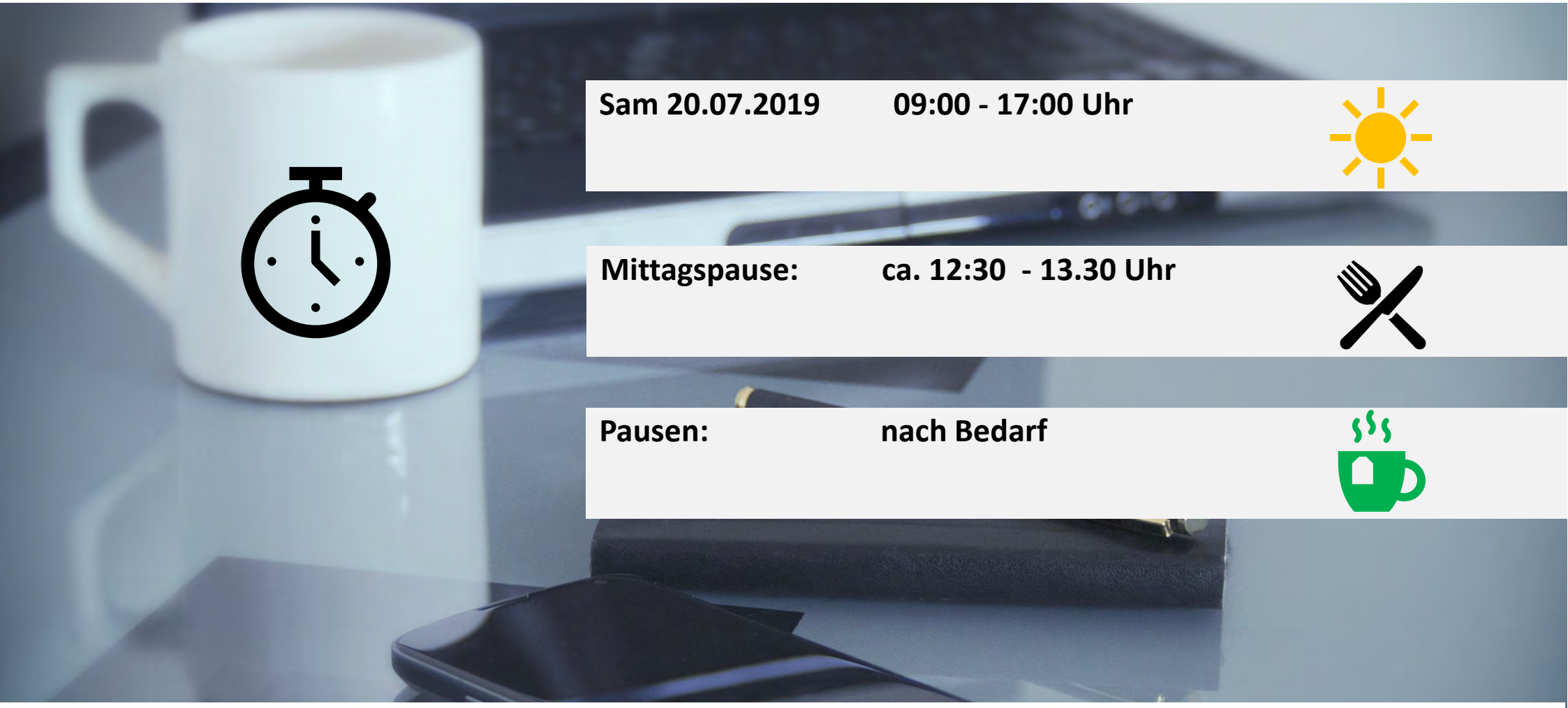
bvve
Bundesverband der Vereine
und des Ehrenamtes e.V.

Workshop „Datenschutz-Checkup“
Wo stehen wir heute?

Referent Hans-Jürgen Schwarz
Präsident des Bundesverbandes der
Vereine und des Ehrenamtes e.V. | bvve

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

ÜBERBLICK UND ORGA



Sam 20.07.2019	**09:00 - 17:00 Uhr**
Mittagspause:	**ca. 12:30 - 13.30 Uhr**
Pausen:	**nach Bedarf**

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 Daten-schutzgrundverordnung 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 Organi-satorische Maßnahmen
- Verfahrensverzeichnisse

WORKSHOPS

zur Umsetzung und Anwendung der DSGVO

UMSETZUNG, AUSBILDUNG UND WEITERBILDUNGEN

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

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

DIE HERAUSFORDERUNG

Informationspflichten


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

INFORMATIONSPFLICHTEN | DIE HERAUSFORDERUNG

Informationspflichten, Einwilligungen und Widerrufe

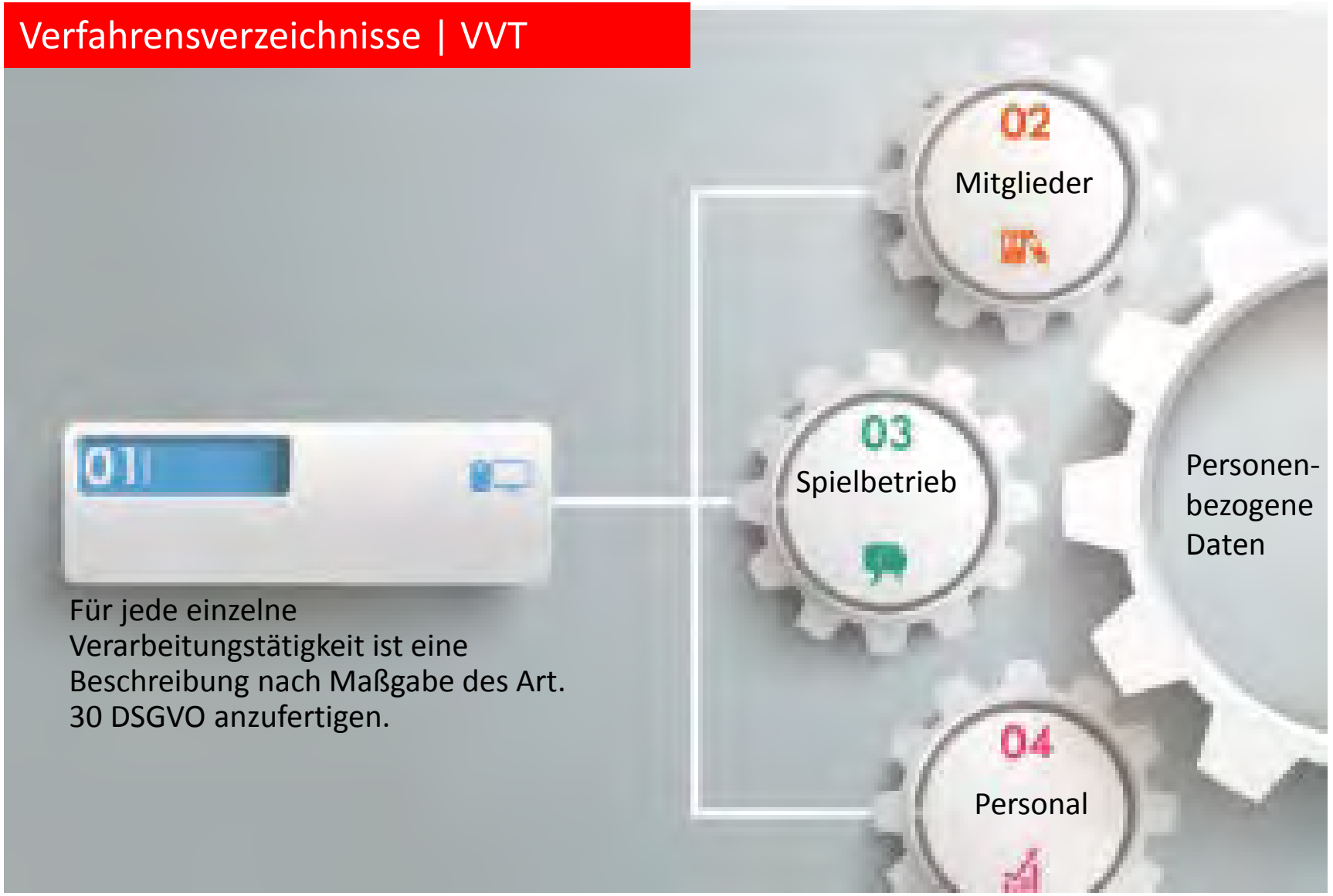
SOZIALE MEDIEN – DATENSCHUTZKONFORME NUTZUNG

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

DATENPANNEN

FRAGE

… und wo stehen Sie?

RECHTS-GRUNDLAGEN DSGVO | BDSG

PERSONEN-BEZOGENE DATEN

FOTORECHT

DIE SATZUNG

VVT | VERFAHRENS-VERZEICHNISSE

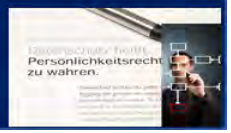
CLOUD

DATEN-GEHEIMNIS DER BESCHÄFTIGTEN

INFORMATIONS PFLICHTEN

SOZIALE NETZWERKE

DSB | DATEN-SCHUTZ-BEAUFTRAGTER



TOM TECHN. ORG. MAßNAHMEN

DATENSCHUTZ-FOLGEN-ABSCHÄTZUNG

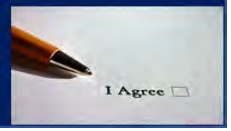
RECHT-MÄßIGKEIT DER VERARBEITUNG

VERÖFFENT-LICHUNGEN

WEBSITE IMPRESSUM DATENSCHUTZ

DATENPANNEN

AUFTRAG-VERARBEITUNG



AUSKUNFTS-ERSUCHEN

HAFTUNG UND SAKTIONEN

DATENÜBER-MITTLUNG | WEITERGABE

E-MAIL VERKEHR

IT-SICHERHEITS-KONZEPTE

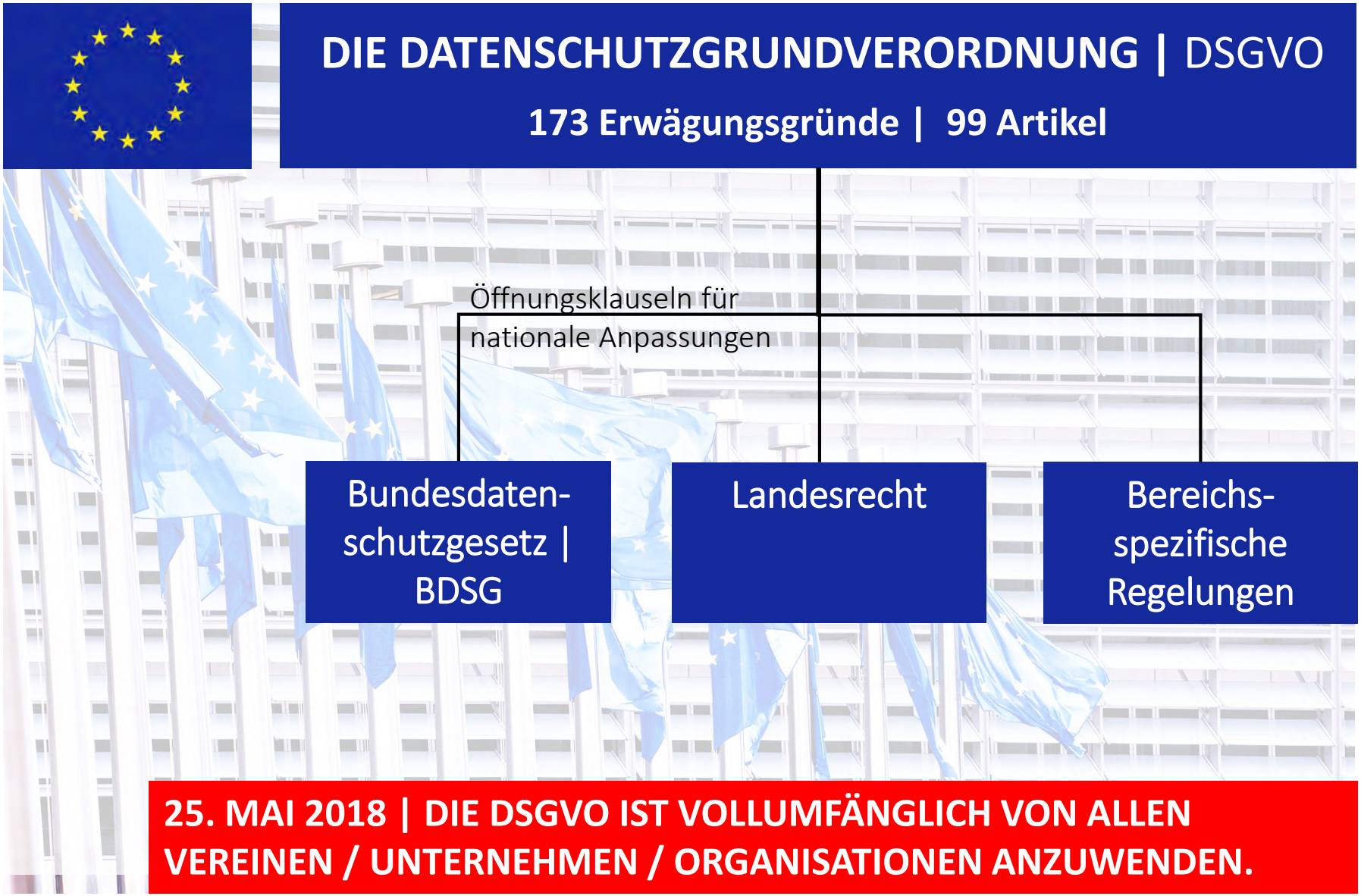
DASHBOARD

bvve
Bundesverband der Vereine und des Ehrenamtes e.V.

WARUM DATENSCHUTZRECHT? – DER ZWECK

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

DIE GESETZLICHEN GRUNDLAGEN



Die DSGVO 173 Erwägungsgründe

99 Artikel in 11 Kapiteln

Im Ergebnis geht es um die drei Kapitel:

KAPITEL 1: Allgemeine Bestimmungen

KAPITEL 2: Grundsätze

KAPITEL 3: Rechte der betroffenen Person

KAPITEL 4: Verantwortlicher und Auftragsverarbeiter

KAPITEL 5: Übermittlung personenbezogener Daten …

KAPITEL 6: Unabhängige Aufsichtsbehörden

KAPITEL 7: Zusammenarbeit und Kohärenz

KAPITEL 8: Rechtsbehelfe, Haftung und Sanktionen

KAPITEL 9: Vorschriften für besondere Verarbeitungssituationen

KAPITEL 10: Delegierte Rechtsakte und Durchführungsrechtsakte

KAPITEL 11: Schlussbestimmungen

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

GESETZGEBUNGSVERFAHREN ZUR EU-DSGVO*

*EU-Datenschutzgrundverordnung

DIE 7 GRUNDPRINZIPIEN DER DSGVO | ARTIKEL 5

Im Zentrum der DSGVO stehen 7 Grundsätzen zur rechtskonformen Speicherung und Verarbeitung personenbezogener Daten.

Wichtig: Vereine, Unternehmen und Organisationen müssen sich diese Prinzipien zu eigen machen.

PRINZIPIEN DER DSGVO

ZIEL

Die einzelnen Prinzipien als begleitende Vorgaben auslegen können und praktisch mit Beispielen füllen können.

INHALTE

1. Rechtmäßigkeit, Treu und Glauben, Transparenz
2. Zweckbindung
3. Datenminimierung
4. Richtigkeit
5. Speicherbegrenzung
6. Integrität und Vertraulichkeit
7. Rechenschaftspflicht

GESETZLICHER HINTERGRUND

in Kapitel 2 DSGVO
Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten

Erwägungsgründe
(**39**) Grundsätze der Datenverarbeitung

DSGVO | WAS SCHÜTZ SIE ART. 1 DSGVO

Art. 1 DSGVO Gegenstand und Ziele

(1) Die DSGVO schützt natürliche Personen bei der Verarbeitung personenbezogener Daten (pbD)

(2) Die DSGVO schützt die Grundrechte und Grundfreiheiten … Insbesondere … Schutz personenbezogener Daten

(3) Der freie Verkehr von pbD in der Union darf aus Gründen des Schutzes … weder eingeschränkt noch Verboten werden.

Art. 2 DSGVO Sachlicher Anwendungsbereich

Art. 2 DSGVO Sachlicher Anwendungsbereich

(1) Die DSGVO **gilt für die ganz oder teilweise automatisierte Verarbeitung** … sowie für die nichtautomatisierte Verarbeitung … die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Die DSGVO gilt **nicht** für
… im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt, …
… in den Anwendungsbereich von Titel V Kapitel 2 EUV (nationale Sicherheiten etc) …
… ausschließliche Tätigkeit im persönlichen oder familiären Umfeld
… bei der Verhütung, Ermittlung, Aufdeckung Abwehr von Gefahren, Schutz der öffentlichen Sicherheit…

(3) Die DSGVO gilt für die Verarbeitung … durch Organe, Einrichtungen, Ämter …
(4) Richtline 2000/31/EG Verantwortlichkeit der Vermittler bleibt unberührt

DSGVO | ART. 3 DSGVO

Art. 3 DSGVO Räumlicher Anwendungsbereich
„Die DSGVO erweitert den räumlichen Anwendungsbereich der europäischen Datenschutzvorschriften im Vergleich mit bisher geltenden nationalen Regelungen teilweise erheblich zum **Marktortprinzip“**

Verantwortlicher ist **innerhalb** der Union ansässig

(1) Die DSGVO gilt für die Verarbeitung pdD, soweit diese im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Union erfolgt, **unabhängig davon ob** die Verarbeitung in der Union stattfindet

Verantwortlicher ist **außerhalb** der Union ansässig

(2) Die DSGVO gilt für die Verarbeitung pbD, von betroffenen Personen, die sich in der Union befinden, wenn die Datenverarbeitung im Zusammenhang (mit dieser Person) steht

a) Betroffenen in der Union Waren oder Dienstleistungen anzubieten … unabhängig ob Zahlungen zu leisten sind.
b) Das Verhalten Betroffener zu beobachten

(3) Die DSGVO gilt für die Verarbeitung pdD, der aufgrund Völkerrechts dem Recht eines Mitgliedsstaates unterliegt

DOKUMENTATIONSPFLICHTEN WANN UND WO

Allgemeine Dokumentationspflichten

Die Rechenschaftspflicht		**Art. 5 Abs. 2 DSGVO**
Einhaltung ist nachweispflichtig	Die Rechenschaftspflichten als Teil der Datenschutzorganisation	**Art. 5 Abs.1 DSGVO**
Präzisierung der Einhaltung der DSGVO-Konformität		**Art. 24 Abs.1 DSGVO**

Hieraus folgt die Pflicht des Nachweises der Rechenschafts- und Nachweispflichten

Die Erfüllung der Rechenschaftspflichten ist ohne eine effektive Datenschutzorganisation kaum denkbar: Was hilft es Auftragsverarbeitungsverträge zu Nachweiszwecken abzulegen, wenn niemand mehr sagen kann, wer dafür zuständig ist und wo genau die Verträge überhaupt abgelegt wurden. In der Praxis gehen Datenschutzorganisation und lückenlose Dokumentation Hand in Hand.

DOKUMENTATIONSPFLICHTEN WANN UND WO

Wie weit müssen die allgemeinen Rechenschafts- und Nachweispflichten gehen?

Der Umfang ist umstritten - es gibt keine festgelegten Grenzen

Problemstellung ist die Gewährleistung der betrieblichen Prozesse auch unter Einhaltung der DSGVO

Der Verwaltungsaufwand ist umfangreich

Eigenständige einzelne festgelegten Dokumentationspflichten

Hieraus folgt die Pflicht des Nachweises der Rechenschafts- und Nachweispflichten

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 ...

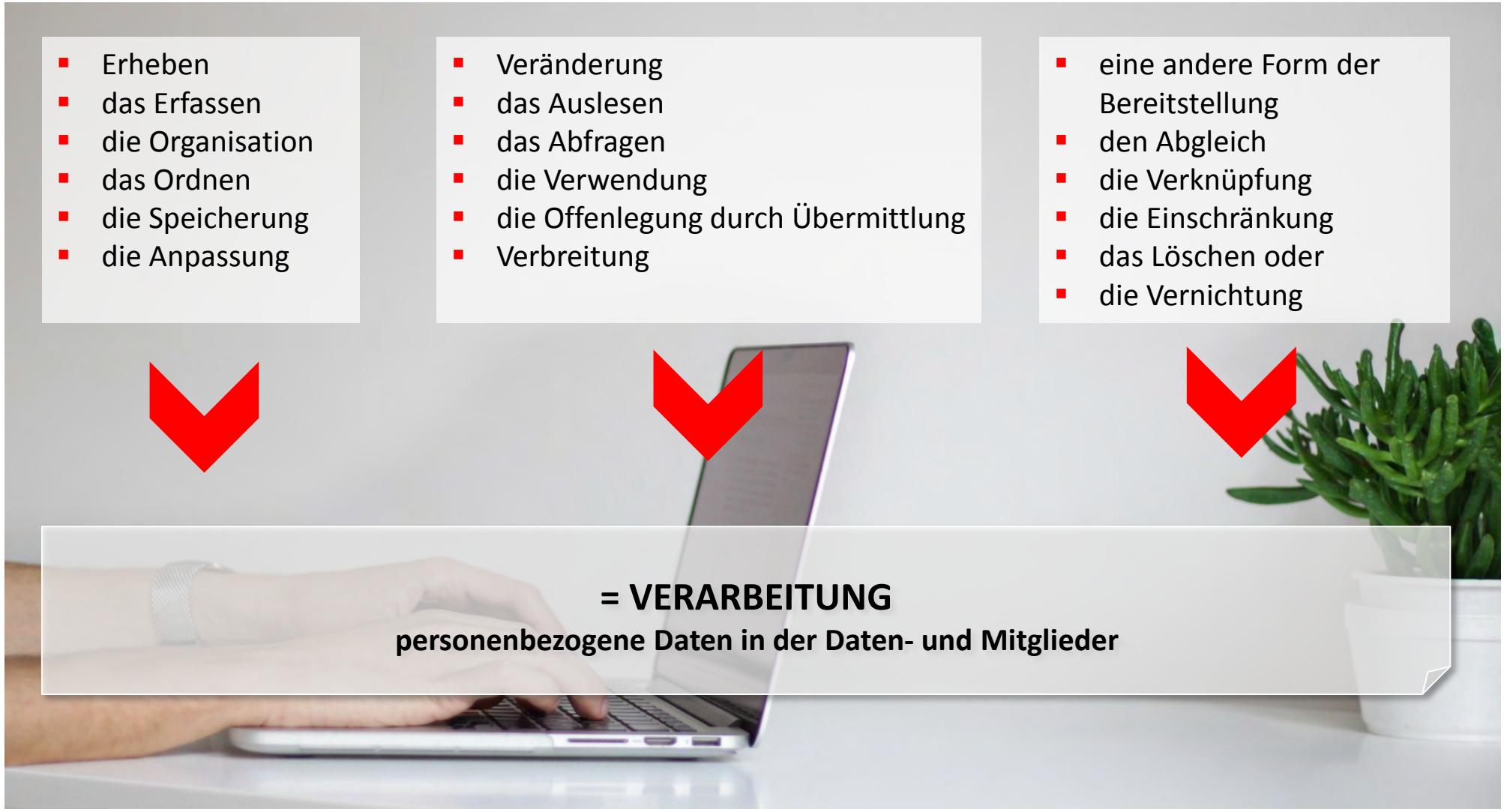
PERSONENBEZOGENE DATEN IM VEREIN

Art. 4 DSGVO (2) „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das

- Erheben
- das Erfassen
- die Organisation
- das Ordnen
- die Speicherung
- die Anpassung

- Veränderung
- das Auslesen
- das Abfragen
- die Verwendung
- die Offenlegung durch Übermittlung
- Verbreitung

- eine andere Form der Bereitstellung
- den Abgleich
- die Verknüpfung
- die Einschränkung
- das Löschen oder
- die Vernichtung



= VERARBEITUNG

personenbezogene Daten in der Daten- und Mitglieder

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)

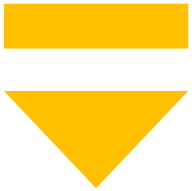
aussagen.

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

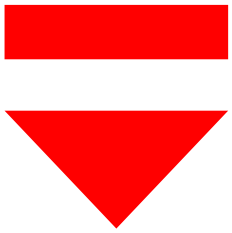
....



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 verarbeiten, 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 …

RECHTMÄßIGKEIT DER VERARBEITUNG

DAS VERBOTSPRINZIP | ART. 6 DSGVO

Der Verantwortliche (Unternehmen, Kanzlei, 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

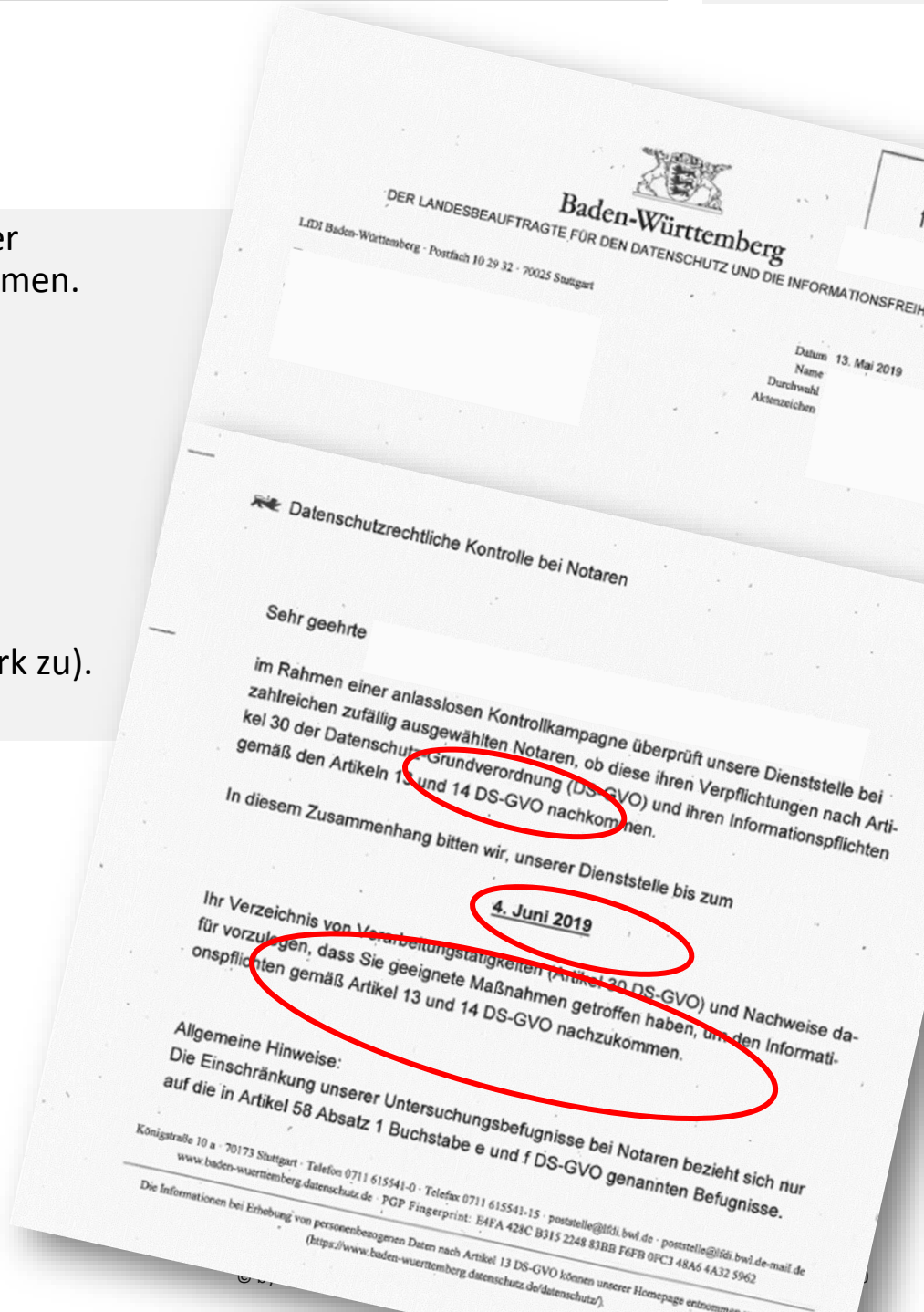
WER TRÄGT DIE VERANTWORTUNG?

DIE DATENSCHUTZ-VERANTWORTUNG TRÄGT IMMER DER VORSTAND DES VEREINS …

VERSTÖßE, DIE IHNEN EINE STRAFE NACH DSGVO EINHANDELN KÖNNEN

Warum kommt die Datenschutzbehörde ….

- Einer Anfrage eines Kunden nach Löschung, Auskunft oder Berichtigung wird nicht oder nicht rechtzeitig nachgekommen.
- Meldung eines eigenen Datenschutzverstoßes | Datenpanne – Prüfung durch die Behörde
- Fehlende SSL Verschlüsselung der Website
- Bei Kontaktformularen fehlt der Datenschutzhinweis und dies wird der Behörde gemeldet
- Sie sind von einer vorsorglichen Kontrolle der Behörden betroffen (die Häufigkeit nimmt aktuell stark zu).



Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIH

LfDI Baden-Württemberg · Postfach 10 29 32 · 70025 Stuttgart

Datum 13. Mai 2019
Name
Durchwahl
Aktenzeichen

Datenschutzrechtliche Kontrolle bei Notaren

Sehr geehrte

im Rahmen einer anlasslosen Kontrollkampagne überprüft unsere Dienststelle bei zahlreichen zufällig ausgewählten Notaren, ob diese ihren Verpflichtungen nach Artikel 30 der Datenschutz-Grundverordnung (DS-GVO) und ihren Informationspflichten gemäß den Artikeln 13 und 14 DS-GVO nachkommen.

In diesem Zusammenhang bitten wir, unserer Dienststelle bis zum

4. Juni 2019

Ihr Verzeichnis von Verarbeitungstätigkeiten (Artikel 30 DS-GVO) und Nachweise dafür vorzulegen, dass Sie geeignete Maßnahmen getroffen haben, um den Informationspflichten gemäß Artikel 13 und 14 DS-GVO nachzukommen.

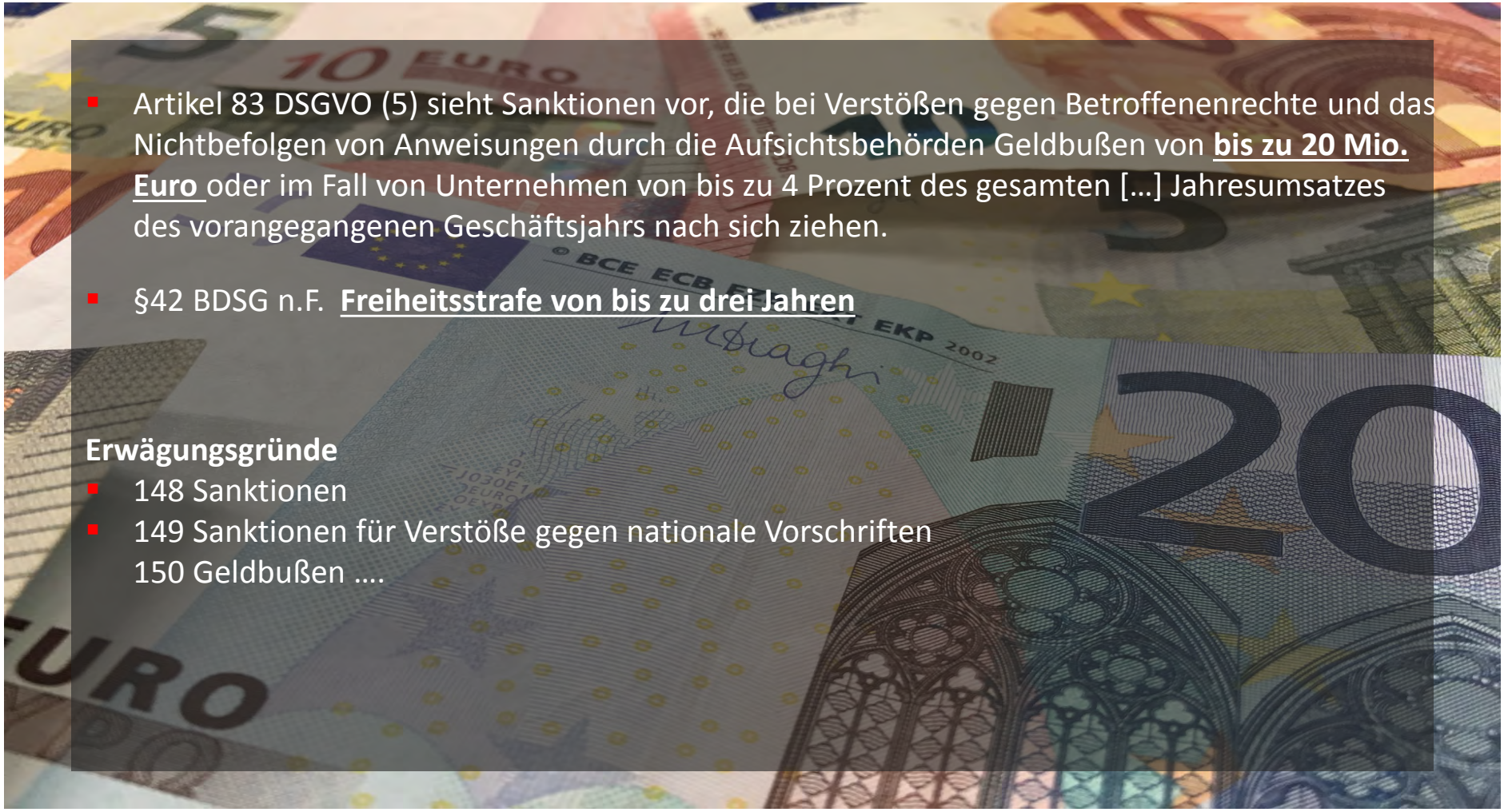
Allgemeine Hinweise:
Die Einschränkung unserer Untersuchungsbefugnisse bei Notaren bezieht sich nur auf die in Artikel 58 Absatz 1 Buchstabe e und f DS-GVO genannten Befugnisse.

Königstraße 10 a · 70173 Stuttgart · Telefon 0711 615541-0 · Telefax 0711 615541-15 · poststelle@lfdi.bwl.de · poststelle@lfdi.bwl.de-mail.de
www.baden-wuerttemberg.datenschutz.de · PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962
Die Informationen bei Erhebung von personenbezogenen Daten nach Artikel 13 DS-GVO können unserer Homepage entnommen (https://www.baden-wuerttemberg.datenschutz.de/datenschutz/).

BEISPIEL: PRÜFUNGSANORDNUNG

SANKTIONEN IN DER VERANTWORTLICHKEIT

Sanktionen



- Artikel 83 DSGVO (5) 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.

- §42 BDSG n.F. **Freiheitsstrafe von bis zu drei Jahren**

Erwägungsgründe

- 148 Sanktionen
- 149 Sanktionen für Verstöße gegen nationale Vorschriften
  150 Geldbußen ….

DIE SATZUNG IM VEREIN

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

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 ohne Satzungscharakter

Der Verein muss aber immer seinen Informationspflichten nach Art. 13 ff nachkommen …

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

… eine schlanke Satzung macht den Verein „lean“
… flexibel für die Nachfolgefindung!

LEISTUNGEN, DIE DER VEREIN ERFÜLLEN MUSS

Informationspflichten, Betroffenenrechte

DAS WICHTIGSTE ZUERST: 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**

Inhalte Datenschutz Informationspflichten	geprüft
Grundsätze der Datenverarbeitung bei der Mustermann GmbH	O
Sie sind über einen Link auf diese Seite gekommen, weil Sie sich über unseren Umgang mit (Ihren) personenbezogenen Daten informieren wollen. Um unsere Informationspflichten nach den Art. 12 ff. der Datenschutz-Grundverordnung (DSGVO) zu erfüllen, stellen wir Ihnen nachfolgend gerne unsere Informationen zum Datenschutz dar:	O
Wer ist für Datenverarbeitung verantwortlich?	O
Verantwortlicher im Sinne des Datenschutzrecht ist die	O
Mustermann GmbH	O
Musterstr. 123	O
12345 Musterstadt	O
Sie finden weitere Informationen zu unserem Unternehmen, Angaben zu den vertretungsberechtigten Personen und auch weitere Kontaktmöglichkeiten im Impressum unserer Internetseite: https://www.mustermann.de/impressum	O
Welche Daten von Ihnen werden von uns verarbeitet? Und zu welchen Zwecken?	O
Wenn wir Daten von Ihnen erhalten haben, dann werden wir diese grundsätzlich nur für die Zwecke verarbeiten, für die wir sie erhalten oder erhoben haben.	O
Eine Datenverarbeitung zu anderen Zwecken kommt nur dann in Betracht, wenn die insoweit erforderlichen rechtlichen Vorgaben gemäß Art. 6 Abs. 4 DSGVO vorliegen. Etwaige Informationspflichten nach Art. 13 Abs. 3 DSGVO und Art. 14 Abs. 4 DSGVO werden wir in dem Fall selbstverständlich beachten.	O
Auf welcher rechtlichen Grundlage basiert das?	O
Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten ist grundsätzlich – soweit es nicht noch spezifische Rechtsvorschriften gibt – Art. 6 DSGVO. Hier kommen insbesondere folgende Möglichkeiten in Betracht:	O
• Einwilligung (Art. 6 Abs. 1 lit. a) DSGVO)	O
• Datenverarbeitung zur Erfüllung von Verträgen (Art. 6 Abs. 1 lit. b) DSGVO	O
• Datenverarbeitung auf Basis einer Interessenabwägung (Art. 6 Abs. 1 lit. f) DSGVO)	O

• Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c) DSGVO)	O
• die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen - hier nicht zutreffend - (Art. 6 Abs. 1 lit. d) DSGVO)	O
• die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde; - hier nicht zutreffend - (Art. 6 Abs. 1 lit. e) DSGVO)	O
Widerruf und Widerspuch	O
Wenn personenbezogene Daten auf Grundlage einer **Einwilligung** von Ihnen verarbeitet werden, haben Sie das Recht, die Einwilligung jederzeit mit Wirkung für die Zukunft uns gegenüber zu **widerrufen**.	O
Wenn wir Daten auf Basis einer **Interessenabwägung** verarbeiten, haben Sie als Betroffene/r das Recht, unter Berücksichtigung der Vorgaben von Art. 21 DSGVO der Verarbeitung der personenbezogenen Daten zu **widersprechen.**	O
Wie lange werden die Daten gespeichert?	O
Wir verarbeiten die Daten, solange dies für den jeweiligen Zweck erforderlich ist.	O
	O
Soweit gesetzliche Aufbewahrungspflichten bestehen – z.B. im Handelsrecht oder Steuerrecht – werden die betreffenden personenbezogenen Daten für die Dauer der Aufbewahrungspflicht gespeichert. Nach Ablauf der Aufbewahrungspflicht wird geprüft, ob eine weitere Erforderlichkeit für die Verarbeitung vorliegt. Liegt eine Erforderlichkeit nicht mehr vor, werden die Daten gelöscht.	O
Prüfung auf Erforderlichkeit	O
Grundsätzlich nehmen wir gegen Ende eines Kalenderjahres eine Prüfung von Daten im Hinblick auf das Erfordernis einer weiteren Verarbeitung vor. Aufgrund der Menge der Daten erfolgt diese Prüfung im Hinblick auf spezifische Datenarten oder Zwecke einer Verarbeitung.	O
Auskunfsrecht	O
Selbstverständlich können Sie jederzeit (s.u.) Auskunft über die bei uns zu Ihrer Person gespeicherten Daten verlangen und im Falle einer nicht bestehenden Erforderlichkeit eine Löschung der Daten oder Einschränkung der Verarbeitung verlangen.	O
An welche Empfänger werden die Daten weitergegeben | Datenübermittlung?	O
Eine Weitergabe Ihrer personenbezogenen Daten an Dritte findet grundsätzlich nur statt, wenn dies für die Durchführung des Vertrages mit Ihnen erforderlich ist, die Weitergabe auf Basis einer Interessenabwägung i.S.d. Art. 6 Abs. 1 lit. f) DSGVO zulässig ist, wir rechtlich zu der Weitergabe verpflichtet sind oder Sie insoweit eine Einwilligung erteilt haben.	O

Wo werden die Daten verarbeitet?	O
Ihre personenbezogenen Daten werden von uns ausschließlich in Rechenzentren der Bundesrepublik Deutschland oder innerhalb der Europäischen Union verarbeitet.	O
Ihre Rechte als „Betroffene“	O
• Sie haben das Recht auf Auskunft über die von uns zu Ihrer Person verarbeiteten personenbezogenen Daten.	O
Bei einer Auskunftsanfrage, die nicht schriftlich erfolgt, bitten wir um Verständnis dafür, dass wir dann ggf. Nachweise von Ihnen verlangen, die belegen, dass Sie die Person sind, für die Sie sich ausgeben.	O
Ferner haben Sie ein Recht auf • Berichtigung oder • Löschung oder • auf Einschränkung der Verarbeitung, soweit Ihnen dies gesetzlich zusteht. • ein Widerspruchsrecht gegen die Verarbeitung im Rahmen der gesetzlichen Vorgaben • ein Recht auf Datenübertragbarkeit besteht ebenfalls im Rahmen der datenschutzrechtlichen Vorgaben.	

Insbesondere haben Sie ein Widerspruchsrecht nach Art. 21 Abs. 1 und 2 DSGVO gegen die Verarbeitung Ihrer Daten im Zusammenhang mit einer Direktwerbung, wenn diese auf Basis einer Interessenabwägung erfolgt.	O
Wir setzen keine Verarbeitungen ein, die auf einer automatisierten Entscheidungsfindung einschließlich Profiling i.S.d. Art. 22 DSGVO beruhen.	O
oder: Wir setzen Verarbeitungen ein, die auf einer automatisierten Entscheidungsfindung einschließlich Profiling i.S.d. Art. 22 DSGVO beruhen.	
Hier muss dann genaue Beschreibung erfolgen	O
Unsere Datenschutzbeauftragte	O
Wir haben eine Datenschutzbeauftragte in unserem Unternehmen benannt. Sie erreichen diese unter folgenden Kontaktmöglichkeiten:	O
Mustermann GmbH	O
– Datenschutzbeauftragte –	O
Musterstr. 123	O
12345 Musterstadt	O
E-Mail: datenschutz@mustermann.de	O
Beschwerderecht	O
Sie haben das Recht, sich über die Verarbeitung personenbezogenen Daten durch uns bei einer Aufsichtsbehörde für den Datenschutz zu beschweren.	
Die für uns zuständige Aufsichtbehörde ist:	
Link oder Anschrift der Aufsichtsbehörde	O
Stand: 30.05.2018	O

Veröffentlichungen

Die Herausforderungen liegt in den Informationspflichten bei

- Veröffentlichungen und
- Ergebnisdiensten …

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.**

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)

VIDEOÜBERWACHUNG!

Verantwortlicher:
Maxi Mustermann GmbH
Musterstr. 123
12345 Musterstadt
info@mustermann.de

Zweck:
Die Videoüberwachung erfolgt zur Wahrnehmung des Hausrechts, zur Vermeidung von Straftaten sowie zur Beweissicherung bei Straftaten. Rechtsgrundlage der Videoüberwachung ist Art. 6 Abs. 1 lit. f) DSGVO, wobei unsere Interessen sich aus den vorgenannten Zwecken ergeben.

Weitere Hinweise:
Weitere Hinweise zum Datenschutz (insbesondere Ihren Rechten), zur Speicherdauer sowie Kontaktdaten unseres Datenschutzbeauftragten finden Sie im Internet unter: **www.mustermann.de/video**
Alternativ können Sie die Informationen auch jederzeit bei uns anfordern.

SOZIALE MEDIEN – DATENSCHUTZKONFORME NUTZUNG

- Facebook
- WhatsApp
- Instagram
- Snapshot
- ….

Wie überprüfe ich einen Anbieter auf DSGVO-Konformität?

- Impressum
- Datenschutzerklärung
- Wo steht der Server?

Siehe auch Facebook Urteil

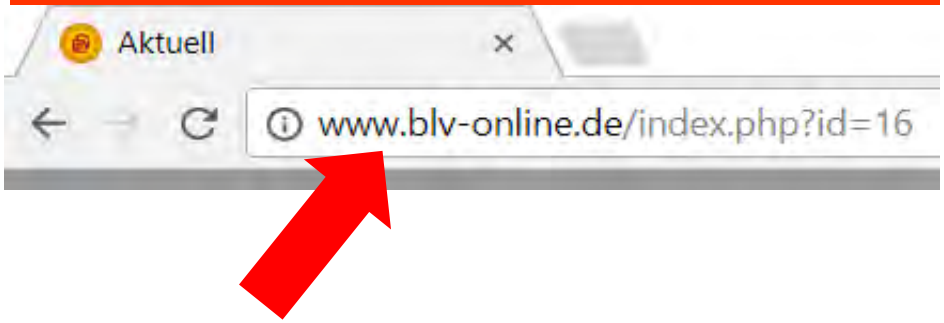
IMPRESSUM | DATENSCHUTZERKLÄRUNG

- Impressum
- Datenschutzerklärung
- E-Mail-Verkehr

VERPFLICHTUNG ZU SICHEREN WEBSEITEN

SSL oder TLS für Webseiten nachrüsten!

Nicht sichere Website

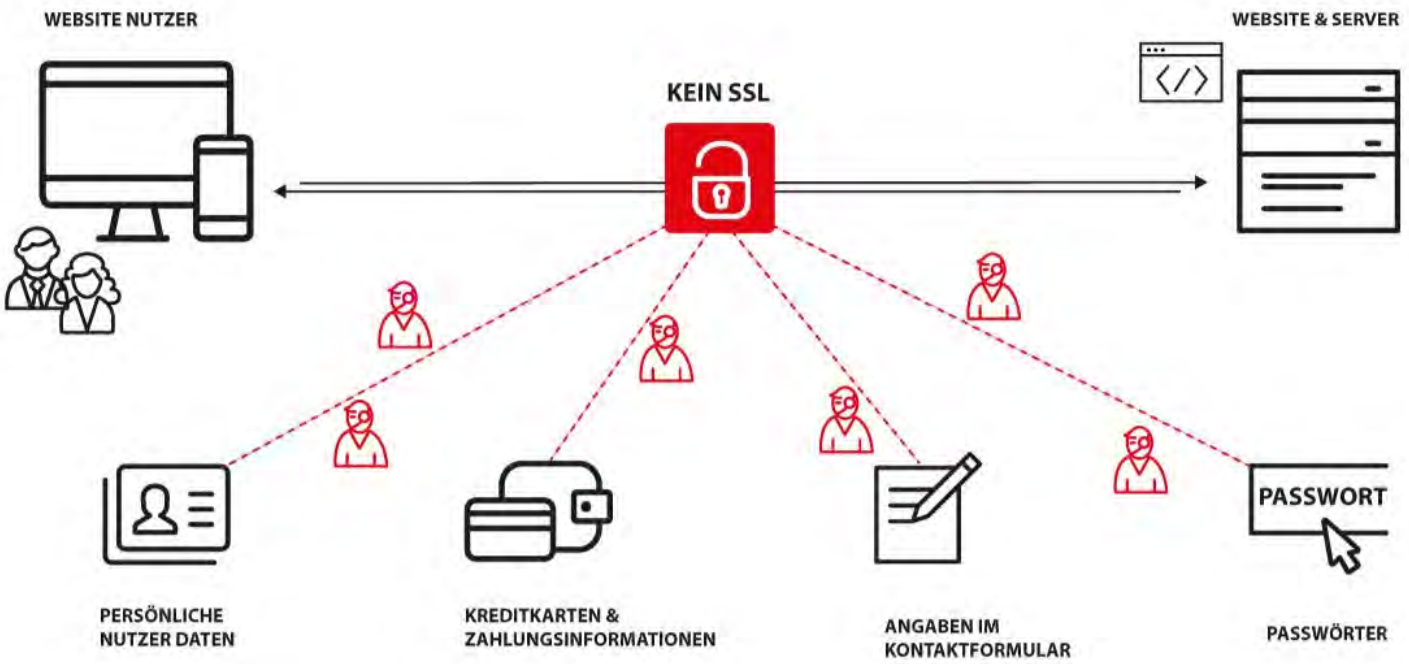


Sichere Website

SSL oder TLS für Webseiten nachrüsten!

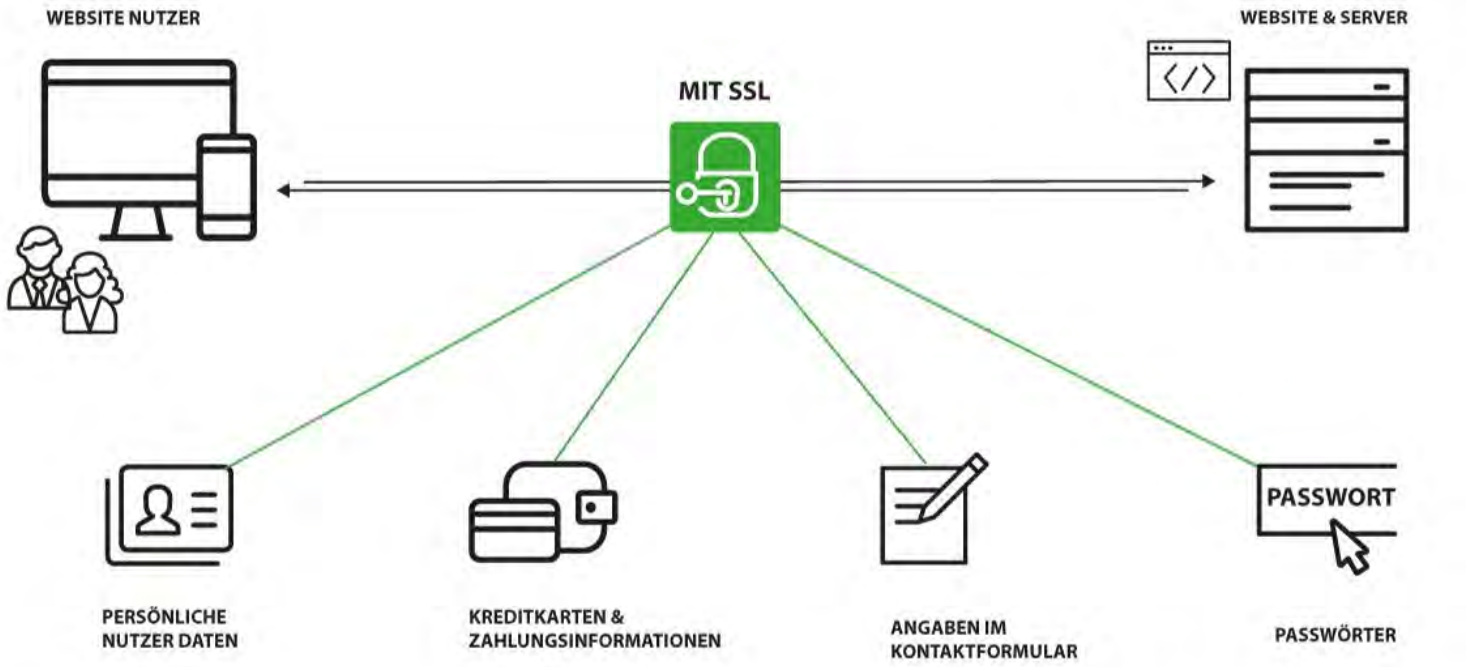
VERPFLICHTUNG ZUR VERSCHLÜSSELUNG | WEBSITE

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?

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

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.

WAS REGELT DIE DATENSCHUTZERKLÄRUNG

… online auf der Website…

- … zunächst einmal auf die Datenverarbeitung auf Ihrer Webseite.
- Wenn Daten „offline Daten“ erhoben werden,
  sollten in diesem diesem Formular gesondert über den Umgang mit diesen Daten informieren werden.

Wichtig

Die Informationspflicht muss immer

- transparent und in
- klarer
- einfacher
- leichtverständlicher Sprache

erfolgen

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

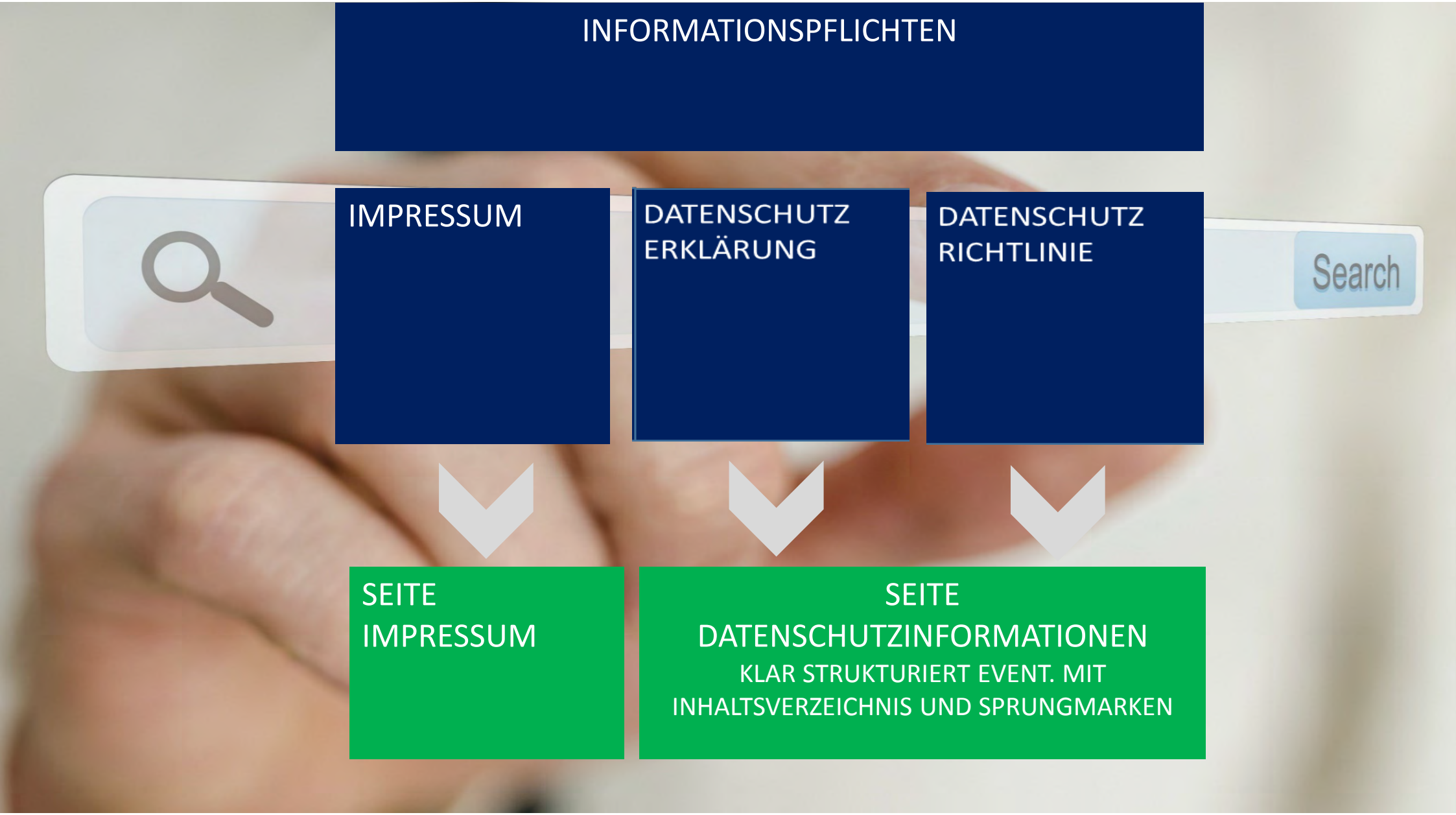
- Hieraus leiten sich ab die **weiteren Verpflichtungen** zur Information zu:
  - Cookie-Verwendung
  - Registrierung für Kunden
  - Newsletters-Abo
  - Kontaktformular
  - Blog oder redaktionelle Artikel
  - Online-Bewerbungsmöglichkeiten (auch per E-Mail).

- **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.


INFORMATIONSPFLICHTEN
IMPRESSUM
DATENSCHUTZ ERKLÄRUNG
DATENSCHUTZ RICHTLINIE
Search
SEITE IMPRESSUM
SEITE DATENSCHUTZINFORMATIONEN
KLAR STRUKTURIERT EVENT. MIT INHALTSVERZEICHNIS UND SPRUNGMARKEN


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.

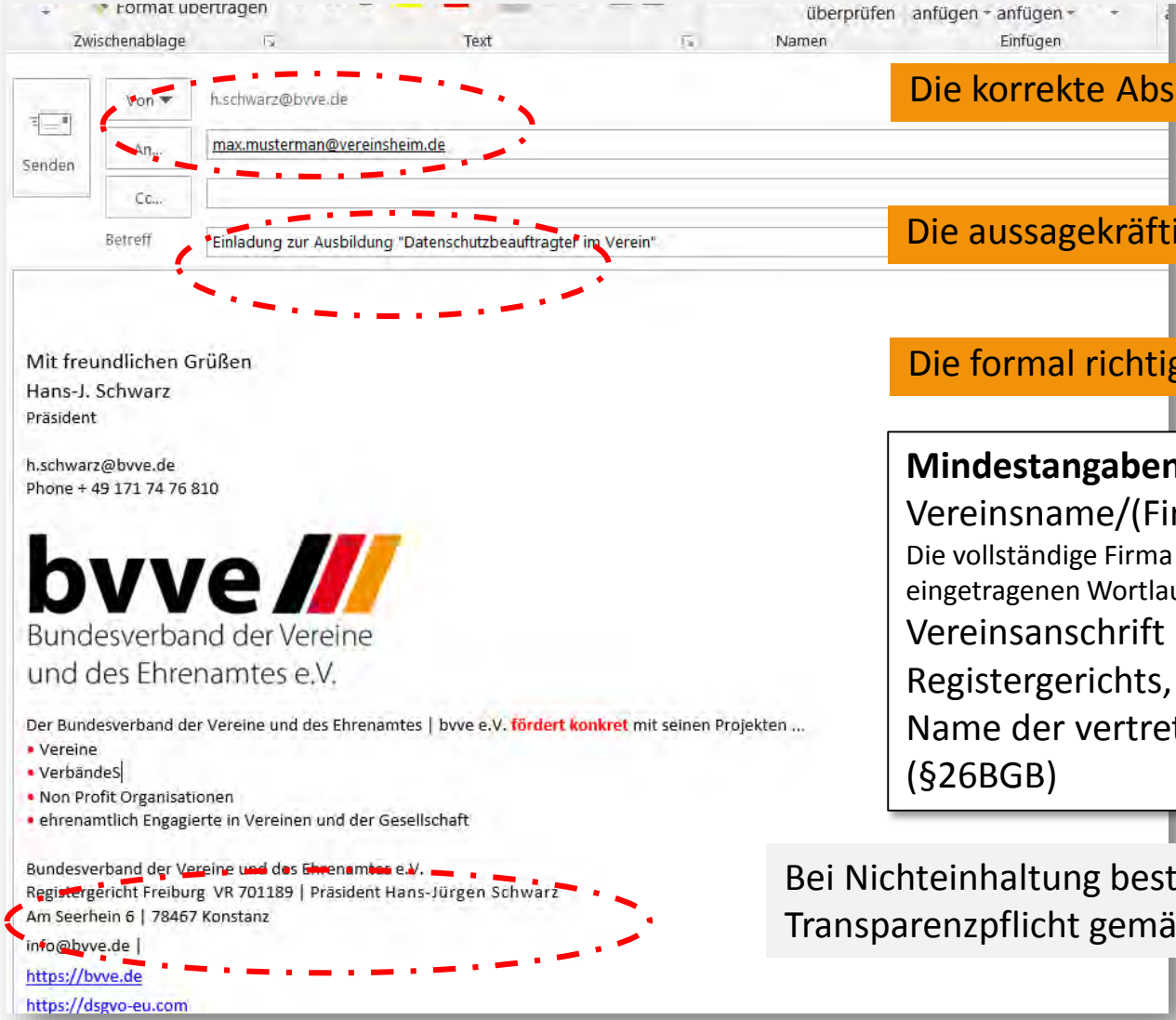
Die Versendung von E-Mails, in denen im Empfängerfeld andere Empfänger sichtbar sind, ist unzulässig!

→ 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)

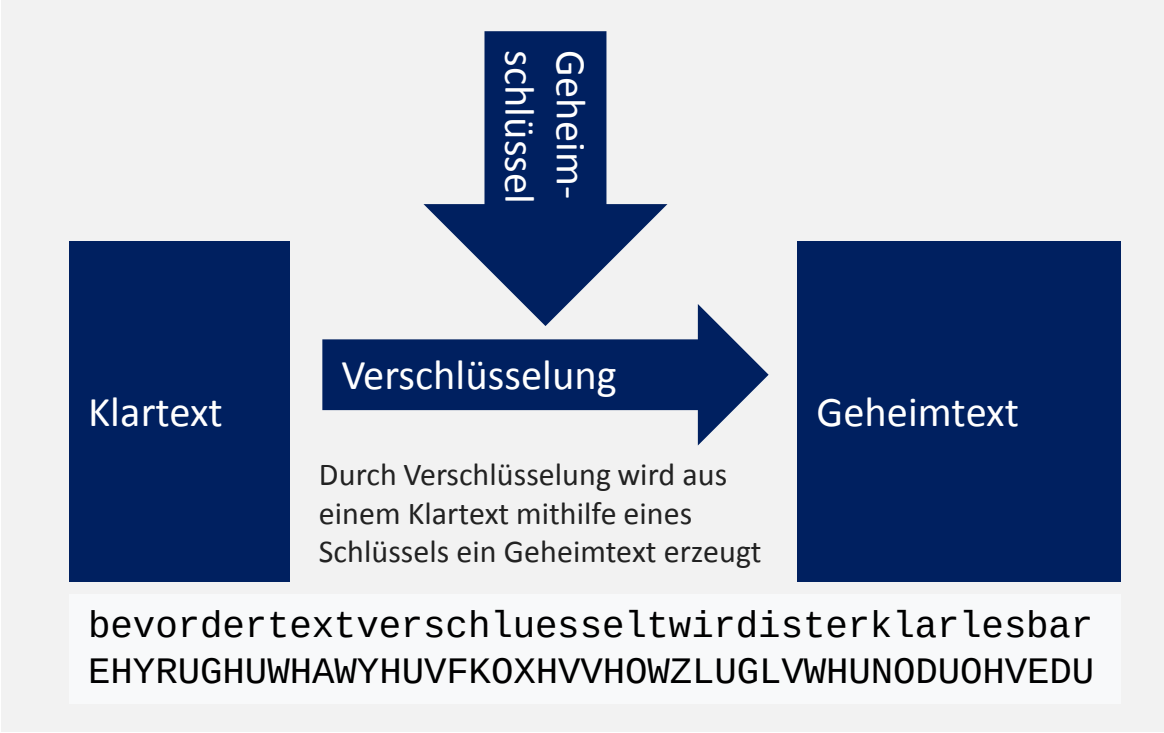
Registergerichts, Registernummer und

Name der vertretungsberechtigten Vorstände (§26BGB)

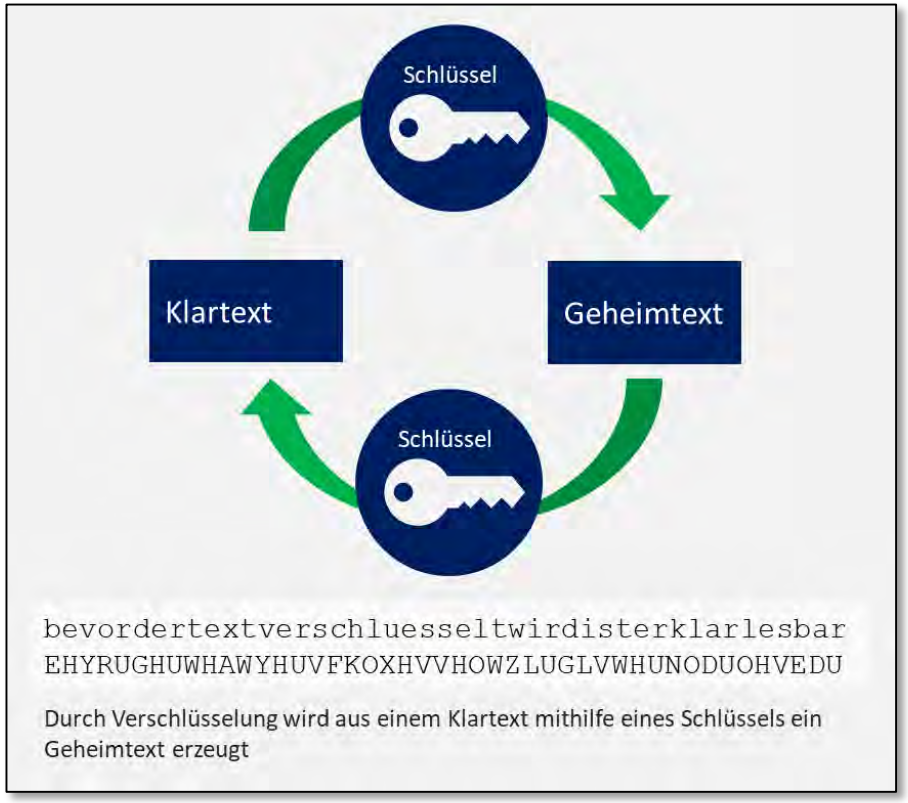
Bei Nichteinhaltung besteht eventuell ein Verstoß gegen die Transparenzpflicht gemäß § 6 des Telemediengesetzes (TMG).

2.4a Weitergabekontrolle | Verschlüsselung

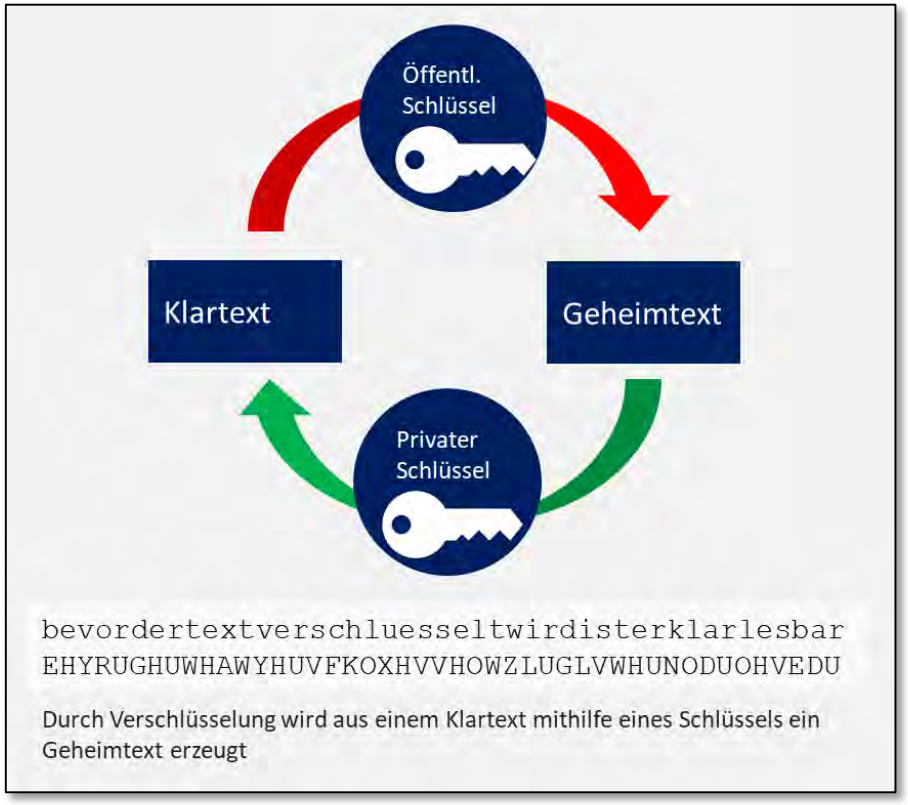
Verschlüsselung (auch: **Chiffrierung** oder **Kryptierung**)[1] ist die von einem Schlüssel abhängige Umwandlung von „Klartext“ genannten Daten in einen „Geheimtext“ (auch: „Chiffrat“), so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann. Sie dient zur Geheimhaltung von Nachrichten, beispielsweise um Daten gegenüber unbefugtem Zugriff zu schützen oder um Nachrichten vertraulich übermitteln zu können.



Bei der symmetrischen Verschlüsselung dient der Schlüssel auch zur Entschlüsselung



Bei der asymmetrischen Verschlüsselung gibt es zwei unterschiedliche Schlüssel, den öffentlichen Schlüssel zur Verschlüsselung und den privaten Schlüssel zur Entschlüsselung



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

GRUNDPRINZIPIEN DER DSGVO

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:

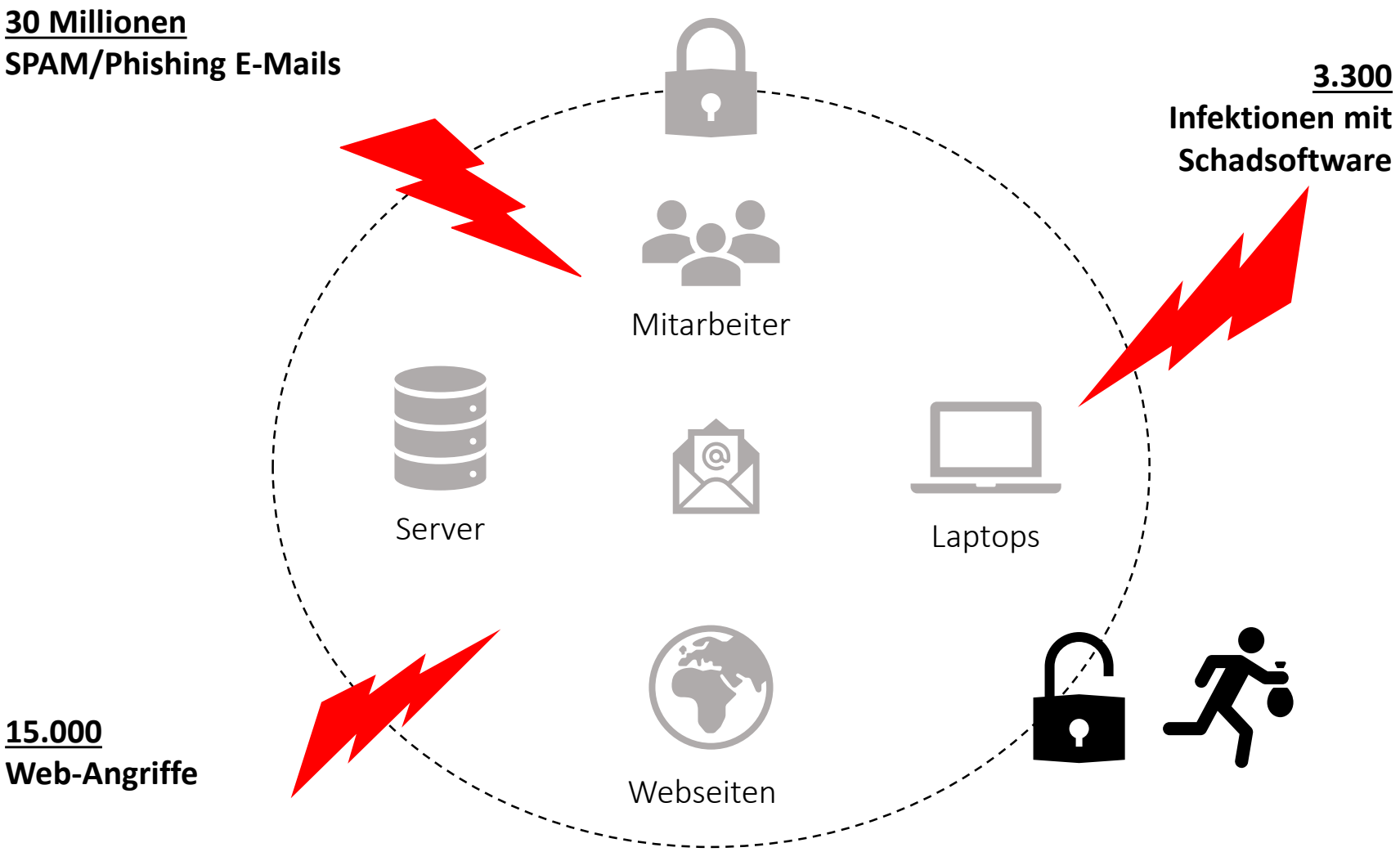
- Unternehmen
- Vereine
- Verbände
- Selbstständige
- Behörden
- Auftragsverarbeiter
- …

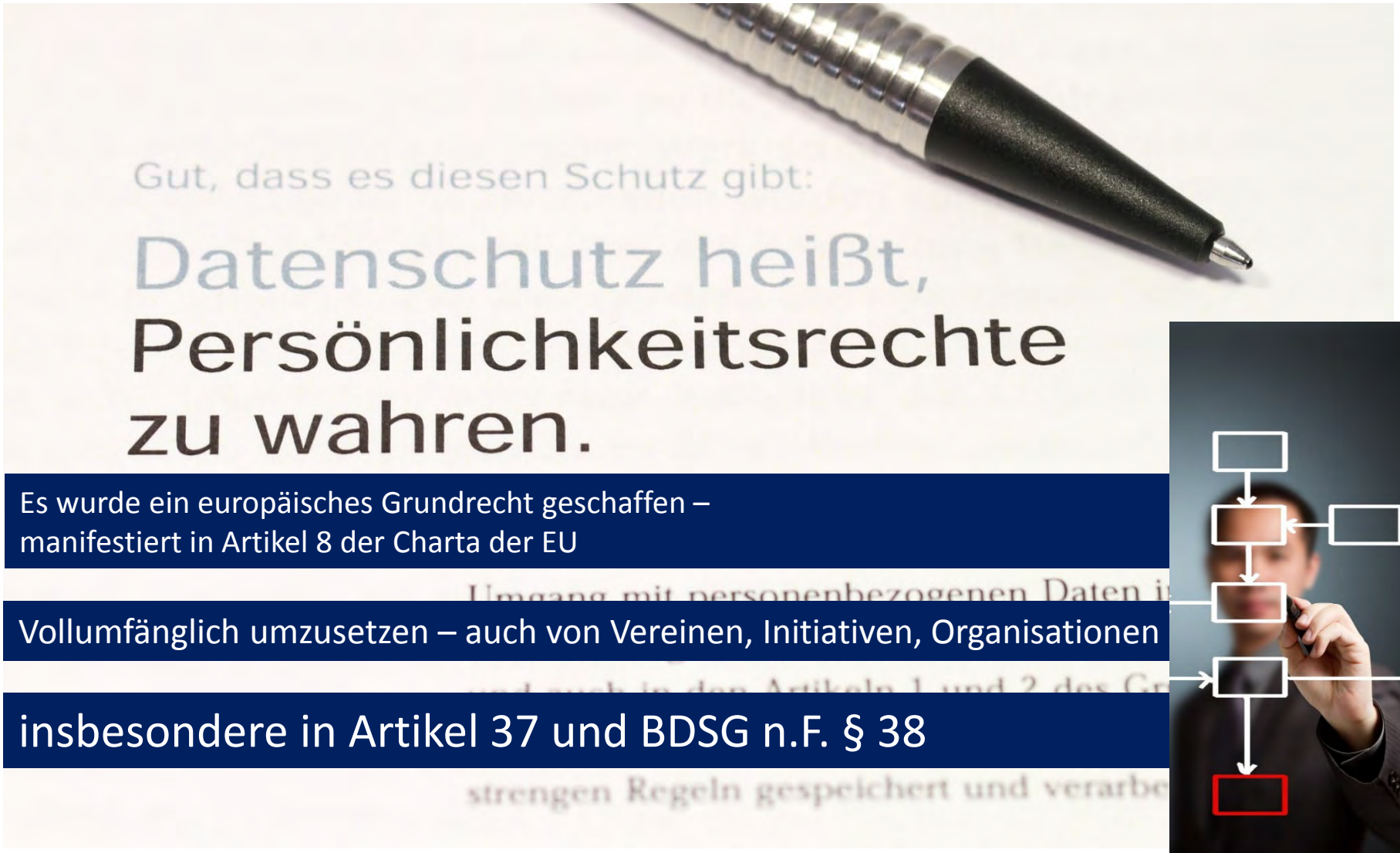
WAS REGELT DIE DATENSCHUTZ-GRUNDVERORDNUNG |DSGVO

- 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:





Es wurde ein europäisches Grundrecht geschaffen –
manifestiert in Artikel 8 der Charta 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**

- **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

DSB | DATEN-SCHUTZ-BEAUFTRAGTER

ZIEL

Das Berufsbild Datenschutzbeauftragter mit seinen rechtlichen Rahmenbedingungen und Anforderungen verstehen und einordnen können.

INHALTE

Aufgaben
Qualifikationen
Stellung
Haftung
Bestellung

GESETZLICHER HINTERGRUND

Art. 37 DSGVO Benennung eines Datenschutzbeauftragten Abs. 5
Erwägungsgründe (97) Datenschutzbeauftragter
§ 5 BDSG Benennung
§ 38 BDSG Datenschutzbeauftragte nichtöffentlicher Stellen Art. 38 DSGVO Stellung des Datenschutzbeauftragten
Erwägungsgründe (97) Datenschutzbeauftragter
§ 6 BDSG Stellung
Art. 39 DSGVO Aufgaben des Datenschutzbeauftragten
Erwägungsgründe (97) Datenschutzbeauftragter
§ 7 BDSG Aufgaben

LEGAL

DATENSCHUTZBEAUFTRAGTER | BENENNUNG AB WANN

Wer benötigt einen Datenschutzbeauftragten?

Art. 35 | Datenschutzfolgeabschätzung

Art. 37 DSGVO

a) Behörden oder öffentlichen Stellen

b) Kerntätigkeit regelmäßige systematische Überwachung

c) Verarbeitung …besondere personenbezogene Daten nach Art. 9 DSGVO

d) Verarbeitung … strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO

BDSG n.F.
§ 5 Behörden oder öffentlichen Stellen

Erwägungsgrund 97
der DSGVO

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

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

- Die Benennungspflicht eines Datenschutzbeauftragten (DBS) besteht für Vereine, Unternehmen, Organisationen 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

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.

WER MUSS MITGEZÄHLT WERDEN?

Unsere E-Mail vom 19. März 2019 an den LDIS

Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

LfDI Baden-Württemberg · Postfach 10 29 32 · 70025 Stuttgart

Datum 20. Mai 2019
Name Frau Röhr
Durchwahl 0711/615541-36
Aktenzeichen D 3050/729
(Bitte bei Antwort angeben)

Per E-Mail

Herrn
Hans-Jürgen Schwarz

Datenschutzrechtliche Anfrage, Ergänzungsfragen
Ihre E-Mail vom 19. März 2019
Unser Schreiben vom 23. Oktober 2018, Az. D 3050/729

Sehr geehrter Herr Schwarz,

ergänzend zu Art. 37 Abs. 1 lit. b) und c) der Datenschutz-Grundverordnung
GVO) benennen der Verantwortliche und der Auftragsverarbeiter eine Date
beauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel n
zehn Personen ständig mit der automatisierten Verarbeitung personenbez
ten beschäftigen, vgl. § 38 Abs. 1 S. 1 des Bundesdatenschutzgesetzes

„Ständig" beschäftigt ist eine Person, wenn sie für diese Aufgabe auf lär
vorgesehen ist und sie entsprechend wahrnimmt. Irrelevant ist, ob die F
Verein beschäftigt oder ehrenamtlich tätig ist. Die Aufgabe braucht auc
aufgabe der Person zu sein. Das Tatbestandsmerkmal „ständig" ist da
füllt, wenn die Aufgabe selbst nur gelegentlich anfällt, die betreffende
stets wahrzunehmen hat. Ständig bedeutet daher, dass die Person i
der Verarbeitung personenbezogener Daten beschäftigt ist, wenn di
fällt. Nachlesen können Sie diese Beschreibung in unserem Praxisratgeber (S. 6),
der wie folgt unter der unten genannten Stelle u. a. auch zu dieser Frage abrufbar ist.

Verarbeitet ein Verein (Verband) ganz oder teilweise automatisiert personenbezogene Daten seiner Mitglieder und sonstiger Personen oder erfolgt eine nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, ist nach Art. 2 Abs. 1 DS-GVO deren Anwendungsbereich eröffnet, vgl. unsere unten genannte Orientierungshilfe auf S. 5.

Zu Ihrer Ergänzungsfrage a):
Unter der Voraussetzung, dass der Wanderwart stets die Kontaktdaten aufnimmt und diese z. B. in einem Dateisystem verarbeitet (z. B. Karteikasten), zählt auch diese Person zu den unter § 38 Abs. 1 S.1 BDSG genannten 10 Personen.

Zu Ihrer Ergänzungsfrage b):
Auch für Auftragsverarbeiter trifft dies zu.

Zu Ihrer Ergänzungsfrage c):
Dateisystem ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob die Sammlung zentral, dezentral oder nach funktionalen oder geographischen Gesichtspunkten geordnet geführt wird (Art. 4 Nr. 6 DS-GVO). Dazu zählen auch Papier-Akten; vgl. S. 6 der u. g. Orientierungshilfe. Es hängt also mit der Ablage des Formblattes zusammen: Eine alphabetische Reihung wäre dazu ausreichend.

Abschließend verweisen wir auch auf unsere Veröffentlichungen zum Datenschutz in Vereinen im Internet, z. B.

- die Orientierungshilfe, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf,
- den Praxisratgeber, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-für-Vereine.pdf,
- die FAQs, https://www.baden-wuerttemberg.datenschutz.de/faq-vereine/.

Wir hoffen, wir konnten Ihnen mit den oben stehenden Ausführungen behilflich sein.

Mit freundlichen Grüßen
Im Auftrag
gez. Röhr

Wer benötigt einen Datenschutzbeauftragten?

Ausführlich

(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln,

- **die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters** in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen**, oder
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung **besonderer Kategorien von Daten gemäß Artikel 9** oder
- von personenbezogenen Daten über **strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10** besteht.

Art. 37 DSGVO

Erwägungsgrund 97 der DSGVO

In welcher Form sind Datenschutzbeauftragte zu benennen?

Die DSGVO verlangt keine Schriftform der Bestellung.

Die DSGVO spricht von der Benennung | früher Bestellung § 4f Absatz 1 Satz 1 BDSG a.F. geregelt

Bestellung ist empfehlenswert:

Aus Beweisgründen und zur Rechtsklarheit ist eine schriftliche Benennung von Datenschutzbeauftragten jedoch empfehlenswert.

Empfehlung: Aufgabendefinition des DSB in (Dienstleistungs-)Vertrag explizit festhalten.

Dies dient der Klarstellung der Aufgaben zwischen Verantwortlichem und Datenschutzbeauftragten

Art. 37 DSGVO

Erwägungsgrund 97 der DSGVO

§ 5 BDSG Benennung § 38 BDSG Datenschutzbeauftragte nichtöffentlicher Stellen

DATENSCHUTZBEAUFTRAGTER | DSB - FRIST DER BENENNUNG

Innerhalb welcher Frist sind Datenschutzbeauftragte zu benennen?

Der DSB ist sofort zu benennen, wenn ein Grund vorliegt oder sobald die Voraussetzungen zur Benennung auftritt.

Dies leitet sich aus dem fehlen einer Frist in der DSGVO ab.

Anmerkung:

- Bereits erfolgte Benennungen nach dem BDSG werden vor diesem Hintergrund Bestand haben.
- Stellung und Aufgaben von Datenschutzbeauftragten werden nun aber nach der DS-GVO bzw. der JI-RL auszurichten sein.

Empfehlung: Eine (formale) Neubestellung zur Klarstellung unter dem Regime der neuen Rechtsordnung ist zu empfehlen

Art. 37 DSGVO

Erwägungsgrund 97 der DSGVO

§ 5 BDSG Benennung
§ 38 BDSG Datenschutzbeauftr. nichtöffentlicher Stellen

Welche Voraussetzungen muss ein Datenschutzbeauftragter erfüllen?

Die Mindestqualifikationen des Datenschutzbeauftragten sind:

- umfassende Kenntnis des Datenschutzrechts
- umfassende Kenntnis der Anwendung des Datenschutzrechts
- Kenntnis der technischen und organisatorischen Maßnahmen und Verfahren
- Die fachlichen Anforderungen an den Datenschutz durch Technik
- Kenntnisse der datenschutzrechtlichen Voreinstellungen für Datensicherheit (Provacy by Default and Design)

Art. 37 DSGVO Satz 5

Art. 38 DSGVO Stellung

Art. 39 DSGVO Stellung

Erwägungsgrund 97 der DSGVO

Kenntnisse und/oder Berufserfahrung im betreffenden Vereins / Wirtschaftsbereich

- Der DSB muss im Stande sein die spezifischen Verarbeitungsprozesse zu erfassen
- Behördliche Datenschutzbeauftragte sollten dementsprechend ein fundiertes Fachwissen im Bereich der Verwaltung vorweisen können und die internen Prozesse gut kennen.
- solides Fachwissen in Bezug auf das IT-System und IT-Sicherheitsmaßnahmen
- datenschutzrechtlichen Bedürfnisse erkennen
  datenschutzrechtlichen Bedürfnisse im Arbeitsalltag berücksichtigen
- Das erforderliche Niveau des Fachwissens richtet sich insbesondere nach den durchgeführten Verarbeitungsvorgängen
- dem erforderlichen Schutz für die personenbezogenen Daten

Wichtig: Je komplexer Datenverarbeitungen im Einzelfall sind oder je größer die Menge sensibler Daten ist, desto höhere Anforderungen sind an das notwendige Fachwissen des Datenschutzbeauftragten zu stellen.

Welche Voraussetzungen muss ein Datenschutzbeauftragter erfüllen?

Weitere Qualifikationen | Kenntnisse

- sektorspezifischen Kenntnis des Datenschutzrechts in seinem Handlungsumfeld (Gesundheitswesen, Zahnarztpraxis, Energieunternehmen, Verein, Non Profit Organisationen)

Anmerkung: Die Qualifikationsprofile sind so zwar nicht konkret in die DSGVO aufgenommen worden, sind aber vom Düsseldorfer-Kreis , der Art. 29 Gruppe sowie vom BGH klar definiert

TIP: In der praktischen Anwendung kann es dennoch keine Abstriche bei der Qualifikation geben. Es läuft also im Idealfall auf einen Datenschutzbeauftragten hinaus, der über **umfassende Kenntnisse im Datenschutzrecht** und den **Rechtswissenschaften** im allgemeinen sowie der Informatik verfügt.

Art. 37 DSGVO Satz 5

Erwägungsgrund 97 der DSGVO

§ 5 BDSG Benennung
§ 38 BDSG Datenschutzbeauftr. nichtöffentlicher Stellen

AUFGABEN DES DSB

Die Aufgaben eines externen Datenschutzbeauftragten hängen von unterschiedlichen Faktoren ab.

Die drei wesentlichen Hauptaufgaben des DSB

- Unterrichtung und Beratung des Unternehmens | Vereins | Organisation
- Überwachung der Einhaltung von datenschutzrechtlichen Vorgaben
- Kontrolle für die Einhaltung der **datenschutzrechtlichen Bestimmungen bezüglich des Umgangs mit personenbezogenen Daten** bei der verantwortlichen Stelle
- Beratung und Überwachung im Rahmen der Datenschutz-Folgenabschätzung

Weitere Hauptaufgaben sind

- Ansprechpartner im Unternehmens | Verein| Organisation, zu Fragen zum Thema Datenschutz für Verantwortliche, Mitarbeiter und Betroffene (Kunden, Lieferanten, Mitglieder, Sponsoren …)
- Ansprechpartner für die Aufsichtsbehörden

Art. 39 DSGVO

Erwägungsgrund 97 der DSGVO

Grundsätzlich gilt: Je größer das Unternehmen und je komplexer die Datenverarbeitung, desto umfangreicher und vielseitiger gestalten sich die typischen Aufgaben und Tätigkeitsbereiche eines externen Datenschutzbeauftragten.

AUFGABEN DES DSB

- Einbeziehen in **alle relevanten betrieblichen Planungs- und Entscheidungsabläufe**
- **Pflicht zur Kontrolle und Überwachung** der Abläufe auf die **Einhaltung der Datenschutzbestimmungen**
- regelmäßige Schulung der Beschäftigten **hinsichtlich des Datenschutzes**
- informiert regelmäßig intern über Datenschutzrichtlinien, Bekanntmachungen
- **Gesamtüberblick über sämtliche Verfahrensverzeichnisse**
- **Überwachung der rechtmäßigen Entsorgung und Löschung**
- zuständig für Aufbau einer Datenschutzorganisation
- 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.

STELLUNGNAHME DES BGH ZUM DATENSCHUTZBEAUFTRAGTEN

BGH und der Daten-schutzbeauftragte aus Ende 2018

BGH Urteil sieht mit der DSGVO

- die „Tätigkeit von Datenschutzbeauftragten ist schwieriger…“
- die herausgehobene Bedeutung des Amtes eines Datenschutzbeauftragten
- die Verantwortung des Datenschutzbeauftragten
- die Anforderungen an seine Qualifikation

Der BGH sieht den Kern- und Schwerpunkt des DSB in:

- Auslegung und Anwendung der datenschutzrechtlichen Vorgaben
- sowie in der Überwachung der Einhaltung dieser Vorgaben

Anmerkung: Dabei wurde insbesondere herausgearbeitet, dass der Pflichtenkreis und die Komplexität der Rechtsfragen sich gegenüber der alten Rechtslage vor der DSGVO deutlich **erhöht haben.**

Der BGH sieht daraus abgeleitet das Fachwissen gegenüber dem technischer Fachkunde als dominierend an.

Keine Vorgaben der DSGVO auf das „WIE“ der Erlangung der Kennnisse

- Die DSGVO verzichtet auf Vorgaben, wie Datenschutzbeauftragte die notwendige fachliche Qualifikation erwerben sollen.
- Schulungen und Zertifikate sind nicht verpflichtend,
- im Prinzip wäre auch ein Selbststudium möglich.
- Es ist jede Fortbildungsmaßnahme zu begrüßen, die der Aufrechterhaltung oder dem Erwerb der Fachkunde dienlich sein kann.

Aus Stellungnahme LDI-NRW 05-2019

- Eine Empfehlung für bestimmte Fortbildungsmaßnahmen kann nicht getätigt werden.

HAFTUNG DES DSB

Haftung interner DSB:

Ein interner Datenschutzbeauftragter haftet mit der sogenannten beschränkten Arbeitnehmerhaftung.

Das bedeutet, dass der Arbeitnehmer lediglich bei Vorsatz und grober Fahrlässigkeit in vollem Umfang haftet. **Bei leichtester Fahrlässigkeit scheidet eine Haftung des internen DSB aus.**

Achtung bei Konzerndatenschutzbeauftragten: Im Fall, das ein angestellter – also interner – Beauftragter für Datenschutz gleichzeitig andere Unternehmen im Konzern oder Verband betreut.

Sofern der Datenschutzbeauftragte hier nicht angestellt ist, ist er bei diesen Unternehmen oder Verband dann externer Datenschutzbeauftragter.

Haftung externer DSB

Der externe Datenschutzbeauftragte ist im Gegensatz zum internen Datenschutzbeauftragten beim Auftraggeber nicht angestellt. Ein externer Datenschutzbeauftragter profitiert demnach nicht vom „innerbetrieblichen Schadenausgleich“.

Im Gegensatz zum internen DSB haftet ein externer DSB für seine Beratung auch bei leichter Fahrlässigkeit in voller Höhe. Dies führt zu einer Risikominimierung für das Unternehmen. *(d.h.i.R. Haftung nur für Falschberatung, deshalb entsprechende Versicherung für Berater notwendig!)*

Wer von einem Unternehmen **als interner (betrieblicher) oder externer** Datenschutzbeauftragter bestellt wird, nimmt gemäß der Datenschutz-Grundverordnung (DSGVO) **nicht nur eine beratende Funktionen im Unternehmen ein, sondern auch eine überwachende.**

HAFTUNG DES DSB

Keine Haftung für:

- Der DSB übernimmt keine Haftung für die Datenverarbeitung des Verantwortlichen
- und haftet damit nicht für die Datenschutzverstöße des Verantwortlichen.

Grund: Im Rahmen seiner Stellung kann der Beauftragte für Datenschutz keine Weisungen erteilen und demnach Ursachen für Verstöße gegen das Datenschutzrecht nicht selbst abstellen.

Schadensansprüche gegen den Datenschutzbeauftragten:

Das Unternehmen sowie auch die Betroffene können Schadensersatzansprüche geltend machen:

Wichtig: Der externe Datenschutzbeauftragte haftet für die Erfüllung der Aufgaben und der ihm vertraglich auferlegten Pflichten in vollem Umfang.

STRAFRECHTLICHE HAFTUNG DES DSB

Welche strafrechtlichen Aspekte betreffen den Datenschutzbeauftragten?

- Mangels Weisungsbefugnis kann er nicht **sich nicht direkt strafbar machen**
- Beihilfe zur Straftat ist jedoch bei bewusster Duldung einer datenschutzrechtlich unzulässigen Aktion möglich

Beispiel: Das wäre insbesondere dann der Fall, wenn der Datenschutzbeauftragte eine datenschutzrechtlich unzulässige Aktion – aus welchen Gründen auch immer – bewusst zulässt oder „durchgehen lässt“.

JURISTISCHE PERSONEN ALS DATENSCHUTZBEAUFTRAGTE

Aus Stellungnahme LDI-NRW 05-2019

Können juristische Personen als Datenschutzbeauftragte benannt werden?

Erwägungsgrund 97 der DSGVO

Die Benennung juristischer Personen als Datenschutzbeauftragte ist unzulässig, da

- Wortlaut und
- Systematik der DSGVO
  nur natürliche Personen als Datenschutzbeauftragte vorsehen
- Benennung nach Art. 37 nur nach Qualifikation und Fachwissen.
  Nur natürliche Personen können die nötige „berufliche“ Fachkunde und Zuverlässigkeit aufweisen und nur zu diesen ist eine
- vertrauliche Beziehung der Beteiligten sind nur zu natürlichen Personen möglich.

Wichtig – Hilfspersonal darf sein: Die zu Datenschutzbeauftragten benannten natürlichen Personen dürfen jedoch Hilfspersonal einsetzen, wie etwa Vertreter, Datenschutzansprechpartner und Koordinatoren.

Info: Die Artikel 29 Gruppe wurde nach Art.68 DSGVO am 25.Mai 2018 durch den **Europäischen Datenschutzausschuss abgelöst.**

DATENSCHUTZBEAUFTRAGTER | STELLUNG

Welche Position hat der Datenschutzbeauftragte im Unternehmen?

- Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.
- Der Verantwortliche und der Auftragsverarbeiter unterstützen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 39, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen.
- Der DSB ist nicht Weisungsgebunden
- **Ansprechpartner** bei Bedenken und Fragen zum Datenschutz im Verein/Unternehmen
- der DSB ist **unabhängiges Kontrollorgan**
  Kontrolle für die Einhaltung der **datenschutzrechtlichen Bestimmungen bezüglich des Umgangs mit personenbezogenen Daten** bei der verantwortlichen Stelle

Art. 38DSGVO

Erwägungsgrund 97 der DSGVO

§ 5 BDSG Benennung
§ 38 BDSG Datenschutzbeauftr. nichtöffentlicher Stellen

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.

Art. 39 DSGVO

Erwägungsgrund 97 der DSGVO

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 | 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.

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.

Begriffsbestimmungen sind zu finden in § 46 BDSG

WER MUSS MITGEZÄHLT WERDEN?

Unsere E-Mail vom 19. März 2019 an den LDIS

Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

LfDI Baden-Württemberg · Postfach 10 29 32 · 70025 Stuttgart

Datum 20. Mai 2019
Name Frau Röhr
Durchwahl 0711/615541-36
Aktenzeichen D 3050/729
(Bitte bei Antwort angeben)

Per E-Mail

Herrn
Hans-Jürgen Schwarz

Datenschutzrechtliche Anfrage, Ergänzungsfragen
Ihre E-Mail vom 19. März 2019
Unser Schreiben vom 23. Oktober 2018, Az. D 3050/729

Sehr geehrter Herr Schwarz,

ergänzend zu Art. 37 Abs. 1 lit. b) und c) der Datenschutz-Grundverordnung
GVO) benennen der Verantwortliche und der Auftragsverarbeiter eine Date
beauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel n
zehn Personen ständig mit der automatisierten Verarbeitung personenbez
ten beschäftigen, vgl. § 38 Abs. 1 S. 1 des Bundesdatenschutzgesetzes (

„Ständig" beschäftigt ist eine Person, wenn sie für diese Aufgabe auf lär
vorgesehen ist und sie entsprechend wahrnimmt. Irrelevant ist, ob die F
Verein beschäftigt oder ehrenamtlich tätig ist. Die Aufgabe braucht auc
aufgabe der Person zu sein. Das Tatbestandsmerkmal „ständig" ist da
füllt, wenn die Aufgabe selbst nur gelegentlich anfällt, die betreffende
stets wahrzunehmen hat. Ständig bedeutet daher, dass die Person i
der Verarbeitung personenbezogener Daten beschäftigt ist, wenn di
fällt. Nachlesen können Sie diese Beschreibung in unserem Praxisratgeber (S. 6),
der wie folgt unter der unten genannten Stelle u. a. auch zu dieser Frage abrufbar ist.

Verarbeitet ein Verein (Verband) ganz oder teilweise automatisiert personenbezogene Daten seiner Mitglieder und sonstiger Personen oder erfolgt eine nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, ist nach Art. 2 Abs. 1 DS-GVO deren Anwendungsbereich eröffnet, vgl. unsere unten genannte Orientierungshilfe auf S. 5.

Zu Ihrer Ergänzungsfrage a):
Unter der Voraussetzung, dass der Wanderwart stets die Kontaktdaten aufnimmt und diese z. B. in einem Dateisystem verarbeitet (z. B. Karteikasten), zählt auch diese Person zu den unter § 38 Abs. 1 S.1 BDSG genannten 10 Personen.

Zu Ihrer Ergänzungsfrage b):
Auch für Auftragsverarbeiter trifft dies zu.

Zu Ihrer Ergänzungsfrage c):
Dateisystem ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob die Sammlung zentral, dezentral oder nach funktionalen oder geographischen Gesichtspunkten geordnet geführt wird (Art. 4 Nr. 6 DS-GVO). Dazu zählen auch Papier-Akten; vgl. S. 6 der u. g. Orientierungshilfe. Es hängt also mit der Ablage des Formblattes zusammen: Eine alphabetische Reihung wäre dazu ausreichend.

Abschließend verweisen wir auch auf unsere Veröffentlichungen zum Datenschutz in Vereinen im Internet, z. B.

- die Orientierungshilfe, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf,
- den Praxisratgeber, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-für-Vereine.pdf,
- die FAQs, https://www.baden-wuerttemberg.datenschutz.de/faq-vereine/.

Wir hoffen, wir konnten Ihnen mit den oben stehenden Ausführungen behilflich sein.

Mit freundlichen Grüßen
Im Auftrag
gez. Röhr

DER DATENSCHUTZKOORDINATOR

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

Lassen Sie sich dies in der nächsten Mitgliederversammlung legitimieren!

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:

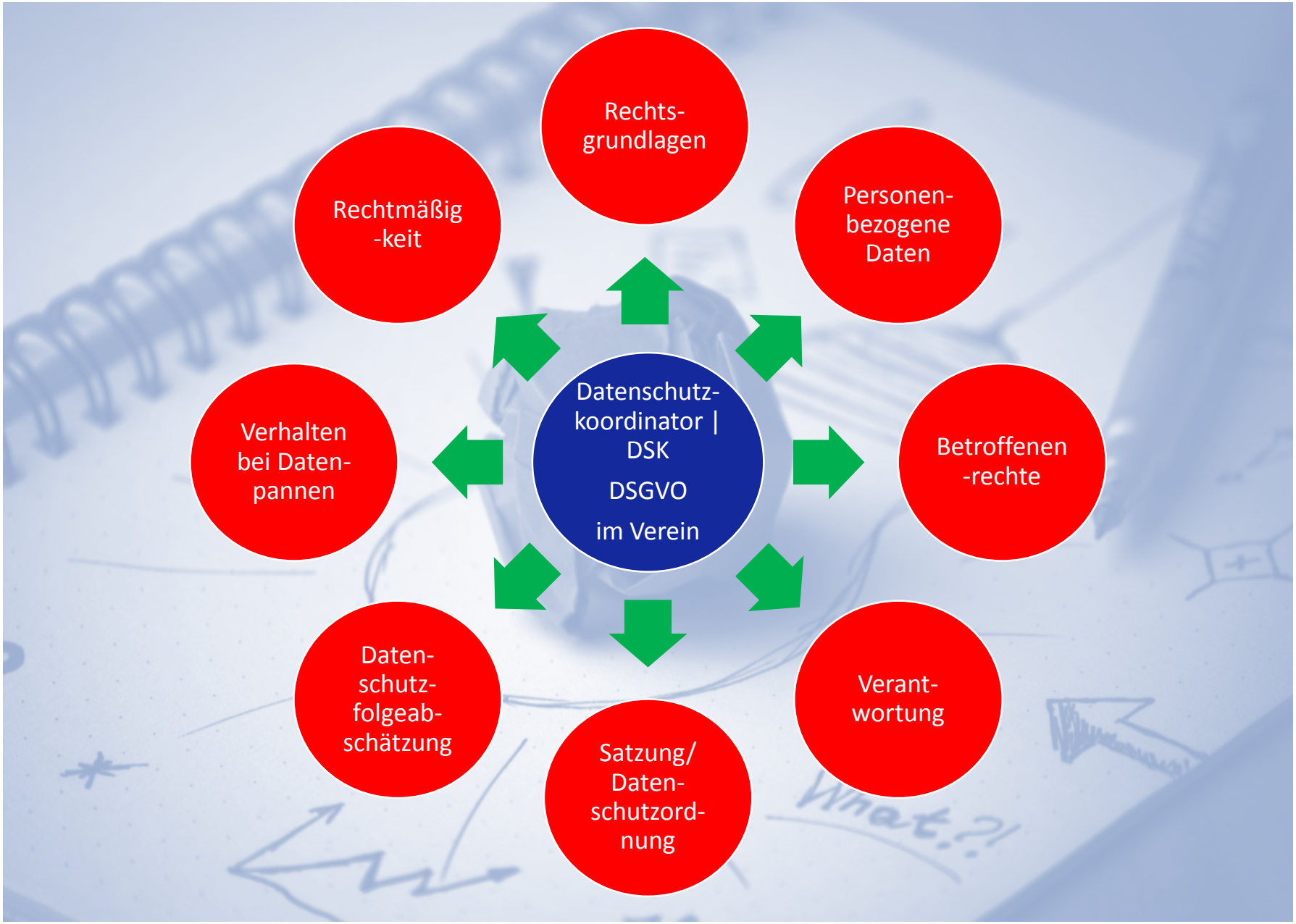
- Integration der Anforderungen der DSGVO in die vereinsinternen Abläufe
- notwendige neue Strukturen und Abläufe erarbeiten und vorschlagen
- datenschutzkonforme Entscheidungen treffen
- fundierte Einschätzungen vornehmen
- Zusammenhänge und Folgen abschätzen

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

Datenschutzinformationszentrale des bvve für Vereine im Stadt oder Landkreis
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 des bvve für Vereine im Stadt oder Landkreis

Externer Datenschutzbeauftragte des bvve e.V.

als zentraler externer DSB für die Vereine

finanziert über Fördergelder der Städte, Kommunen und des Landes – das ist der Wunsch!

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!

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**

DATENPANNEN

ZIEL

Erkennen, wann, wo und von wem personenbezogene Daten weitergegeben und übermittelt werden.

INHALTE

Definition einer Datenpannen
Meldefristen einer Datenpanne
Notwendigkeit der Betroffeneninformation

GESETZLICHER HINTERGRUND

Art.33 – EU-DSGVO – Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Art. 32 Abs. 1 Datenschutz-Grundverordnung deshalb auf, geeignete technische und organisatorische Maßnahmen zur Sicherung der personenbezogenen Daten zu treffen

DATENPANNEN

- Die Meldung muss spätestens nach 72 Stunden, nach Bekanntwerden der Datenpanne gemeldet werden. 365/12/24
- Die Meldung an die Behörde kann nur unterbleiben, wenn voraussichtlich kein Schaden den Betroffenen entstehen.
- Bei größeren Verstößen müssen auch die Betroffenen benachrichtigt werden
- Es besteht die Pflicht zur Schadensminimierung gegenüber den Betroffenen

DIE HERAUSFORDERUNG

Verpflichtung zur Führung von Verfahrensverzeichnissen

ERHEBUNG DER PERSONENBEZOGENEN DATEN

ERHEBUNG PERSONENBEZOGENER DATEN

Prozesse der Daten des Unternehmen / Vereins:

- Welche Daten werden verarbeitet?
- Wo werden die Daten verarbeitet?
- Wie werden die Daten verarbeitet?
- Wofür werden die Daten verarbeitet?
- Wer hat Zugang zu den Daten?
- Darf der Verantwortliche die Daten überhaupt in Besitz halten?

= Rechtmäßigkeit der Verarbeitung

CHECKLISTE VVT I

CHECKLISTE – GRUNDLAGEN DER DATENERHEBUNG

Die Datenschutzrichtlinie beinhaltet
in erster Linie die Prozesse der Daten des Unternehmen / Vereins:

Auszug und Beispiele aus typischen Prozessen

- Welche Daten werden erhoben?
- Welche Daten werden verarbeitet?
- Wo werden die Daten erhoben?
- Wo werden die Daten verarbeitet?
  Vereinsgeschäftsstelle / Homeoffice
- Wer erhebt die Daten?
- Wer verarbeitet die Daten?
- Welche Datenkategorien werden erhoben?
- Welche Datenkategorien werden verwendet?
- Welche Felder sind in welcher Datenkategorie?
- Wohin werden die Daten übermittelt / weitergegeben?
- Wie werden die Daten verarbeitet | IT / manuell?
- Wofür werden die Daten verarbeitet | Zweck?
- Wer hat Zugang zu den Daten?
- Wer hat welche Funktion?
- Wer ist in seiner Funktion auf das Datengeheimnisverpflichtet?
- Wie werden die Daten geschützt?
- Darf der Verantwortliche die Daten überhaupt in Besitz halten?
  Rechtmäßigkeit der Verarbeitung

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.

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.

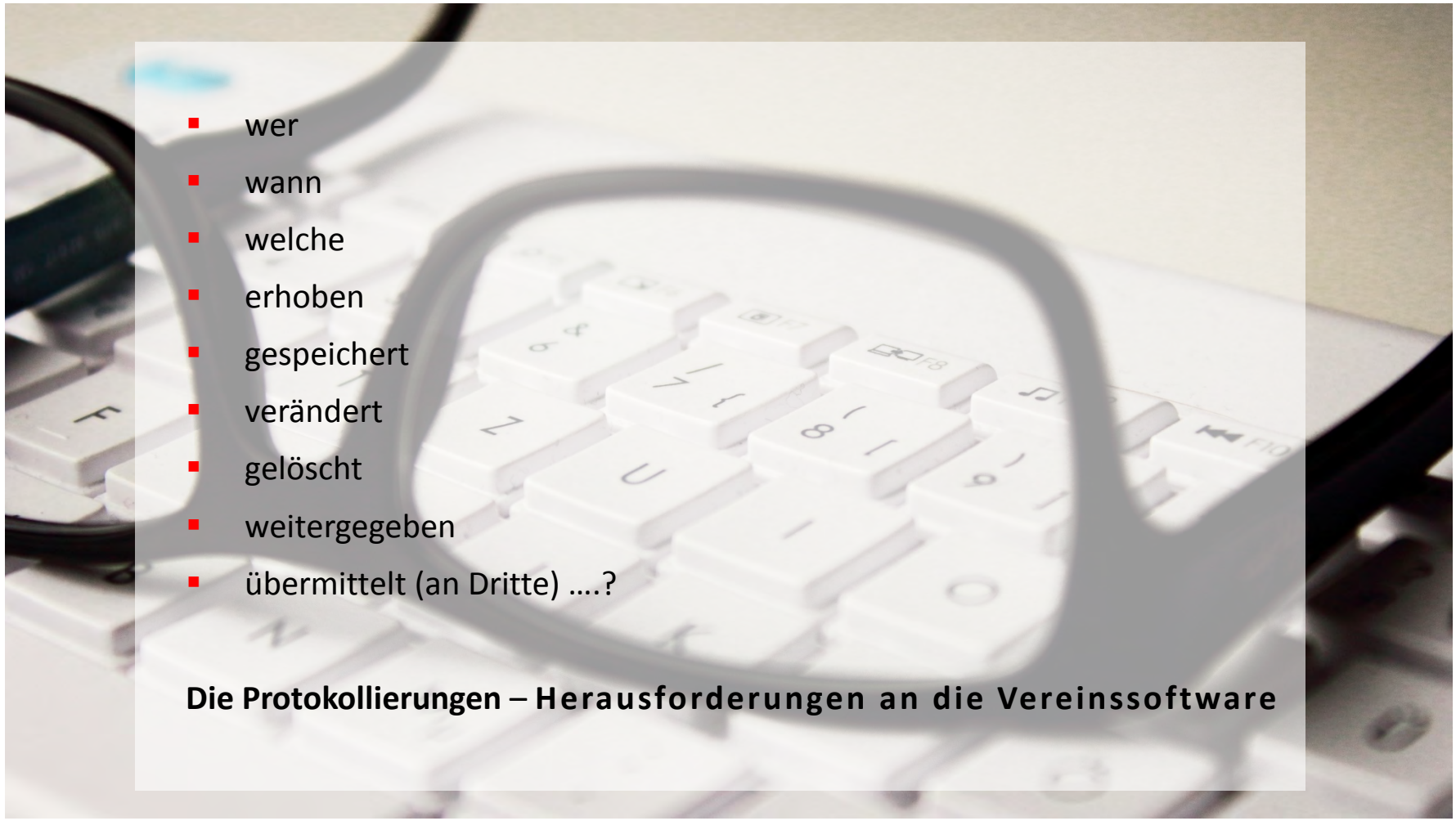
Bei einer nur geringen Zweckänderung muss geprüft werden, ob eine bereits bestehende Beschreibung einer Verarbeitungstätigkeit angepasst werden muss oder ob eine vollständig neue Beschreibung anzufertigen ist.

➔ Die Summe der Einzelbeiträge ergibt das Verzeichnis von Verarbeitungstätigkeiten.

IT-Sicherheitskonzepte

PROTOKOLLIERUNGEN

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



Kontrolle | Protokollierungen

TOM |
TECHN. - ORG.
MAßNAHMEN

ZIEL

Notwendige technisch-organisatorische Maßnahmen für die Verarbeitung personenbezogener Daten definieren und umsetzen.

INHALTE

Zutrittskontrolle
Zugangskontrolle
Zugriffskontrolle
Weitergabekontrolle
Auftragskontrolle
Eingabekontrolle
Verfügbarkeitskontrolle
Datentrennung

GESETZLICHER HINTERGRUND

Art. 32 DSGVO | Sicherheit der Verarbeitung

Passende Erwägungsgründe

(75) Risiken für die Rechte und Freiheiten natürlicher Personen (76) Risikobewertung (77) Leitlinien zur Risikobewertung (78) Geeignete technische und organisatorische Maßnahmen (79) Zuteilung der Verantwortlichkeit (83) Sicherheit der Verarbeitung

BDSG § 64 n.F. Anforderungen an die Sicherheit der Datenverarbeitung

ZUTRITTS-KONTROLLE	ZUGANGS-KONTROLLE	ZUGRIFFS-KONTROLLE	WEITERGABE-KONTROLLE	AUFTRAGS-KONTROLLE	EINGABE-KONTROLLE	VERFÜGBARKEITS-KONTROLLE	DATENTRENNUNG

TECHNISCH ORGANISATORISCHE MAßNAHMEN

TOM |
TECHN. - ORG.
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)

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),

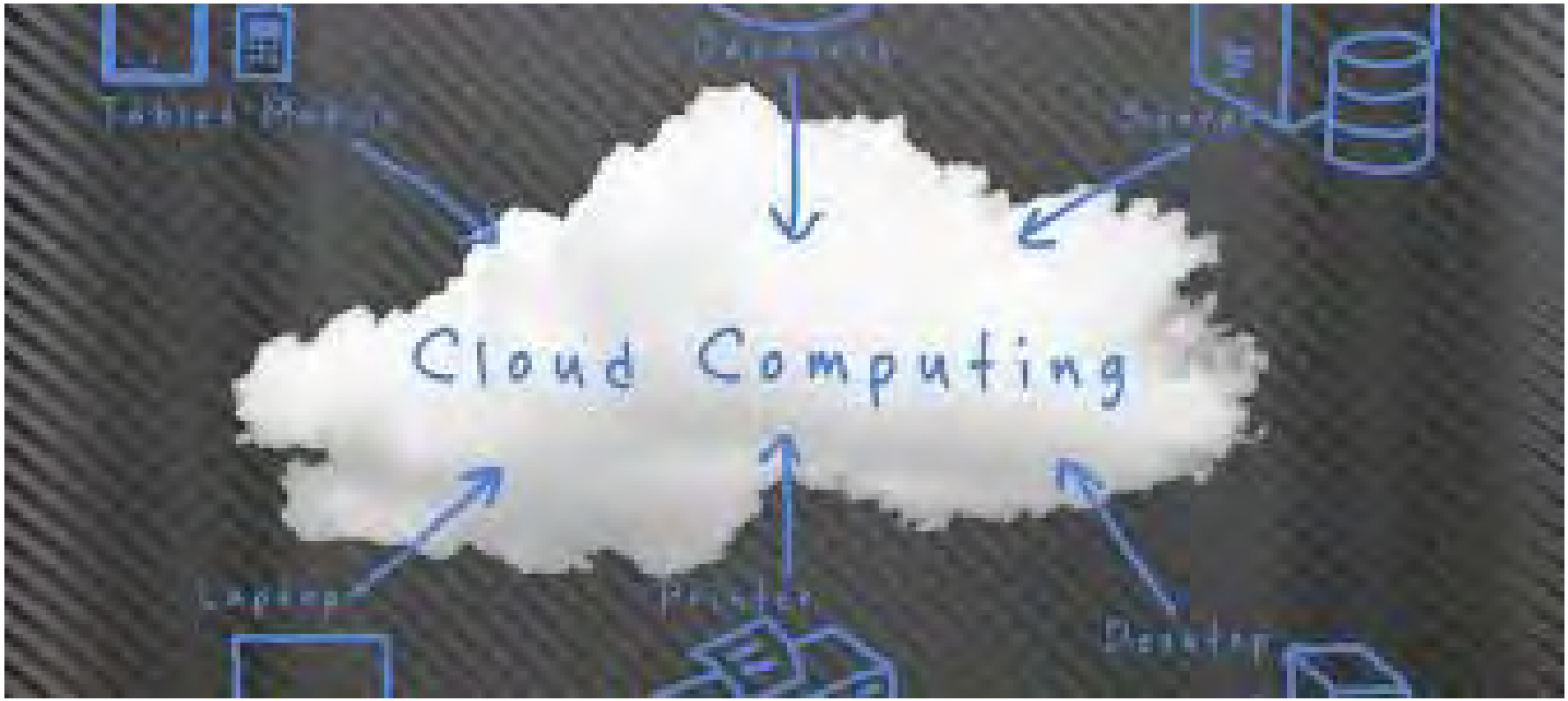
MINDESTANFORDERUNGEN AV | ART. 28 DSGVO

- 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.

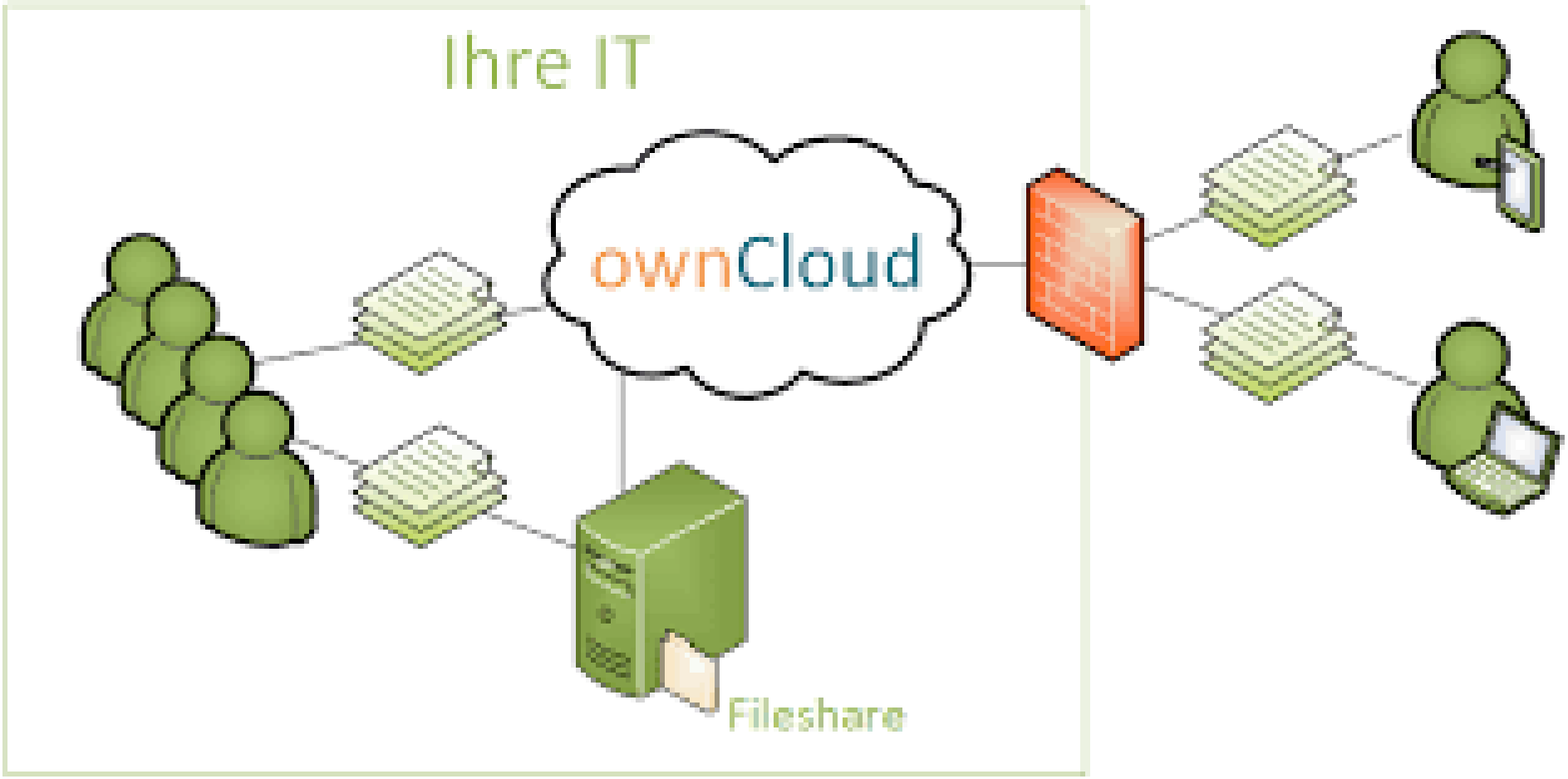
Vertrag über Auftragsverarbeitung
– Hauptvertrag- Generalvertrag
- Unterverträge für fallbasierende Themen generieren

CLOUD COMPUTING

Filesharing und zentrale Verwaltung in der Cloud



OWNCLOUD IM VEREIN



T

CHECKLISTE DOKUMENTATION

Status des Datenschuzes Stand anhand der Checkliste Übergabestatuzs

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 _____

_____

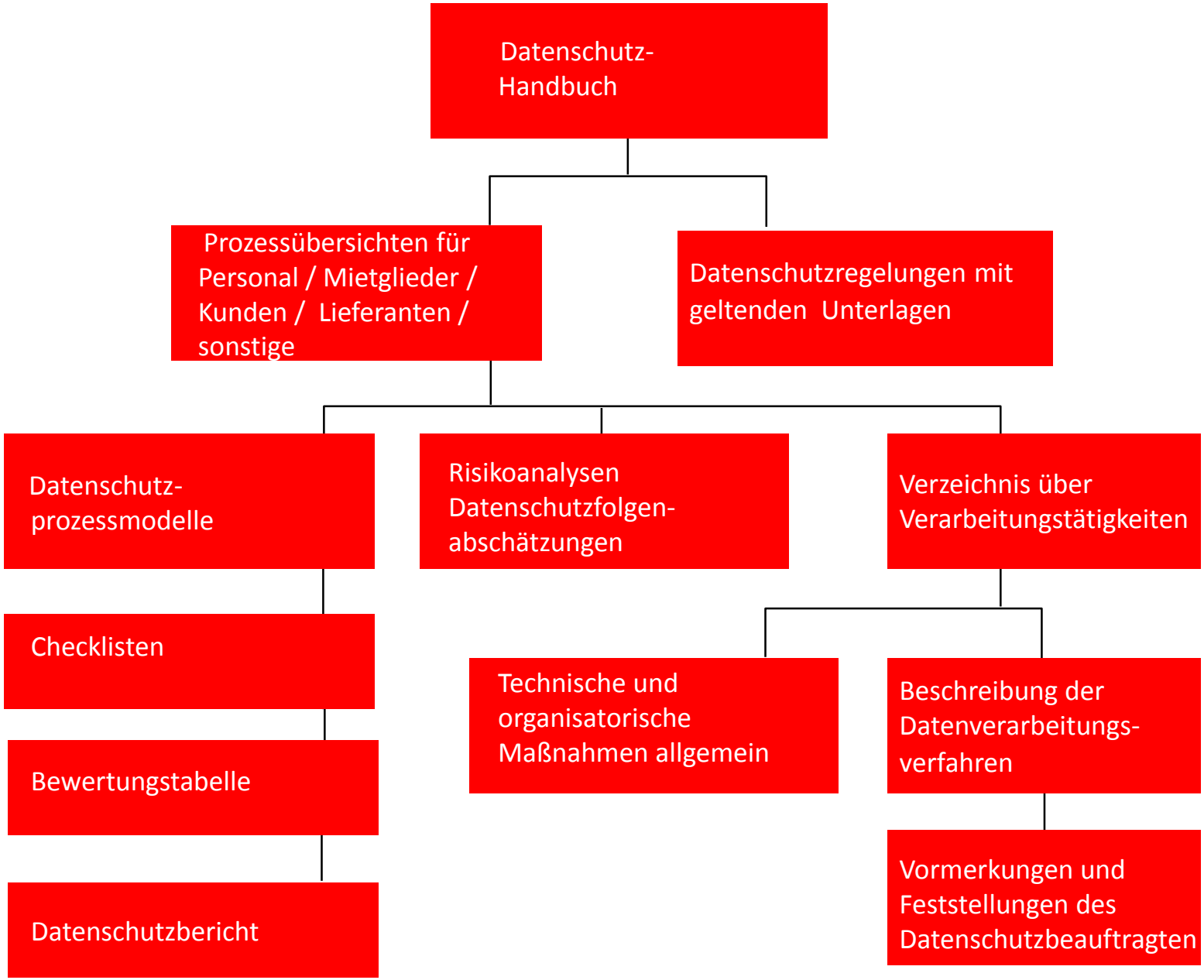
[ ] Sonstige Dokumentationen – wenn ja, welche _____

_____

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

DATENSCHUTZHANDBUCH | DATENSCHUTZMANAGMENTSYSTEM

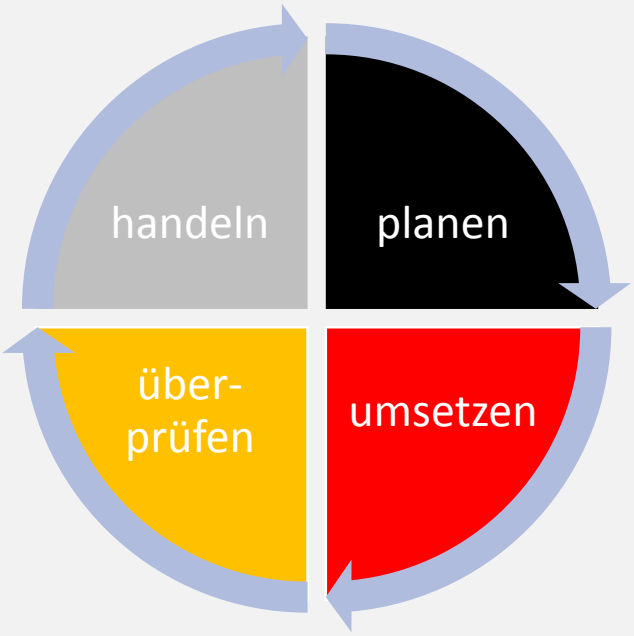
DAS DATENSCHUTZHANDBUCH



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



VIELEN DANK,

dass Sie da sind …

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

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

