBNIS

Datenschutzinformationszentrale für Vereine im Enzkreis

Externer Datenschutzbeauftragte des bvve e.V.
als zentraler externer DSB für die Vereine

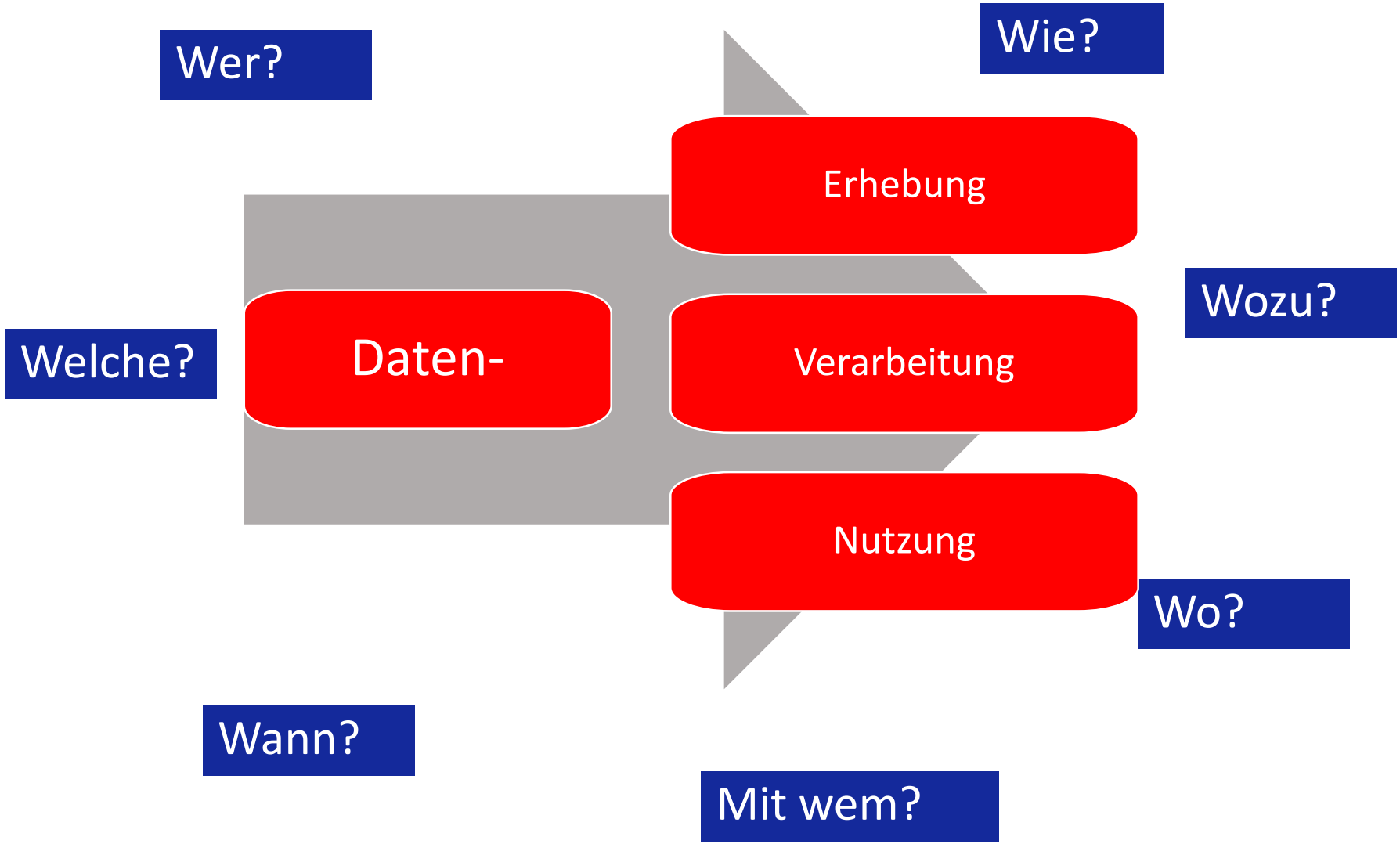


DER DATENSCHUTZKOORDINATOR

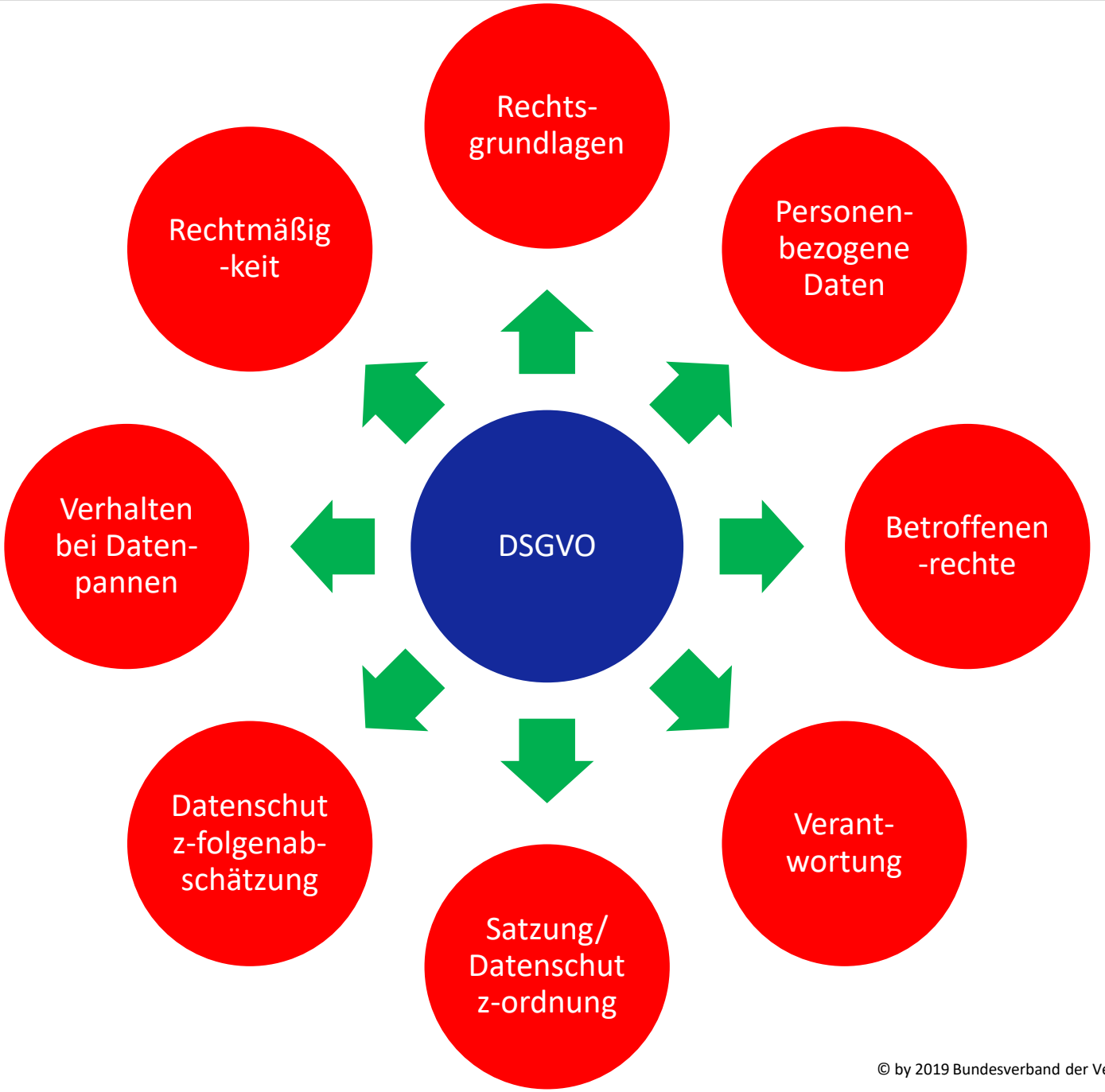
Der Datenschutzkoordinator
muss eine neue Stabstelle
im Vorstand des Vereins werden.

Lassen Sie sich dies in der nächsten Mitgliederversammlung legitimieren!

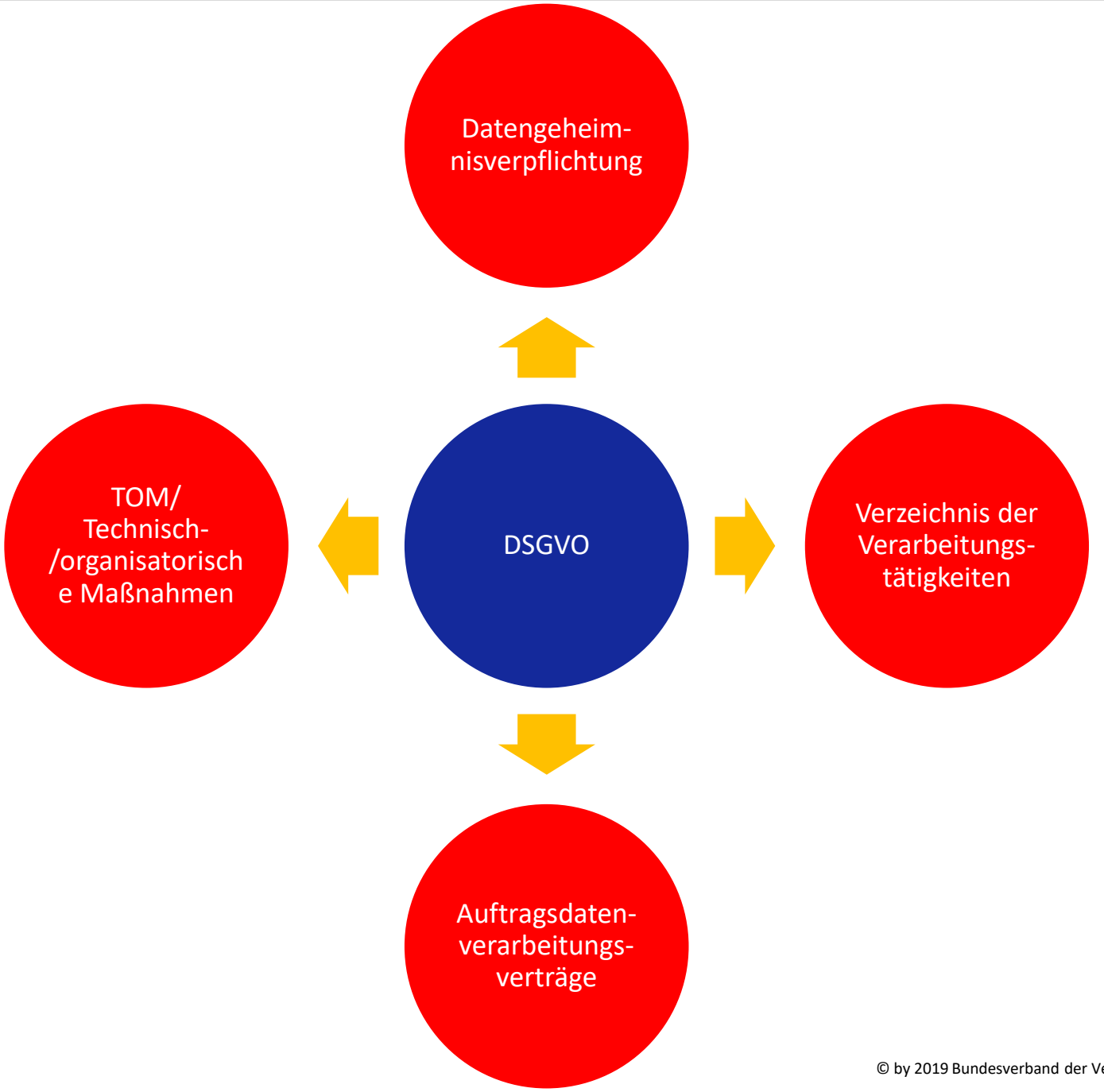
WELCHE ABLÄUFE HABEN SIE IM VEREIN



GRUNDLAGEN DER DSGVO



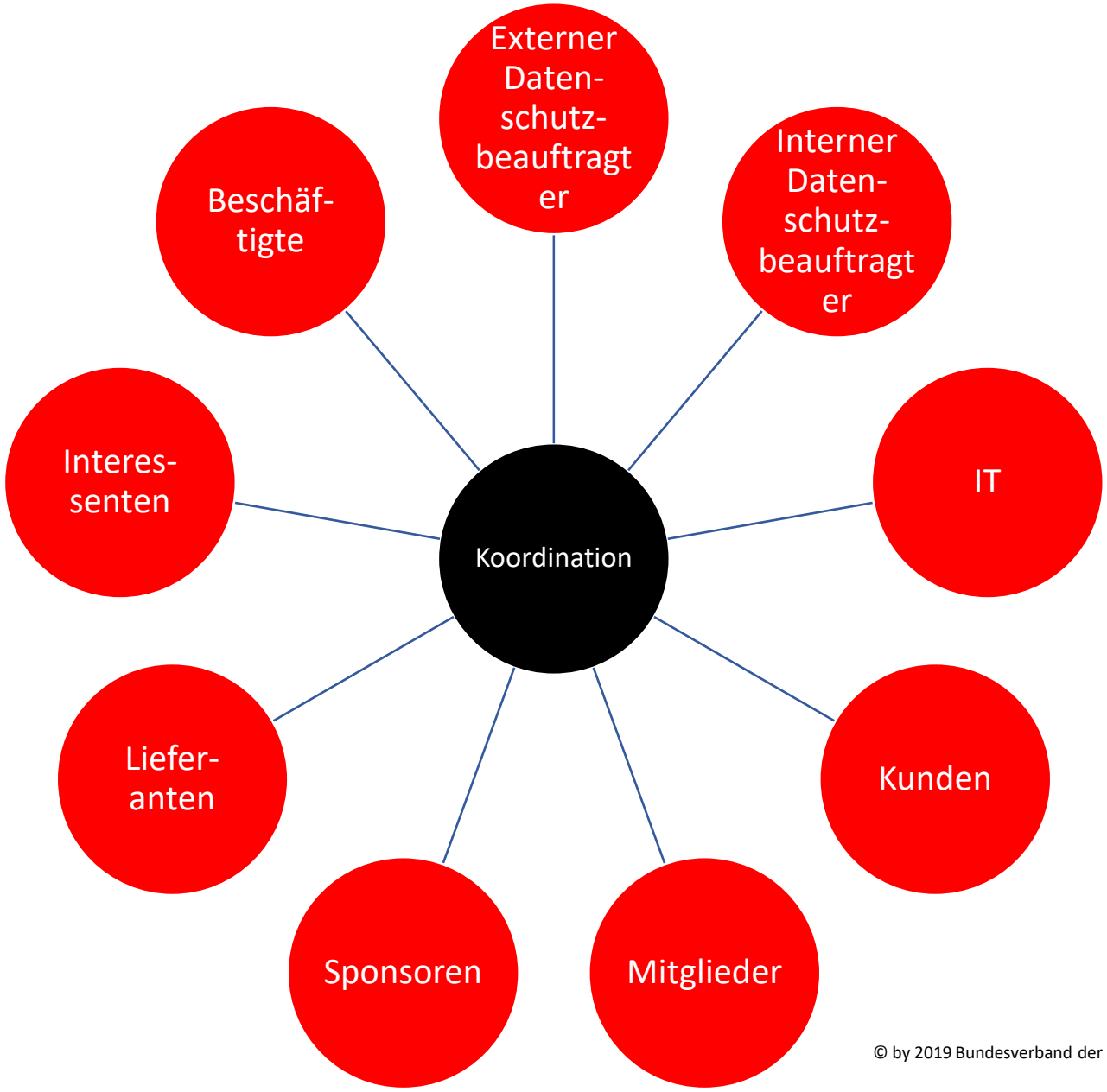
PFLICHTEN



IM AUßENKONTAKT

DER DATENSCHUTZKOORDINATOR

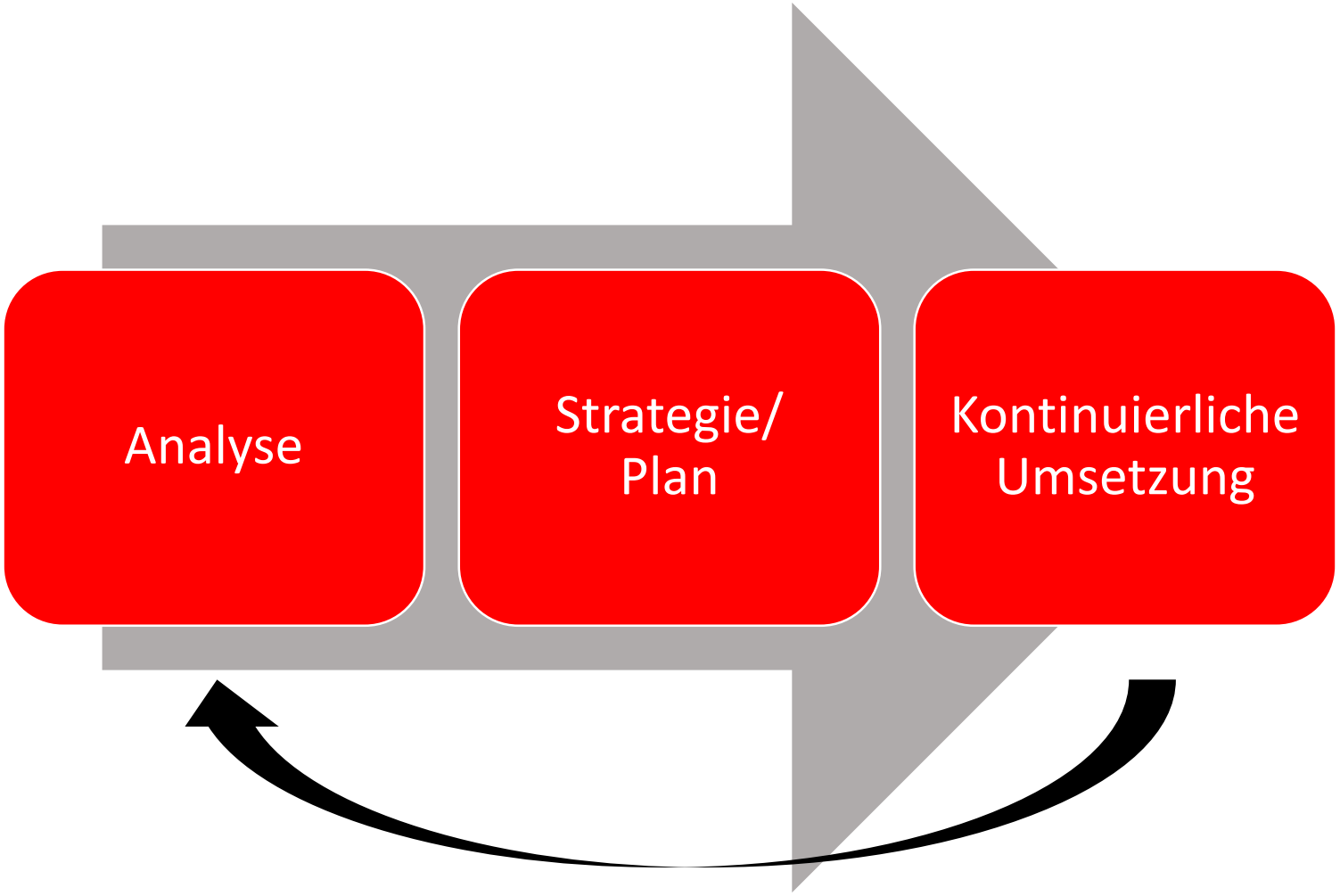
Persönliche Ebene



DER DATENSCHUTZKOORDINATOR

Drohnenperspektive

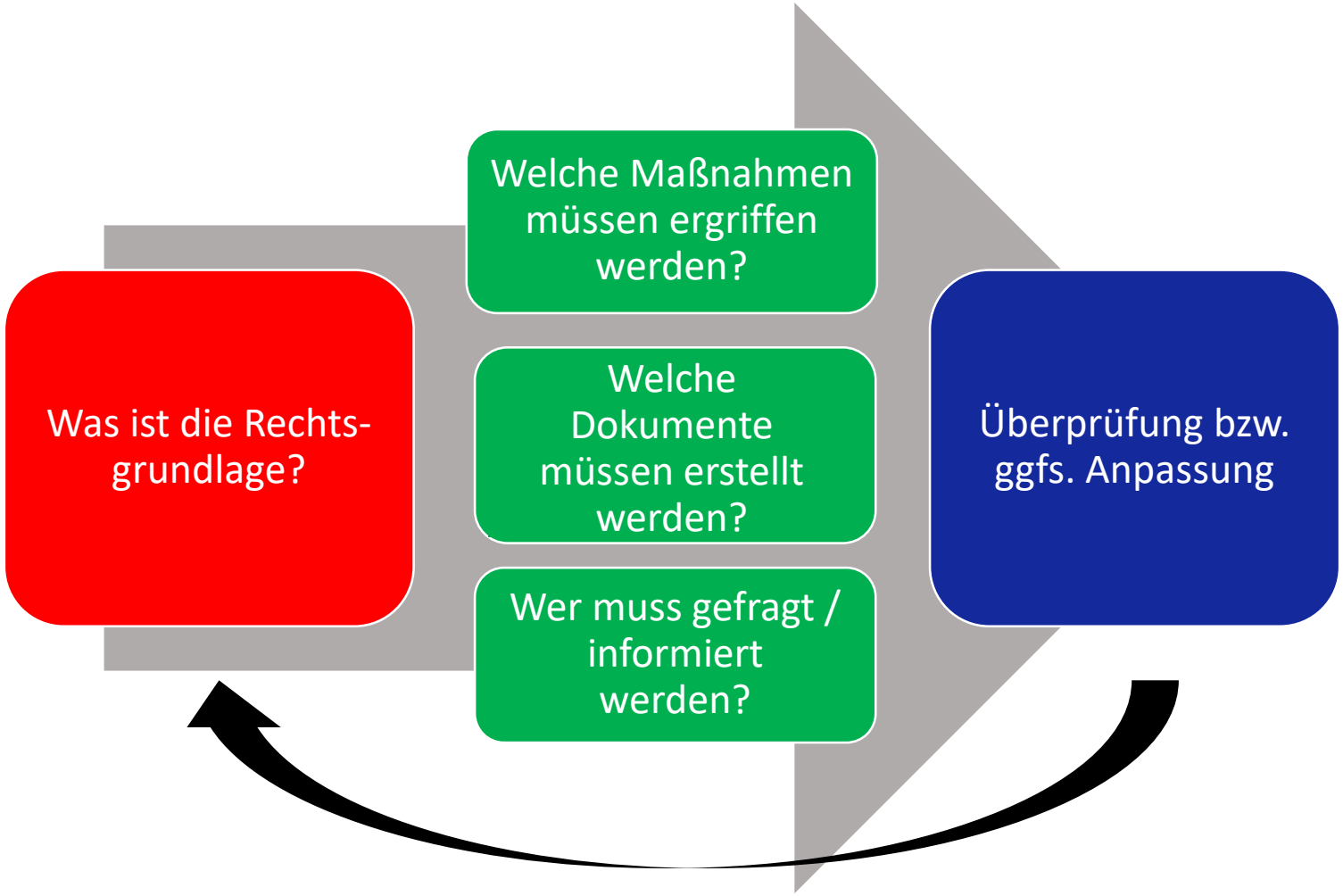
DIE ARBEITSWEISE | ASU



Analyse, Strategie und Umsetzung | ASU

ANALYSE, STRATEGIE UND UMSETZUNG

Im Einzelnen …



DIE HERAUSFORDERUNG

Verpflichtung zur Führung von Verfahrensverzeichnissen

Verfahrensverzeichnisse

Der Zweck ergibt sich aus dem Erwägungsgrund (ErwGr.) 82 zu Art. 30 DSGVO

- **Dieses Verzeichnis betrifft sämtliche ganz oder teilweise automatisierte Verarbeitungen,** sowie nichtautomatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen**.**
- **Für jede einzelne Verarbeitungstätigkeit** ist eine Beschreibung nach Maßgabe des Art. 30 DSGVO anzufertigen.

Anmerkung: Als Verarbeitungstätigkeit wird im Allgemeinen ein Geschäftsprozess auf geeignetem Abstraktionsniveau verstanden.

Es ist ein strenger Maßstab anzulegen, so dass jeder neue Zweck der Verarbeitung eine eigene Verarbeitungstätigkeit darstellt.

Bei einer nur geringen Zweckänderung muss geprüft werden, ob eine bereits bestehende Beschreibung einer Verarbeitungstätigkeit angepasst werden muss oder ob eine vollständig neue Beschreibung anzufertigen ist.

➔ Die Summe der Einzelbeiträge ergibt das Verzeichnis von Verarbeitungstätigkeiten.

Verfahrensverzeichnisse | Beispiele

- **Mitgliederverwaltung**
  In der Mitgliederverwaltung werden die Aufnahme neuer, die Abrechnung bestehender und die allgemeine Information von Mitgliedern verarbeitet. Hier werden regelmäßig die persönlichen Daten wie E-Mail-Adresse, Kontodaten, Alter etc. erfasst. Die Rechtsgrundlage für diese Verarbeitung liegt im Zweck oder dem berechtigten Interesse des Vereins bzw. kann auch durch Einwilligungserklärungen gegeben sein.
- **Turnier und Trainingsverwaltung**
  Wesentlich bei diesem typischen Verfahren sind vor allem die Erhebung und die Übermittlung von Leistungsdaten. An bestimmten Turnieren kann beispielsweise nur teilgenommen werden, wenn eine bestimmte Leistung erbracht wurde. Persönliche Daten in Form von Bestzeiten, Gewicht, Name, Adresse usw. werden erfasst. Die damit verbundene regelmäßige Übertragung der Daten (zum Beispiel zu anderen Vereinen, Leistungsportalen, Dachverbänden) bedarf einer besonderen Rechtsgrundlage.
- **Personalverwaltung**
  Dies ist eine besondere Form der Verarbeitung personenbezogener Daten, die der Verein vornimmt, wenn auch Angestellte beschäftigt werden. Hier müssen auch bestimmte Daten, wie zum Beispiel Name, Kontoverbindung, Familienstand etc. erhoben werden. Hier handelt es sich um eine Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses nach § 26 BDSG-Neu.

ÜBERSICHT DES VERZEICHNISSES VON VERARBEITUNGSTÄTIGKEITEN

Nummer	Bezeichnung des Verfahrens *(Wie lautet das Verfahren?)*	Kurzbeschreibung des Verfahrens *(Was ist der Zweck und wie wird etwas gemacht?)*	Fachlicher Ansprechpartner /Prozessverant-wortlicher *(Wer kann zu dem Verfahren etwas sagen bzw. verantwortet dieses?)*	Gruppe betroffener Personen *(Welche Personen-gruppen sind betroffen?)*	Welche personenbezogenen Daten werden verabeitet?	Was ist die Quelle/Herkunft der personenbezoge-nen Daten?	Rechtsgrundlage/ Einwilligung *(Was ist die Rechtgrundlage bzw. liegt eine Einwilligung vor?)*
Beispiel 1	TSV - 001	Mitgliedsantrag	Mustermann, Max	Neumitglieder	Bankdaten, Kontaktdaten, Identitätsdaten	Mitgliedsantrag	Einwilligung des Betroffenen
Beispiel 2	TSV – 002	Spielerliste Fußball	Trainer XY Fußball	Vereinsmitglieder	Kontaktdaten	Spielerliste	Einwilligung des Betroffenen

Zweckbestimmung *(Mit welchem Ziel werden die personenbezoge-nen Daten verarbeitet?)*	Mit welchen IT-Systemen erfolgt die Verarbeitung?	Werden die personenbezogenen Daten nach der Verarbeitung an eine dritte Stelle weitergegeben?	Besonderheiten, Bemerkungen etc.	Lösch-fristen
Mitglieder-betreuung	Verwaltungs-programm	ja	Fachverband	
Verwaltung Mannschaft	Excel	ja	Fachverband	

➔ Die Summe der Einzelbeiträge (Verarbeitungstätigkeiten/Geschäftsprozesse) ergibt das Verzeichnis von Verarbeitungstätigkeiten.

Datenweitergabe | Datenübermittlung

WEITERGABE UND ÜBERMITTLUNG VON DATEN

Die Weitergabe von Daten ist ein vereinsinterner Vorgang. Dieser stellt eine solche Nutzung dar und ist erlaubt

- seinen unselbständigen Untergliederungen
  (z.B. Ortsvereine oder Ortsgruppen eines überregionalen Vereins)

sowie seinen

- Funktionsträgern
- Auftragnehmern
- vom Verein beschäftigten Mitarbeitern,
  soweit diese im Rahmen der Aufgabenerfüllung für den Verein tätig werden

BEISPIELE ZUR DATENNUTZUNG IM VEREIN

Datenübermittlung von Mitgliederdaten

Die Datenweitergabe an **eigene Vereinsmitglieder ist eine Datenübermittlung i.S.d. § 3 Abs. 4 Satz 2 Nr. 3 BDSG und ist somit nicht ohne Einwilligung zulässig.**

Die Datenweitergabe an **einen Dachverband ist ebenso eine Datenübermittlung i.S.d. § 3 Abs. 4 Satz 2 Nr. 3 BDSG und ist somit nicht ohne Einwilligung zulässig.**

TOM | Die Technisch Organisatorischen Maßnahmen

TECHNISCH ORGANISATORISCHE MAßNAHMEN

Die **Dokumentationspflichten der Technisch Organisatorischen Maßnahmen –**
die Anlage gibt vor, in welchen Kategorien Schutzmaßnahmen sichergestellt sein müssen.

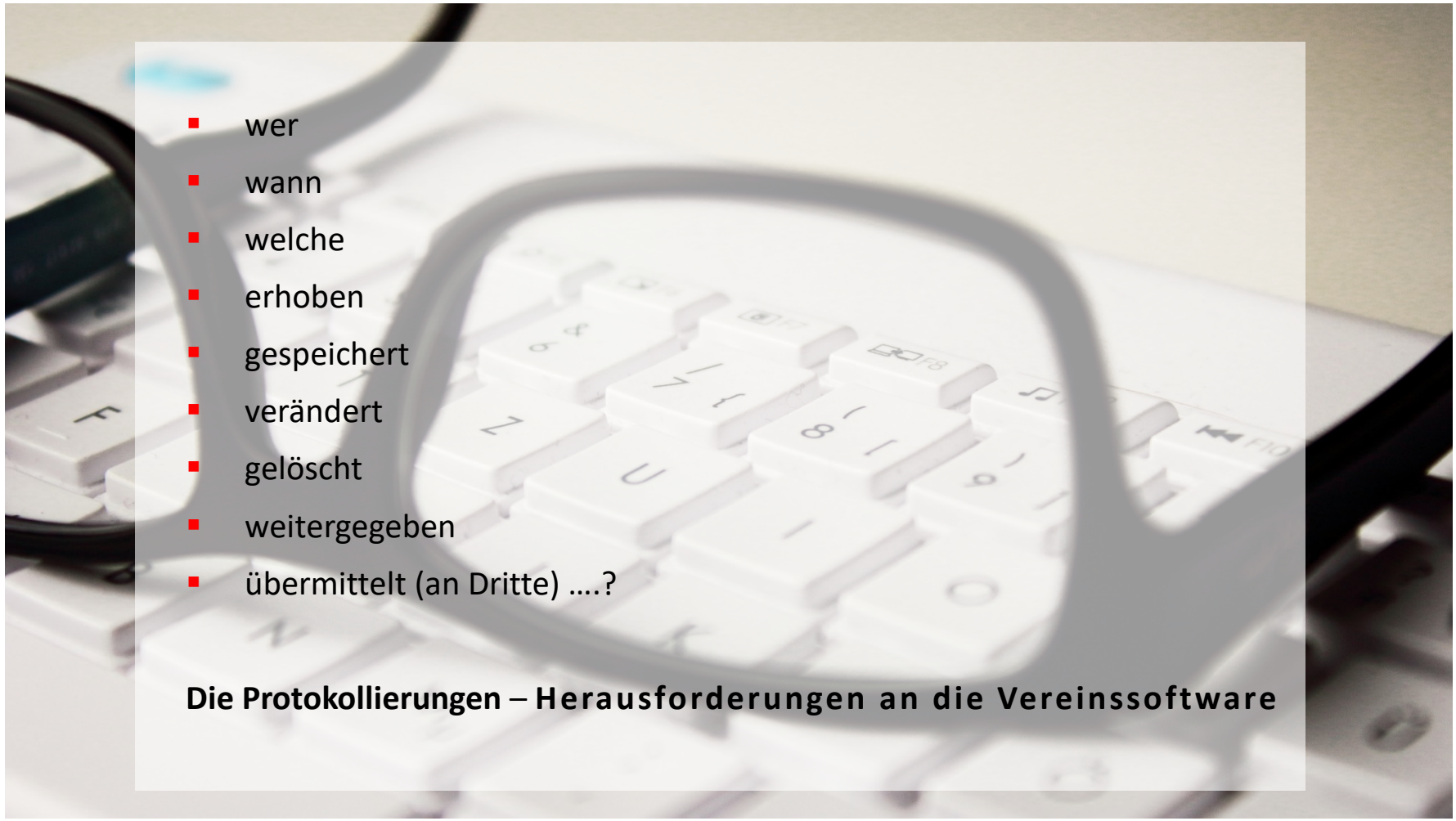
Den Verfahrensverzeichnissen müssen auch die notwendigen TOM zugeordnet werden:

- **Allgemeine Angaben zur verantwortlichen Stelle und dem Ansprechpartner für Datensicherheit**
- **Aufbau IT-Verbund | Struktur**
- **Zutrittskontrolle**
- **Zugangskontrolle**
- **Zugriffskontrolle**
- **Weitergabekontrolle**
- **Eingabekontrolle**
- **Auftragskontrolle**
- **Verfügbarkeitskontrolle**
- **Trennungsgebot**

Folgen bei Nichteinhaltung: Datenverarbeitung ist unzulässig (und Bußgelder)

KONTROLLE | PROTOKOLLIERUNGEN

Gibt es eine Kontrolle / Protokollierungen bei der Nutzung und Verarbeitung?



FRAGERUNDE

AUFTRAGSVERARBEITUNG | AV ART. 28 DSGVO

Ein Verein/Unternehmen (Auftraggeber) beauftragt externe Dienstleister (Auftragnehmer) weisungsgebunden personenbezogene Daten zu verarbeiten.

ART. 28 DSGVO AUFTRAGSVERARBEITUNG | AV

Charakteristisch für die Auftragsdatenverarbeitung ist,

- dass ein Verein/Unternehmen (Auftraggeber) externe Dienstleister (Auftragnehmer) damit beauftragt,
- weisungsgebunden personenbezogene Daten zu verarbeiten.

Die Verantwortung | der Hauptverantwortliche

- Der Auftraggeber ist für die ordnungsgemäße Datenverarbeitung verantwortlich.
- Der Auftraggeber ist und bleibt der Hauptverantwortliche für den Datenschutz.

Der externe Dienstleister wird bei der Auftragsdatenverarbeitung nur unterstützend tätig, er ist praktisch der **„verlängerte Arm“ seines Auftraggebers.**

WANN BESTEHT EINE NOTWENDIGKEIT?

Eine Auftragsdatenverarbeitung besteht **unter anderem in folgenden Fällen:**

Beispiele:

- Ein externes Rechenzentrum wird damit beauftragt, die Lohn- und Gehaltsabrechnung durchzuführen.
- Ein Call-Center erhebt Daten bei den Kunden des Auftraggebers.
- Eine Marketing-Agentur/Druckerei verarbeitet Kunden- und Mitgliederdaten, um Statistiken oder einen Newsletter/eine Vereinsbroschüre zu erstellen und zu versenden.

Die Auftragsverarbeitung umfasst auch nach der DSGVO zum Beispiel folgende Fälle:

- Ein Verein/Unternehmen beauftragt einen Programmierer mit der Installation, Pflege, Überprüfung und Korrektur von Software.
- Ein Verein/Unternehmen beauftragt einen IT-Dienstleister mit der Überprüfung, Reparatur oder dem Austausch von Hardware.
- Ein Verein/Unternehmen beauftragt einen externen Dienstleister mit der Aktenvernichtung.
- Die bloße Möglichkeit des Datenzugriffs durch den Auftragnehmer genügt dabei schon. Es kommt also nicht darauf an, ob der beauftragte Dienstleister tatsächlich auf die Daten zugreift.

WANN BESTEHT EINE NOTWENDIGKEIT?

Das bedeutet:

Sobald ein externer Dienstleister im Rahmen eines Auftrags irgendeine Möglichkeit hat, auf personenbezogene Daten zuzugreifen, sollte eingehend geprüft werden, ob die Vorschriften der Auftragsdatenverarbeitung Anwendung finden!

WANN LIEGT KEINE AV-NOTWENDIGKEIT VOR?

Keine Auftragsdatenverarbeitung liegt bei einer sogenannten Funktionsübertragung vor.

- **Achtung:** Dabei ist die genaue Abgrenzung von Auftragsdatenverarbeitung und Funktionsübertragung bei vielen Dienstleistungen nicht immer eindeutig.

- **Wichtig:** Man kann sich jedoch merken, dass der externe Dienstleister im Rahmen einer Funktionsübertragung **nicht weisungsgebunden ist**, sondern frei entscheiden kann, was mit den Daten des Unternehmens geschieht und ein eigenes Interesse an den Daten des Unternehmens hat.

- Eine Funktionsübertragung liegt somit bspw. vor, wenn ein Dienstleister für seinen Auftraggeber Dienstfahrzeuge anmietet oder ein Inkassounternehmen die Forderungen seines Auftraggebers durchsetzt.

DER HAUPTVERANTWORTLICHE

Müssen sich die externen Dienstleister nicht um den Datenschutz kümmern?

- Das beauftragende Unternehmen darf sich nicht darauf verlassen, dass der Dienstleister das Datenschutzrecht einhält.
- **Der Auftraggeber muss sich selbst um die Datensicherheit kümmern!**
- **Er ist der Hauptverantwortliche für den Datenschutz!**

WANN IST DER AV ABZUSCHLIEßEN?

Um der Verantwortung nach DSGVO und BDSG nachzukommen, müssen die Parteien

vor Beginn der Auftragsdatenverarbeitung einen Vertrag abschließen,

dessen Inhalt das Datenschutzrecht in Art. 28 DSGVO (vorher § 11 Abs. 2 Satz 2 BDSG) genau vorgibt.

Zudem muss der Auftraggeber in regelmäßigen Abständen kontrollieren, ob der Auftragnehmer die Vorgaben des Bundesdatenschutzgesetzes einhält.

Dazu kann er

- Vor-Ort-Kontrollen durchführen,
- das Testat eines Sachverständigen einholen,
- den Bericht des eigenen Datenschutzbeauftragten einholen oder
- eine schriftliche Auskunft des Auftragnehmers einholen.

Welche Maßnahme das beauftragende Unternehmen konkret ergreifen muss und in welchen zeitlichen Abständen Kontrollen durchzuführen sind, **lässt das Datenschutzgesetz offen.**

Maßgeblich sind insbesondere der Umfang der Datenverarbeitung, das Gefährdungspotenzial für die Betroffenen und die Sensibilität der verarbeiteten Daten.

MINDESTANFORDERUNGEN AV | ART. 28 DSGVO

Die in Art. 28 aufgeführten Mindestanforderungen müssen im AV-Vertrag enthalten sein, sie können und sollten einzelfallbezogen vertraglich ausgestaltet bzw. auf den jeweiligen Dienstleister und seine Tätigkeiten angepasst werden

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten, Kreis betroffener Personen
- Umfang der Weisungsbefugnisse
- Pflichten und Rechte des Verantwortlichen
- Pflichten des Auftragsverarbeiters:
- Verarbeitung nach dokumentierter Weisung,
- Wahrung der Vertraulichkeit bzw. Verschwiegenheit,
- Ergreifung geeigneter Maßnahmen für die eigene Sicherheit der Verarbeitung,
- Rechtmäßige Hinzuziehung von Subunternehmen,
- Unterstützung des Verantwortlichen bei der Beantwortung von Anträgen betroffener Personen,
- Unterstützung des Verantwortlichen bei der Einhaltung dessen Pflichten aus Art. 32 bis 36 DSGVO,
- Ergreifung geeigneter Maßnahmen für die Sicherheit der Verarbeitung (Art. 28 III 2 lit. f DS-GVO i.V.m. Art. 32 DSGVO),

MINDESTANFORDERUNGEN AV | ART. 28 DSGVO

- Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 28 III 2 lit. f DS-GVO i.V.m Art. 33 DS-GVO),
- Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Art. 28 III 2 lit. f DS-GVO i.V.m Art. 34 DS-GVO),
- Durchführung einer Datenschutz-Folgenabschätzung (Art. 28 III 2 lit. f DS-GVO i.V.m Art. 35 DS-GVO),
- Konsultierung der Aufsichtsbehörde bei Verarbeitung mit hohen Risiken (Art. 28 III 2 lit. f DS-GVO i.V.m Art. 36 DS-GVO).
- Löschung oder Rückgabe nach Beendigung des Auftrags,
- Zurverfügungstellung von Informationen und Ermöglichung von Überprüfungen
- **Wichtiger Bestandteil des Vertrages ist eine Anlage zu den technischen und organisatorischen Maßnahmen,** mit denen der Auftragnehmer Datensicherheit der ihm überlassenen Daten gewährleistet.

Vertrag über Auftragsverarbeitung
– Hauptvertrag- Generalvertrag
- Unterverträge für fallbasierende Themen generieren

Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DSGVO

GRUNDPRINZIPIEN DER DSGVO

Verpflichtung zur Verschwiegenheit | Datengeheimnis § 53 BDSG

- Mit Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis).
- Sie sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten.
- Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort.

Dabei stehen im Wesentlichen drei Ziele im Vordergrund:

- Bewusstsein für datenschutzrechtliche Probleme schaffen
- Mitarbeiter zu datenschutzkonformem Verhalten befähigen
- Bereitschaft zu datenschutzkonformem Verhalten fördern

WARUM IST DAS THEMA WICHTIG?

Studien zufolge werden **70 Prozent** aller Angriffe direkt über **Mitarbeiter/Personen ausgeführt**, z.B. (Phishing-Mail, Social-Engineering, persönliches Gespräch etc.)

Ihr Verhalten zählt!

Auch im KMU und Verein spielen Personen eine zentrale Rolle und damit auch personenbezogene Daten. Diese müssen geschützt werden!

GRUNDPRINZIPIEN DER DSGVO

Schulungen, die aus einem bestimmten Anlass heraus (z. B.Neueinstellung, Stellenwechsel) oder als Basis in regelmäßigen Zeitabständen angeboten werden sollen (z. B. jährlich).

- Grundschulungen und
- Schulungen zu speziellen Themen (Themenschulungen)

DEFINITION: BESCHÄFTIGTE/R IM VEREIN

- Beschäftigte im Sinne der DSGVO sind alle, die regelmäßig mit personenbezogenen Daten umgehen.
- unabhängig ihrer Bezahlung
- hierzu zählen auch Ehrenamtliche und Helfer

Was regelt die Datenschutz-Grundverordnung? | DSGVO für Beschäftigte

Nach Art. 29 DS-GVO dürfen Beschäftigte eines Verantwortlichen personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen oder Auftragsverarbeiters verarbeiten, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor.

Beispiele von Verantwortlichen:

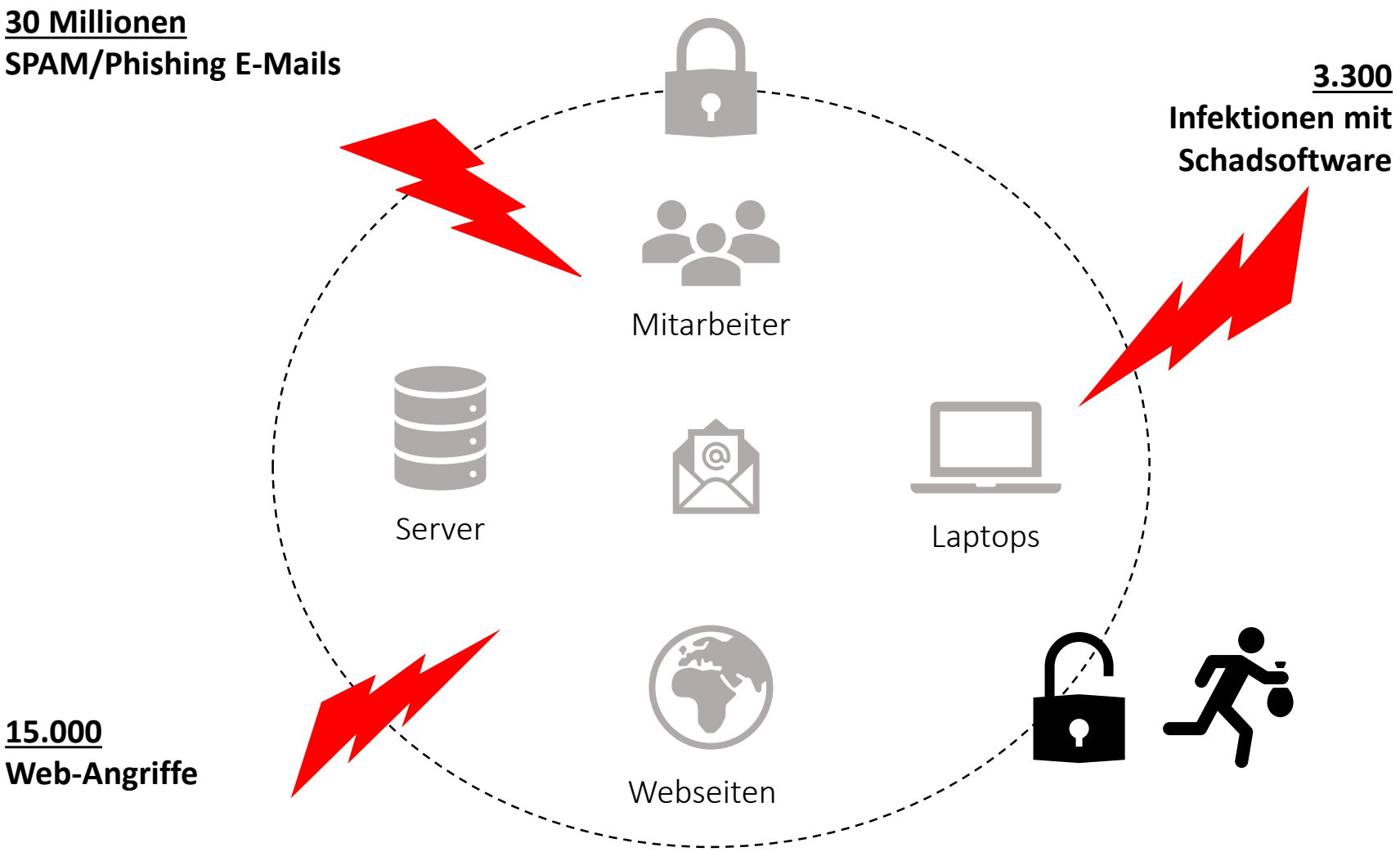
- Unternehmen
- Vereine
- Verbände
- Selbstständige
- Behörden
- Auftragsverarbeiter
- …

WAS REGELT DIE DATENSCHUTZ-GRUNDVERORDNUNG |DSGVO

- Der Verantwortliche bzw. der Auftragsverarbeiter wird durch Artikel 32 Abs. 4 verpflichtet, Schritte einzuleiten, die eben dies sicherstellen.
- Die explizite Verpflichtung zur Vertraulichkeit gilt für die Auftragsverarbeiter und ihre Beschäftigten (Artikel 28 Abs. 3 Satz 2 lit. b DSGVO).
- Diese Verpflichtung trifft inhaltlich aus den oben genannten Gründen auch auf verantwortliche Unternehmen und ihre Beschäftigten zu.

WARUM DATENGEHEIMNIS

Erkannte Sicherheitsvorfälle **pro Monat** eines Welt-Konzerns:

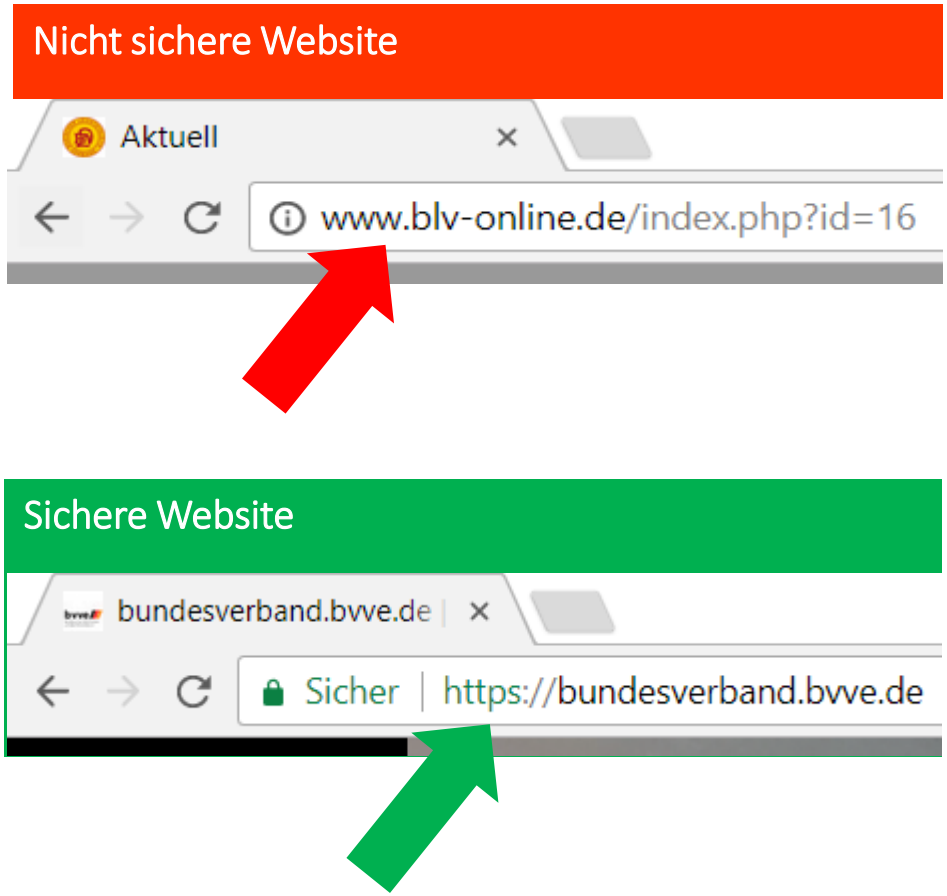


IMPRESSUM | DATENSCHUTZERKLÄRUNG

- Impressum
- Datenschutzerklärung
- E-Mail-Verkehr

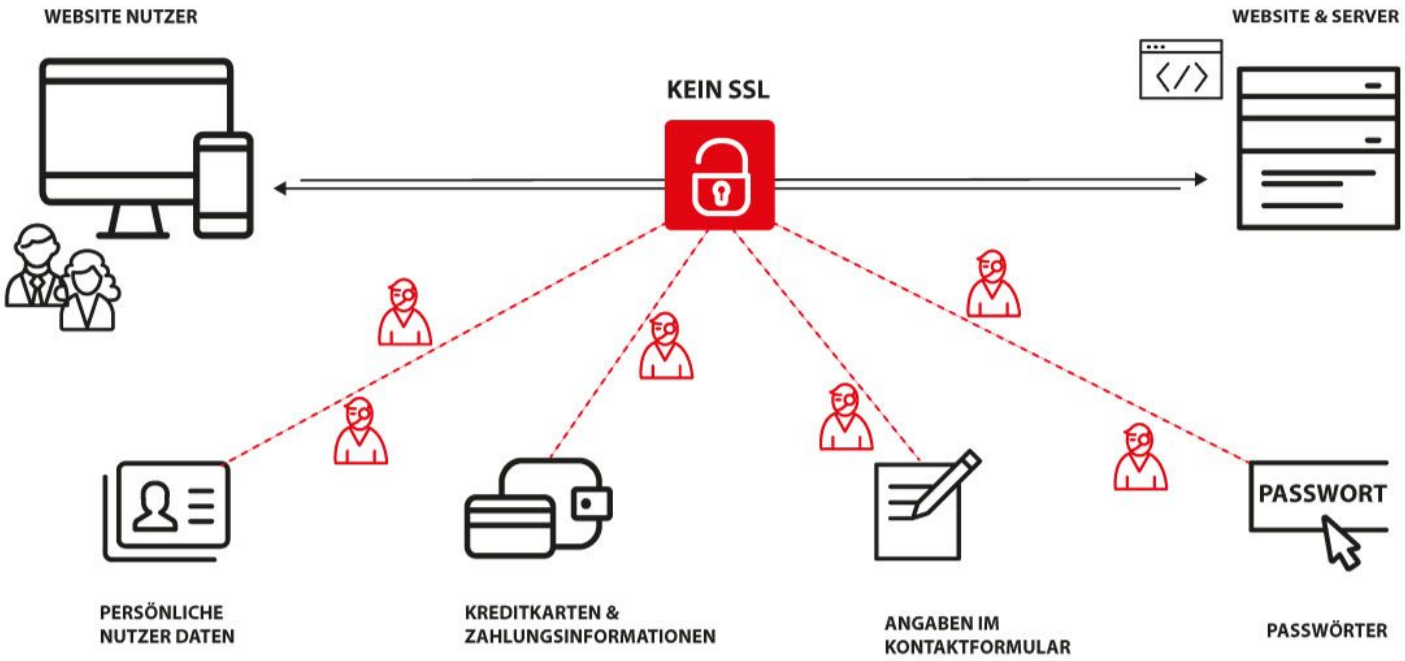
VERPFLICHTUNG ZU SICHEREN WEBSEITEN

SSL oder TLS für Webseiten nachrüsten!



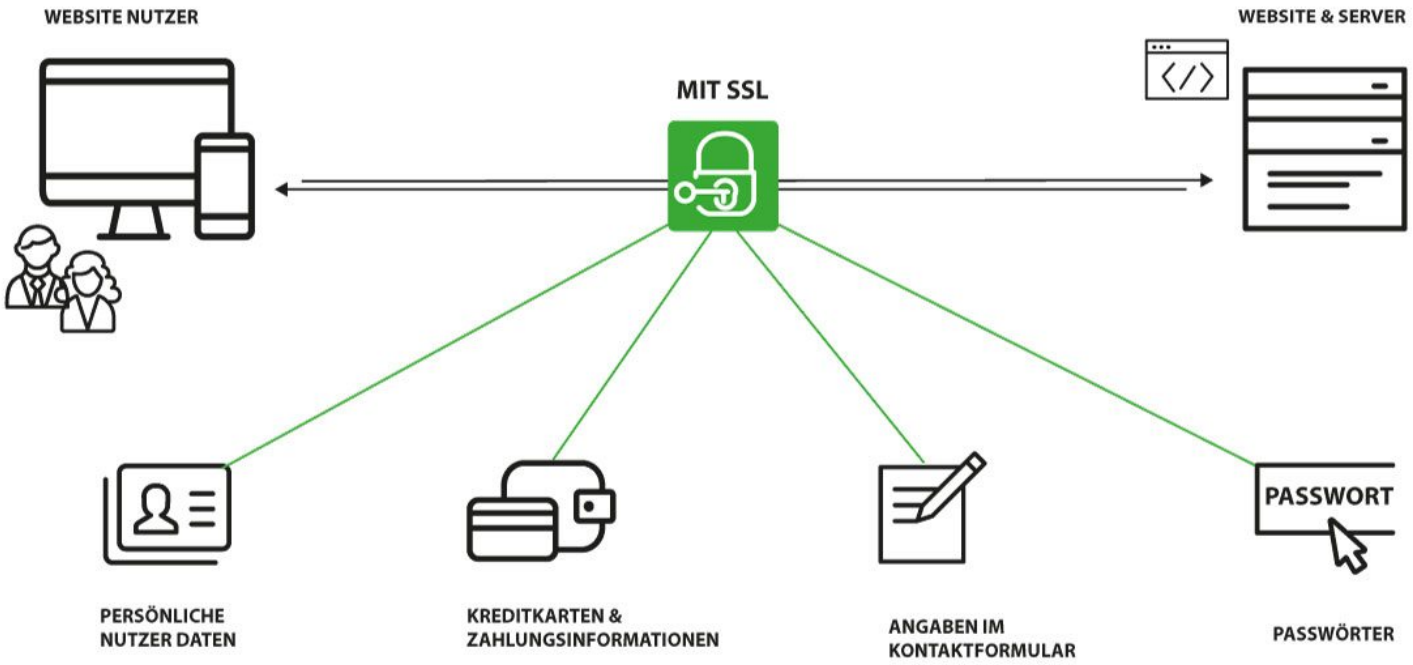
VERPFLICHTUNG ZUR VERSCHLÜSSELUNG | WEBSITE

Problem bei unverschlüsselte Websites:
Alle Daten und Informationen können von Dritten gelesen werden



VERPFLICHTUNG ZUR VERSCHLÜSSELUNG | WEBSITE

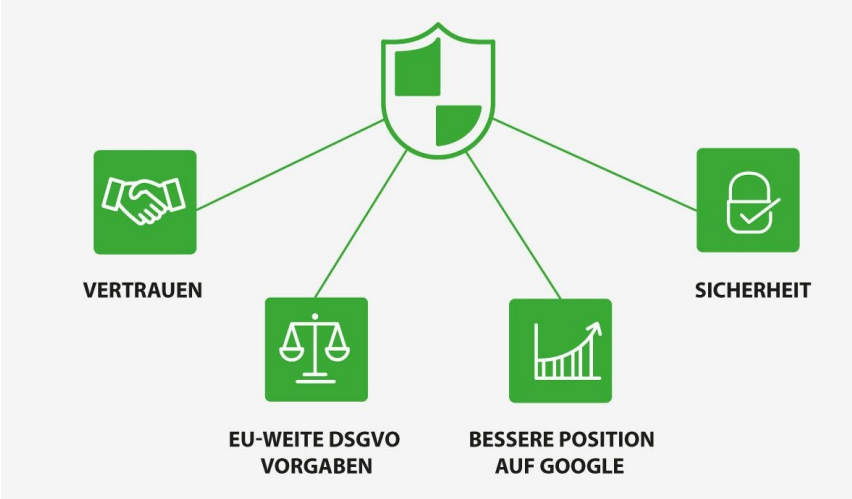
Vorteil der verschlüsselte Website:
Alle Daten und Informationen Ihrer Besucher werden geschützt



VERPFLICHTUNG ZUR VERSCHLÜSSELUNG | WEBSITE

Vorteile der SSL TLS Zertifikatverschlüsselung zusammengefasst

- Besseres Google-Ranking durch HTTPS-/SSL-Verschlüsselung
- Vollautomatische Einbindung der Zertifikate
- Höchste Vertrauenswürdigkeit durch optionale Inhaber-Validierung
- Extended SSL durch grüne Browser-Adresszeile hervorgehoben
- Sichere Verbindung mit bis zu 256-Bit-Verschlüsselung durch AES
- Einbindung auf beliebig vielen externen Servern möglich



RECHTSGRUNDLAGEN HOMEPAGE

Rechtsgrundlagen | aktuell | Impressum

Bundesdatenschutzgesetz | BDSG und Telemediengesetz – TMG regeln die rechtlichen Rahmenbedingungen für sogenannte Telemedien in Deutschland und sind **zentrale Vorschriften des Internetrechts**, z.B. Impressum für Telemediendienste u.a.

Die Informationspflichten gem. § 5 ff. TMG
im Unternehmen, in der Stiftung, im Verein, im Verband…

- Aufführen aller vertretungsberechtigter Vorstandsmitglieder im Sinne des § 26 BGB
- Amtsgericht/HRB oder Vereinsregister, USt-ID (wenn vorhanden)
- Adresse, Telefon, E-Mail
  Fax (nicht zwingend), Internet
- bei Bedarf Aufsichtsbehörde(n) für (genehmigungspflichtige Dienstleistung),
  z.B. Landkreis/Behörde XX
- bei Publikationen wie News oder redaktionellen Beiträgen:
  Benennung des inhaltlich Verantwortlichen für den redaktionellen Teil nach
  § 55 Abs. 2 RStV (Rundfunkt-Staatsvertrag)

MINDESTINHALTE DER DATENSCHUTZERKLÄRUNG

Welche Anforderungen stellt § 13 TMG aktuell an Websitebetreiber?

Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über

- Art
- Umfang und
- Zwecke

der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG […] in allgemein verständlicher Form zu unterrichten.

MINDESTINHALTE DER DATENSCHUTZERKLÄRUNG

Die Datenschutzerklärung soll Nutzer ausführlich darüber informieren,

- ob und in welcher Form die Erhebung personenbezogener oder anderer sensibler Daten auf der Webseite erfolgt | Art. 12 EU-DSGVO

Webseiten mit Informationen für Kinder:

- wenn sich die Verarbeitung an Kinder richtet, sollten aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in **einer kindgerechten Sprache erfolgen**.

Deshalb muss beachtet werden:

- Nutzer haben das Recht, dies unmittelbar auf der Website nachlesen zu können.
- Ebenso sind die Anforderungen nach § 13 TMG an Websitebetreiber zu beachten.

Wichtig: Die Datenschutzerklärung muss individuell auf das jeweilige Unternehmen| den Verein angepasst sein.

MINDESTINHALTE DER DATENSCHUTZERKLÄRUNG

- Hieraus leiten sich ab die **weiteren Verpflichtungen** zur Information zu:
  - Cookie-Verwendung
  - Registrierung für Kunden
  - Newsletters-Abo
  - Kontaktformular
  - Blog oder redaktionelle Artikel
  - Online-Bewerbungsmöglichkeiten (auch per E-Mail).

- **Datenschutzbeauftragter (DSB)** –
  Erklärungen zum DSB
- **Soziale Medien –**
  Verbindungen zu sozialen Medien, z.B. Facebook | Google+ | Instagram |LinkedIn | Myspace| Pinterest …
- **Analyse Tools** –
  Angabe zur Nutzung von Analyse-Tools (z.B. Überwachung von Besucherströmen)
- **Internetwerbung** –
  Datenschutzerklärungen der genutzten Internetwerbedienste (z.B. Google AdWords)

MINDESTINHALTE DER DATENSCHUTZERKLÄRUNG

- **Online-Marketing** – Nennung der Anbieter und Dienste im Online-Marketing
- **WordPress Plugins** – Nennung der benutzen Plugins
- **Zahlungsmöglichkeiten** – Nennung der Drittanbieter für Zahlungsabwicklungen
- **Sonstiges** – Nutzung sonstiger Dienste, z.B. Amazon Partnerprogramm
- Sonstige Informationspflichten, wenn erforderlich, z.B. Widerrufs- bzw. Rückgaberecht, Preisangabenverordnung, Wohnraumvermittlungsgesetz

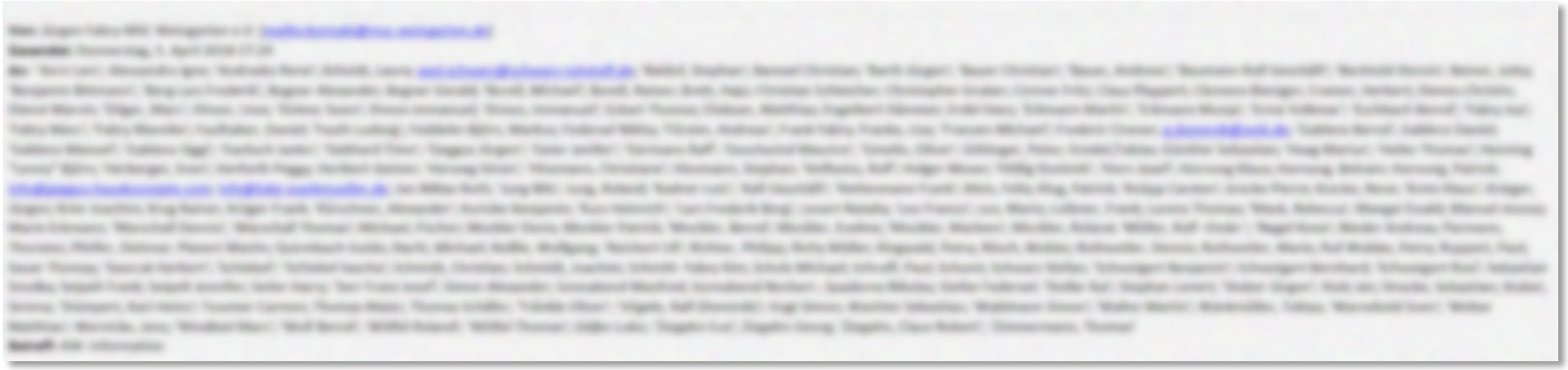
Wichtig: Personenbezogene Daten der Nutzer dürfen von dem Anbieter nur erhoben und verwendet werden, wenn dies das TMG oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, erlaubt oder der Nutzer eingewilligt hat.

E-Mail-Verkehr

E-MAIL AN MEHRERE EMPFÄNGER

CC oder BCC?

In der Praxis zeigt sich häufig ein Problem bei der Nutzung von E-Mails.



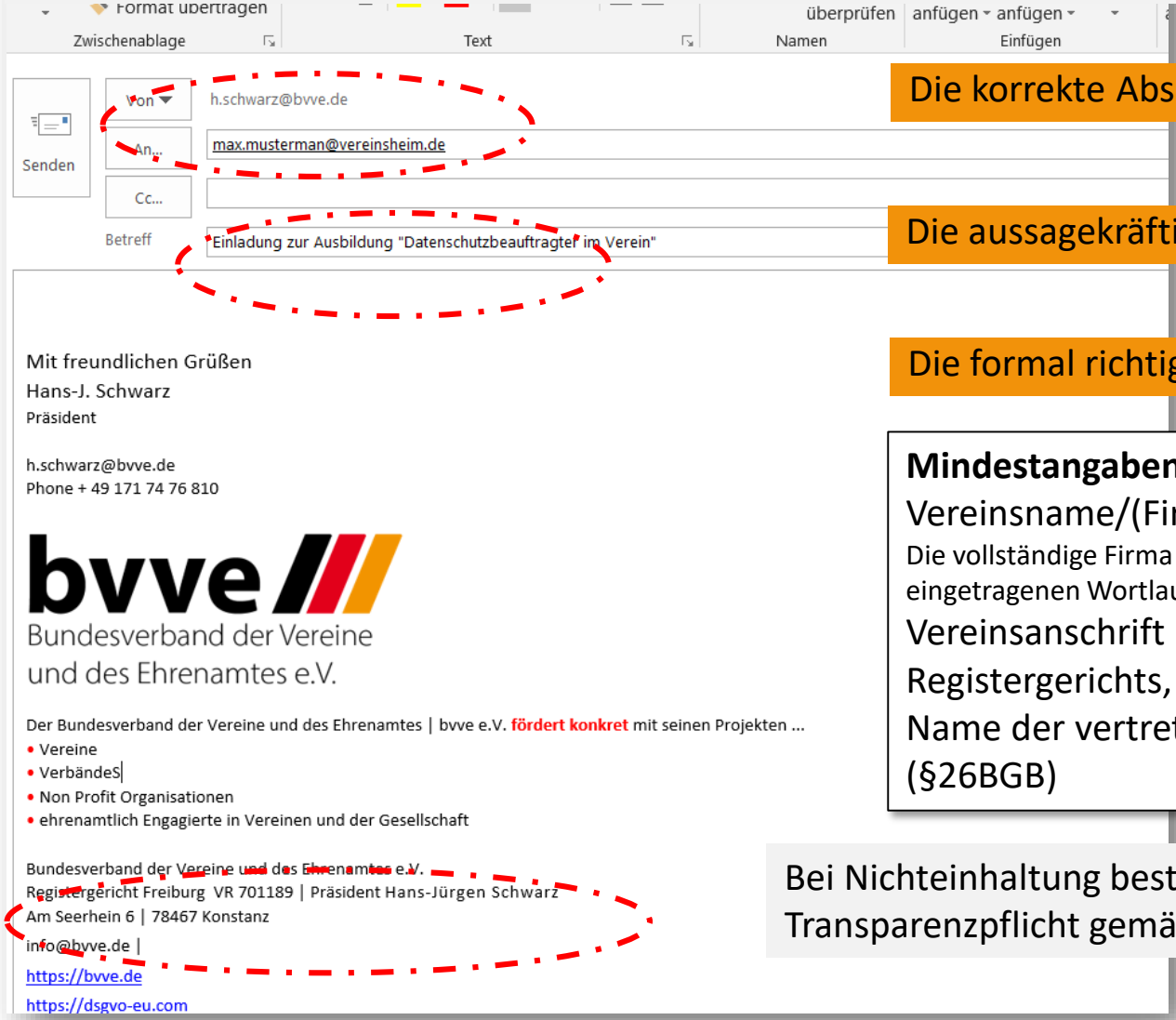
Die Versendung von E-Mails, in denen im Empfängerfeld andere Empfänger sichtbar sind, ist unzulässig!

→ Kopien oder Serienempfänger ausschließlich und immer im BCC!
Es steht jedem Verein frei, dies intern grundlegend – ggf. in der Satzung – zu regeln oder besser in der Kommunikationsordnung als Ergänzung zur Satzung.

E-MAIL-VERKEHR IM VEREIN

In dem Moment, in dem ein Organträger eines e.V. eine E-Mail versendet, handelt es sich gegebenenfalls nicht mehr um eine Privat-E-Mail, sondern um einen Geschäftsbrief, der nach § 37a HGB die üblichen Pflichtangaben enthalten muss.

Die richtige E-Mail enthält deshalb drei unentbehrliche Teile:



Die korrekte Absender-Adresse

Die aussagekräftige Betreffzeile

Die formal richtige Signatur

Mindestangaben

Vereinsname/(Firma)

Die vollständige Firma (in Übereinstimmung mit dem im Handelsregister eingetragenen Wortlaut)

Vereinsanschrift (ladungsfähig)

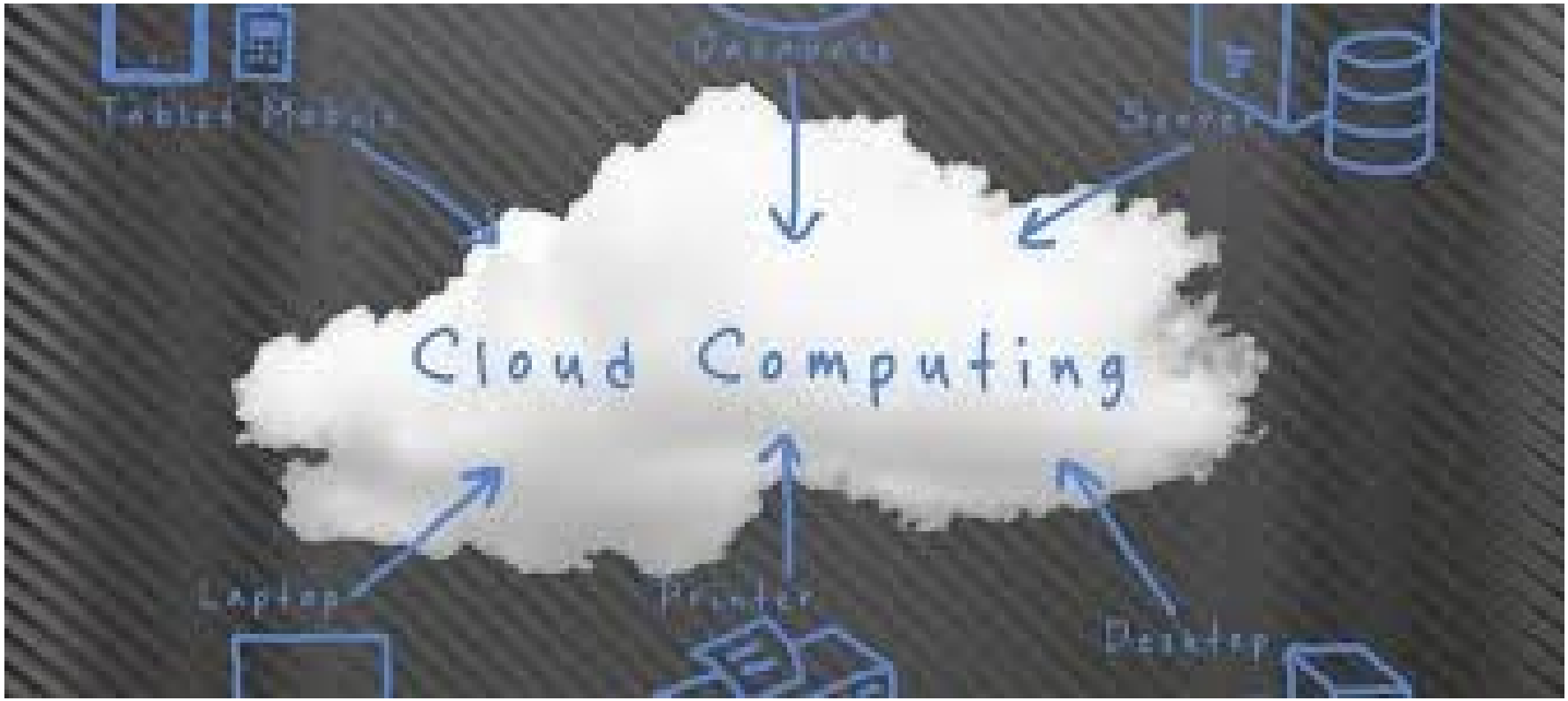
Registergerichts, Registernummer und

Name der vertretungsberechtigten Vorstände (§26BGB)

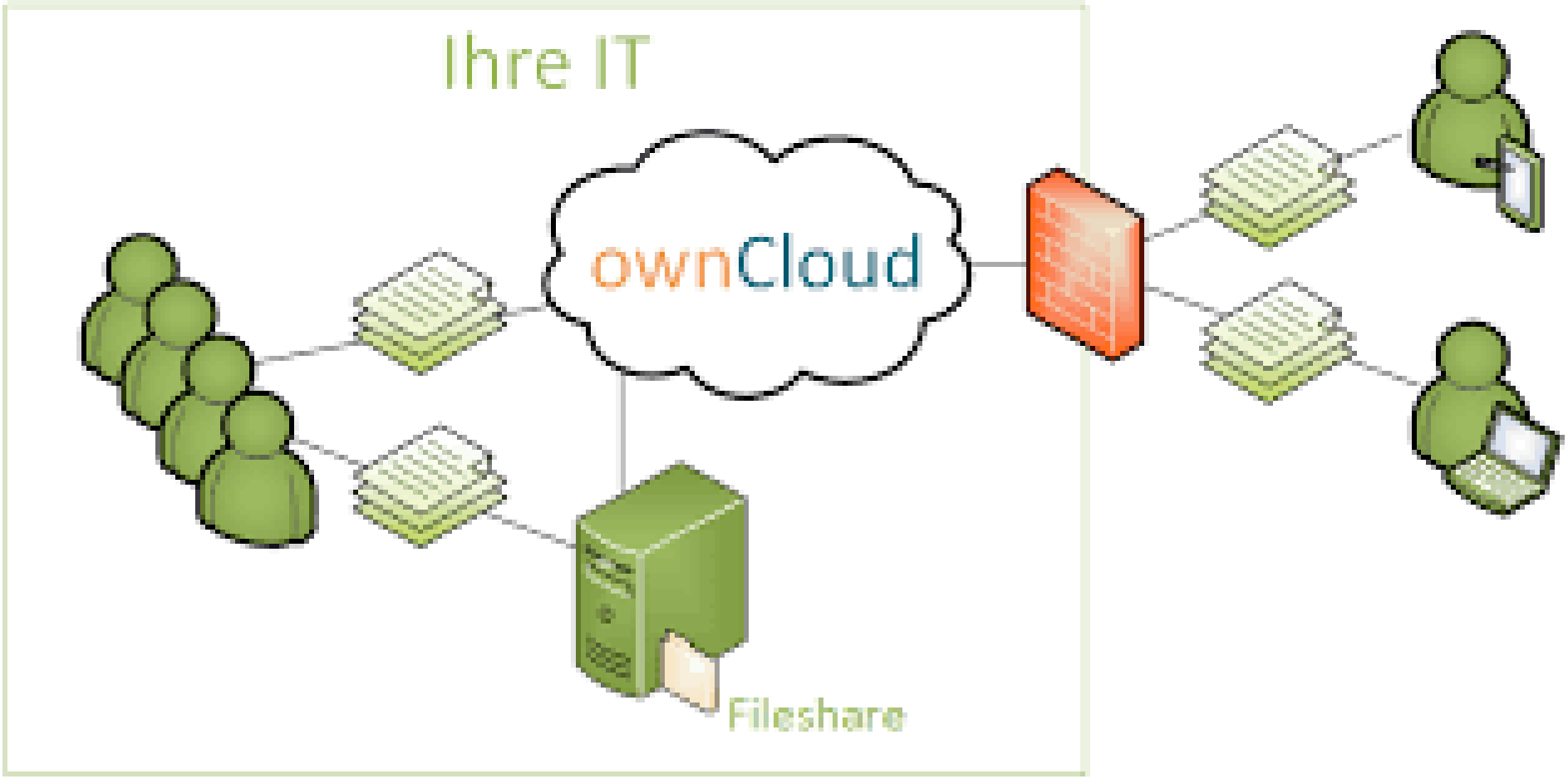
Bei Nichteinhaltung besteht eventuell ein Verstoß gegen die Transparenzpflicht gemäß § 6 des Telemediengesetzes (TMG).

CLOUD COMPUTING

Filesharing und zentrale Verwaltung in der Cloud



OWNCLOUD IM VEREIN



AUSKUNFTSERSUCHEN

BSP. ANFRAGE

Sehr geehrte Damen und Herren,

hiermit erbitte ich von Ihnen gemäß Artikel 15 Absatz 1 DS-GVO
unentgeltliche und schriftliche Auskunft, ob Sie mich betreffende personenbezogene Daten verarbeiten (Definition des Begriffs „Verarbeitung“ siehe Art. 4 Nr. 2 DS-GVO).

Falls ja, schließe ich folgende Fragen an:

1. Welche mich betreffenden personenbezogenen Daten verarbeiten Sie?

2. Zu welchem Zweck (welchen Zwecken) verarbeiten Sie diese Daten?

3. Woher stammen diese mich betreffenden Daten?

4. Haben Sie diese Daten an Dritte übermittelt oder planen Sie, diese an Dritte zu übermitteln?
Wenn ja, an wen, wann und zu welchem Zweck (welchen Zwecken)?

5. Wie lange werden Sie meine Daten verarbeiten (Stichwort Datenlöschkonzeption)?

6. Haben Sie hinsichtlich meiner Person ein Profil angelegt? Falls ja, teilen Sie mir den Inhalt dieses Profils und die Art und Weise des Zustandekommens dieses Profils bitte mit.

7. Welchen aktuellen Scorewert übermitteln Sie hinsichtlich meiner Person und welche genaue Bedeutung hat dieser Scorewert?

8. An wen haben Sie meinen Scorewert in den letzten 12 Monaten übermittelt? Welche einzelnen Daten liegen dieser Scorewertberechnung zugrunde?

9. Woher haben Sie diese Daten?

10. Verarbeiten Sie die mich betreffenden Daten mithilfe einer weiteren automatisierten Entscheidungsfindung?

Falls ja, erläutern Sie bitte mit aussagekräftigen Informationen die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen des bzw. der eingesetzten Verfahren.

Ihre schriftliche Stellungnahme per Briefpost erwarte ich unverzüglich, spätestens aber innerhalb eines Monats (§ 12 Abs. 3 DS-GVO) nach Eingang dieses Schreibens.

Vielen Dank im Voraus.

Mit freundlichen Grüßen

AUSKUNFTSANFRAGE BEARBEITEN

In 7 Schritten auf ein Auskunftsersuchen reagieren

Wann muss Auskunft erteilt werden - relevante Schritte:

1. Identität des Antragstellers überprüfen

Ist der Antragsteller überhaupt die Person, die er vorgibt zu sein …

2. Verarbeiten Sie überhaupt Daten des Antragstellers?

Wenn nein, muss eine Negativauskunft erteilt werden Diese könnte wie folgt aussehen:

Sehr geehrter Herr Mustermann,

mit Ausnahme der Daten, die Sie uns im Zusammenhang mit Ihrem Auskunftsersuchen übermittelt haben, haben wir keine personenbezogenen Daten zu Ihrer Person gespeichert.

Unsere Hinweise zum Datenschutz finden Sie hier (Link ergänzen).

AUSKUNFTSANFRAGE BEARBEITEN

In 7 Schritten auf ein Auskunftsersuchen reagieren

3. Ist das Auskunftsrecht ausnahmsweise ausgeschlossen?

Dies könnte sein bei:

in Fällen der Datenverarbeitung zu wissenschaftlichen, historischen oder statistischen Zwecken (§ 27), zu im öffentlichen Interesse liegenden Archivzwecken (§ 28) und um Datenverarbeitungen durch Berufsgeheimnisträger.

4. Welche Informationen müssen erteilt werden?

Die Auskunftspflicht beschränkt sich natürlich auf personenbezogene Daten. Darunter fallen auch pseudonyme Daten, sofern der Personenbezug nicht gänzlich ausgeschlossen ist (anonymisierte Daten).

Zudem muss die Auskunft die in Artikel 15 DSGVO genannten Informationen enthalten.

5. Wie viel Zeit bleibt für die Beantwortung?

Die Auskunft muss unverzüglich erfolgen. In der Praxis bedeutet dies, dass Sie wohl bis zu einem Monat Zeit dafür haben. Länger darf es nur in besonderen Fällen dauern.

AUSKUNFTSANFRAGE BEARBEITEN

In 7 Schritten auf ein Auskunftsersuchen reagieren

6. Wie muss ich die Auskunft erteilen?

Die DSGVO enthält keine besonderen Formvorschriften für die Auskunftserteilung.
Jedes Unternehmen / Verein kann also eine individuelle Formulierung verwenden.

Zwingend vorgeschrieben – die Auskunft muss in

- in transparenter,
- verständlicher und
- leicht zugänglicher Form und in
- einer klaren und einfachen Sprache verfassen,

sodass auch ein Laie sie verstehen kann.

Sie können die Auskunft schriftlich, per E-Mail oder auf andere Weise erteilen.
In der Regel sollte sie so erteilt werden, wie das Auskunftsersuchen erstellt wurde.
Es sei denn, der Antragsteller verlangt einen anderen Weg.

Bitte beachten: Der Antragsteller kann auch eine mündliche Auskunftserteilung verlangen!

AUSKUNFTSANFRAGE BEARBEITEN

In 7 Schritten auf ein Auskunftsersuchen reagieren

7. Was geschieht mit den durch das Auskunftsersuchen übermittelten Daten?

Um Ihre Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO zu entsprechen und um sich verteidigen zu können, falls im späteren Verlauf die Aufsichtsbehörde eingeschaltet wird, sollten Sie das Auskunftsersuchen sowie Ihre Antwort darauf speichern.

Es ist ratsam, diese Daten 3 Jahre lang aufzubewahren. Denn dann ist eine eventuelle Verletzung von Betroffenenrechten gemäß § 31 OWiG verjährt. Dieser Paragraf ist mangels Verjährungsregelungen in der DSGVO anwendbar.

ART. 15 DSGVO | AUSKUNFTSRECHT …

1. Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

a) die Verarbeitungszwecke;

b) die Kategorien personenbezogener Daten, die verarbeitet werden;

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

ART. 15 DSGVO | AUSKUNFTSRECHT …

2. Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

3. 1Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. 2Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. 3Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

4. Das Recht auf Erhalt einer Kopie gemäß Absatz 3 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Alle diese einzelnen Punkte müssen beantwortet werden.

Passende Erwägungsgründe

(63) Auskunftsrecht (64) Identitätsprüfung

Passende Paragraphen des BDSG

§ 27 BDSG Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken § 28 BDSG Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken § 29 BDSG Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten § 30 BDSG Verbraucherkredite § 34 BDSG Auskunftsrecht der betroffenen Person

T

CHECKLISTE DOKUMENTATION

Status des Datenschuzes Stand anhand der Checkliste Übergabestatuzs

MAßNAHMEN IM VEREIN

- **Einwilligungen anpassen**
- **Erfüllung von Informationspflichten**
  Information, ob Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben ist
  und ob sie für den Vertragsschluss erforderlich sind
- **Einwilligungserklärungen | Betroffenenrechte sicherstellen**(Art. 13 und 14 DSGVO)
- **Auftragsverarbeitung durch Dritte** (Art. 28 DSGVO)
- **Erstellung der Verzeichnisse der Verarbeitungstätigkeiten (Art. 30 DSGVO)**
- **Datenschutzfolgenabschätzung (Art. 35 DSGVO)**
- **Datenschutzbeauftragten ernennen**, wenn notwendig (DPO) (Art. 37 DSGVO)
- **Satzung | Datenschutzrichtlinie**
- **TOM –** Technisch Organisatorische Maßnahmen in Datenverarbeitung und IT
- **Meldepflicht bei Datenpannen** (Art. 4, Abs. 12 + Art. 33 DSGVO)
- **Datenschutzmanagementsystem | DSM zur Erfüllung der Dokumentationspflichten inkl. Richtlinien und Vorgaben und Notfallplänen**
- **Kontrollen**
- **Verpflichtung auf die Verschwiegenheit – Datengeheimnisverpflichtung und Unterweisung | Schulung nach Art. 5 (Rechenschaftspflicht), Art. 24 Abs. 1 DS-GVO) (Sicherstellung der Einhaltung der DSGVO) Art. 29 DS-GVO (Weisung) Art. 32 Abs. 4 DS-GVO (Sicherstellung)**

WELCHE DOKUMENTATIONEN UND VERPFLICHTUNGEN

SIND VORHANDEN BZW. DURCHGEFÜHRT:

Ihr Score

[ ] Impressum Website – geprüft | angepasst _____
[ ] Datenschutzerklärung Website – vorhanden _____
[ ] E-Mail Verkehr – geprüft | angepasst _____
[ ]Homeoffice der Ehrenamtlichen _____
[ ]Trennung der Daten auf PCs der Ehrenamtlichen nach Verein und Privat | TOM _____

[ ] Satzung – Datenschutzrichtline – geprüft | angepasst | vorhanden _____

[ ] Rechtmäßigkeit der Datenerhebung – geprüft | angepasst _____
Gesetzliche Grundlagen
[ ] Betroffenenrechte und Informationspflichten – geprüft | angepasst _____
[ ] Einwilligungen u. Widerrufe – geprüft | angepasst _____
[ ] Einwilligungen u. rechtl. Grundlagen für
Fotoaufnahmen u. Veröffentlichungen – geprüft | angepasst _____

WELCHE DOKUMENTATIONEN UND VERPFLICHTUNGEN

SIND VORHANDEN BZW. DURCHGEFÜHRT:

[ ] Verpflichtungserklärung Verschwiegenheit der Beschäftigten _____
[ ] Schulung zur Verschwiegenheit der Beschäftigten _____
[ ] Mitarbeiterverhaltensrichtlinie (Internet, Telefon, Counter) _____

[ ] Datenschutzbeauftragter Notwendigkeit – geprüft
- [ ] mehr als 9 Beschäftigte nach Art. 37 DSGVO – geprüft _____
- [ ] Verarbeitung personenbezogen Daten nach Art. 9 – geprüft _____
- [ ] Datenschutzfolgeabschätzungsverpflichtung nach Art. 35 – geprüft _____

[ ] Datenschutzbeauftragter – bestellt weil notwendig _____

[ ] Verträge zur Auftragsverarbeitung durch Dritte _____
[ ] Verzeichnis der Verarbeitungstätigkeiten – erstellt | geprüft _____
[ ] Übersicht der technischen und organisatorischen Maßnahmen (TOM) _____

WELCHE DOKUMENTATIONEN UND VERPFLICHTUNGEN

SIND VORHANDEN BZW. DURCHGEFÜHRT:

[ ] Berechtigungskonzept | Trennungsgebot _____
[ ] Löschkonzept – geprüft | angepasst | vorhanden _____
[ ] Auskunftskonzept – geprüft | angepasst | vorhanden _____
[ ] Kontrollkonzept – geprüft | angepasst | vorhanden _____
[ ] Datenpannen Meldekonzept – geprüft | angepasst | vorhanden _____
[ ] IT-Sicherheitskonzept – geprüft | angepasst | vorhanden _____
[ ] BackUp Konzept – geprüft | angepasst | vorhanden _____

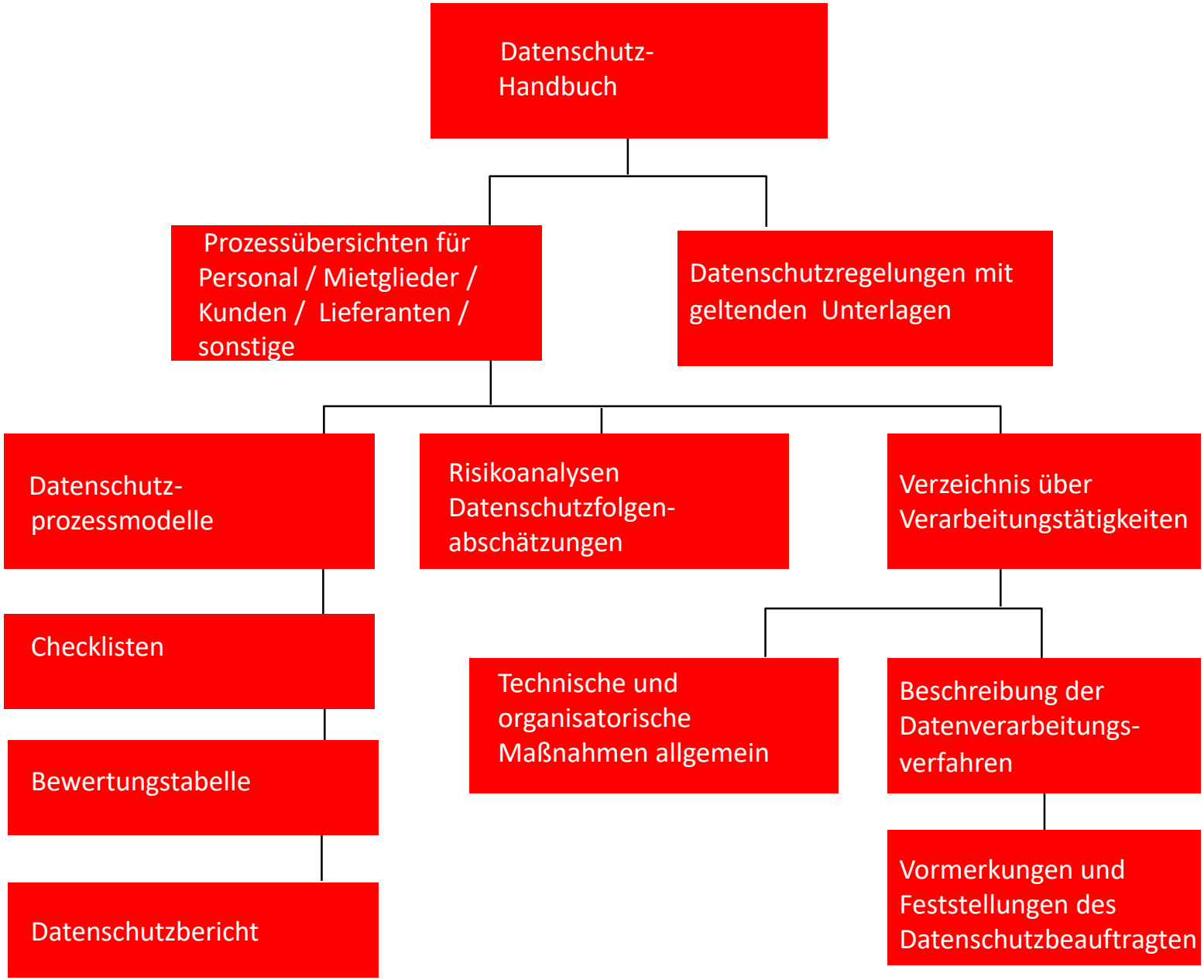
[ ] Datenschutzmanagementsystem – vorhanden _____

[ ] Sonstige Dokumentationen – wenn ja, welche _____

Download Checkliste
https://bundesverband.bvve.de/wp-content/uploads/2018/10/DSIV-DSGVO-Checkliste-Verpflichtungen-Dokumantationen.pdf

DATENSCHUTZHANDBUCH | DATENSCHUTZMANAGMENTSYSTEM

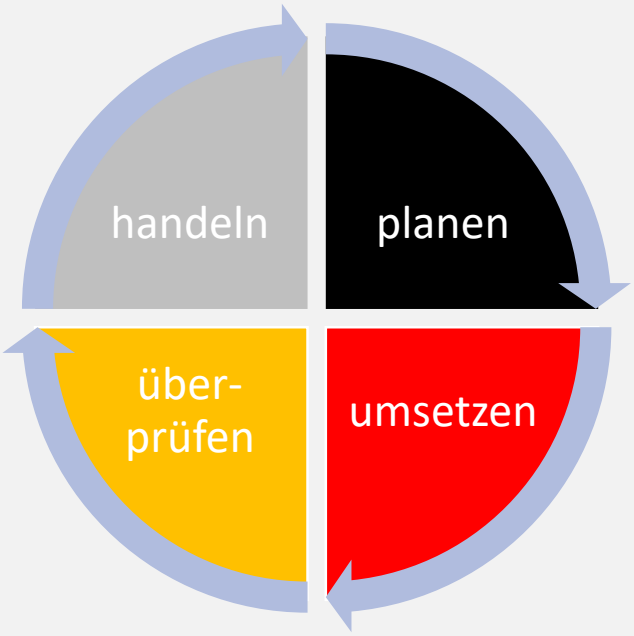
DAS DATENSCHUTZHANDBUCH



DATENSCHUTZMANAGEMENTSYSTEM | AUFBAU

Die Datenschutz Grundverordnung verlangt den Aufbau und Durchführung eines Datenschutzmanagementsystems für eine kontinuierliche Überarbeitung und Kontrolle der Verfahrensprozesse zum Schutz personenbezogener Daten (Datenschutz Compliance Management System).

- Einrichtung eines Dokumentationssystems |Datenschutzrichtlinie
- Festlegen von Prüfzyklen
  Klassischer P-D-C-A* Zyklus wie bei anderen Systemen
- Verantwortlichkeit und Datenschutzorganisation
  (Zuständigkeit - Ansprechpartner)
- Verzeichnis von Verarbeitungstätigkeiten
- Datenschutz-Folgenabschätzung
- Verzeichnis Vertragsmanagement
  (Auftragsdatenverarbeitung)
- Verpflichtungserklärungen auf das Datengeheimnis der Mitarbeiter
- Datenschutz-Schulung der Mitarbeiter
  - Nachweis der Durchführung
  - Dokumentation der Durchführung
- Sicherstellung der Anforderungen wie Meldepflicht und Auskunftsersuche



SCHUTZKLASSEN IN DER DATENVERNICHTUNG

Schutzklassen

Die DIN 66399 spezifiziert drei Schutzklassen, nach denen die Datenträger hinsichtlich ihrer Schutzbedürftigkeit einzuordnen sind:

Schutzklasse	Beschreibung
Schutzklasse 1 - normaler Bedarf für interne Daten	Der Schutz von personenbezogenen Daten muss gewährleistet sein. Andernfalls besteht die Gefahr, dass der Betroffene in seiner Stellung und seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.
Schutzklasse 2 - hoher Bedarf für vertrauliche Daten	Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt wird.
Schutzklasse 3 - sehr hoher Bedarf für besonders geheime Daten	Der Schutz personenbezogener Daten muss unbedingt gewährleistet sein. Andernfalls kann es zu einer Gefahr für Leib und Leben oder für die persönliche Freiheit des Betroffenen kommen.

SCHUTZKLASSEN UND SICHERHEITSSTUFEN NACH DIN 66399

Sicherheitsstufen:

Sicherheitsstufe	Datenträger-Vernichtungsempfehlung
1	Allgemeine Daten - Reproduktion mit einfachem Aufwand
2	Interne Daten - Reproduktion mit besonderem Aufwand
3	Sensible Daten - Reproduktion mit erheblichem Aufwand
4	Besonders sensible Daten - Reproduktion mit außergewöhnlichem Aufwand
5	Geheim zu haltene Daten - Reproduktion mit zweifelhaften Methoden
6	Geheime Hochsicherheitsdaten - Reproduktion technisch nicht möglich
7	Top Secret Hochsicherheitsdaten - Reproduktion ausgeschlossen

SCHUTZKLASSEN UND SICHERHEITSSTUFEN NACH DIN 66399

Zuordnung der Sicherheitsstufen zu den gewählten Schutzklassen

Jeder Schutzklasse können unterschiedliche Sicherheitsstufen zugeordnet werden, möglich sind jedoch nur folgende Kombinationen:

Datenträger der Schutzklasse 1 können den Sicherheitsstufen 1, 2 und 3 zugeordnet werden. Ausnahme: Handelt es sich um personenbezogene Daten, ist nur eine Zuordnung zur Sicherheitsstufe 3 erlaubt.

Datenträger der Schutzklasse 2 können den Sicherheitsstufen 3, 4 und 5 zugeordnet werden.

Datenträger der Schutzklasse 3 können den Sicherheitsstufen 4, 5, 6 und 7 zugeordnet werden.

SCHUTZKLASSEN UND SICHERHEITSSTUFEN NACH DIN 66399

Zuordnung der Sicherheitsstufen zu den gewählten Schutzklassen

Kürzel der Datenträgerart: Jede Datenträgerart ist durch ein Kürzel beschrieben (PFOTHE), welches der jeweiligen Sicherheitsstufe vorangestellt wird:

Kürzel	Datenträgerart
P	Informationsdarstellung in Originalgröße: Papier, Film, Druckformen
F	Informationsdarstellung verkleinert: Film, Mikrofilm, Folie
O	Informationsdarstellung auf optischen Datenträgern: CD, DVD
T	Informationsdarstellung auf magnetischen Datenträgern: Disketten, ID-Karten, Magnetbandkassetten
H	Informationsdarstellung auf Festplatten mit magnetischem Datenträger: Festplatten
E	Informationsdarstellung auf elektronischen Datenträgern: Speicherstick, Chipkarte, Halbleiterfestplatten, mobile Kommunikationsmittel

Anwendungsbeispiel

Bei Personaldaten/-akten ist die Schutzklasse 2 anzuwenden und die Datenträger der Sicherheitsstufe 4 zuzuordnen. Bei Papier ergibt sich somit die Sicherheitsstufe P-4, bei Festplatten

VIELEN DANK,

dass Sie da sind …

Bleiben Sie mit uns in Verbindung:
https://bvve.de

E-Mail: info@bvve.de

Fit-im-Ehrenamt.de
Eine Initiative im Bundesverband
der Vereine und des Ehrenamtes e.V.

bvve
Bundesverband der Vereine
und des Ehrenamtes e.V.

Wir bedanken uns bei unseren Förderern und Unterstützern, die durch ihr Engagement uns die Möglichkeit bieten, die Vereine und Ehrenamtlichen aktiv unterstützen.

GADE
Gesellschaft für angewandten
Datenschutz in Europa

