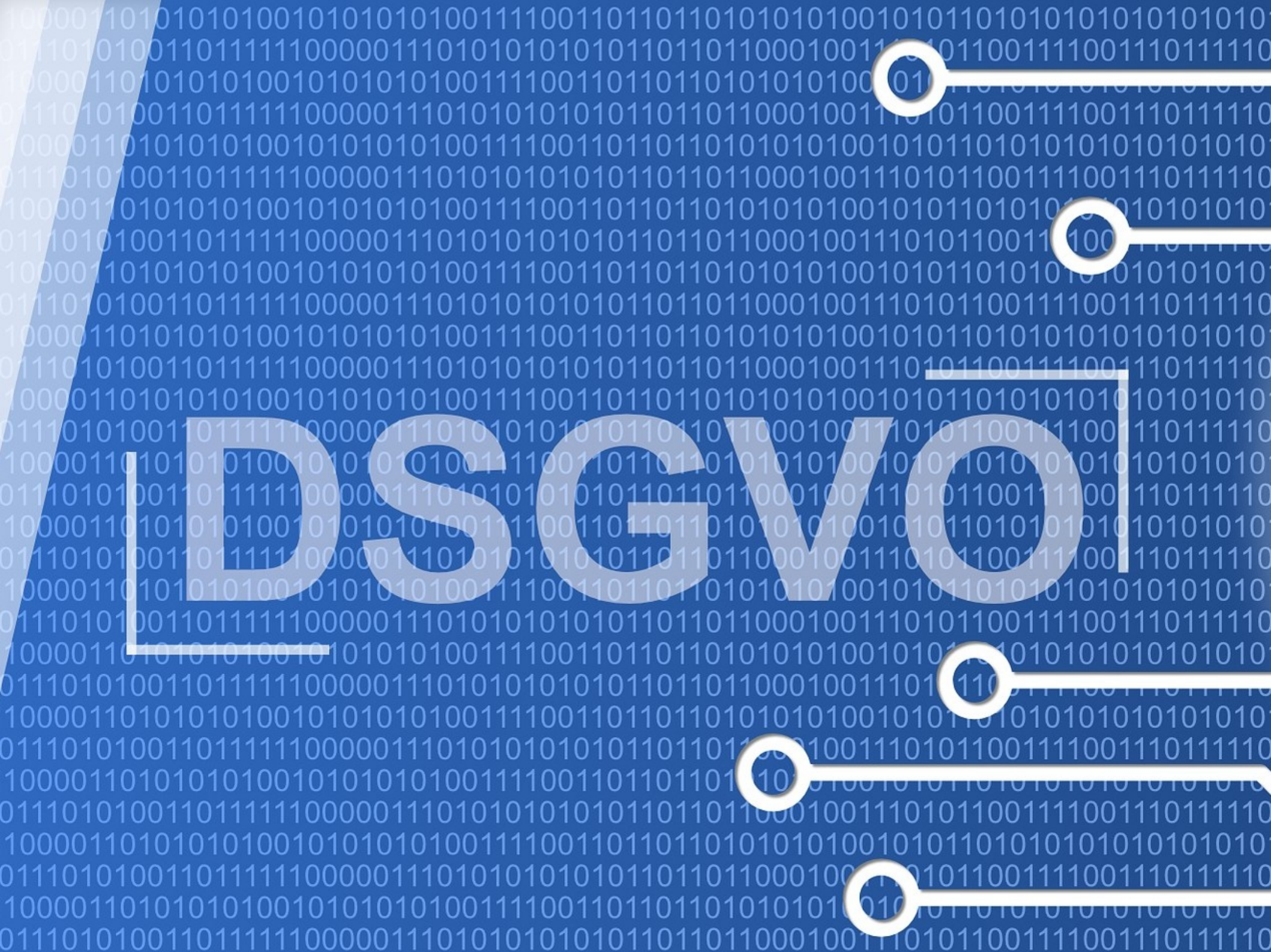
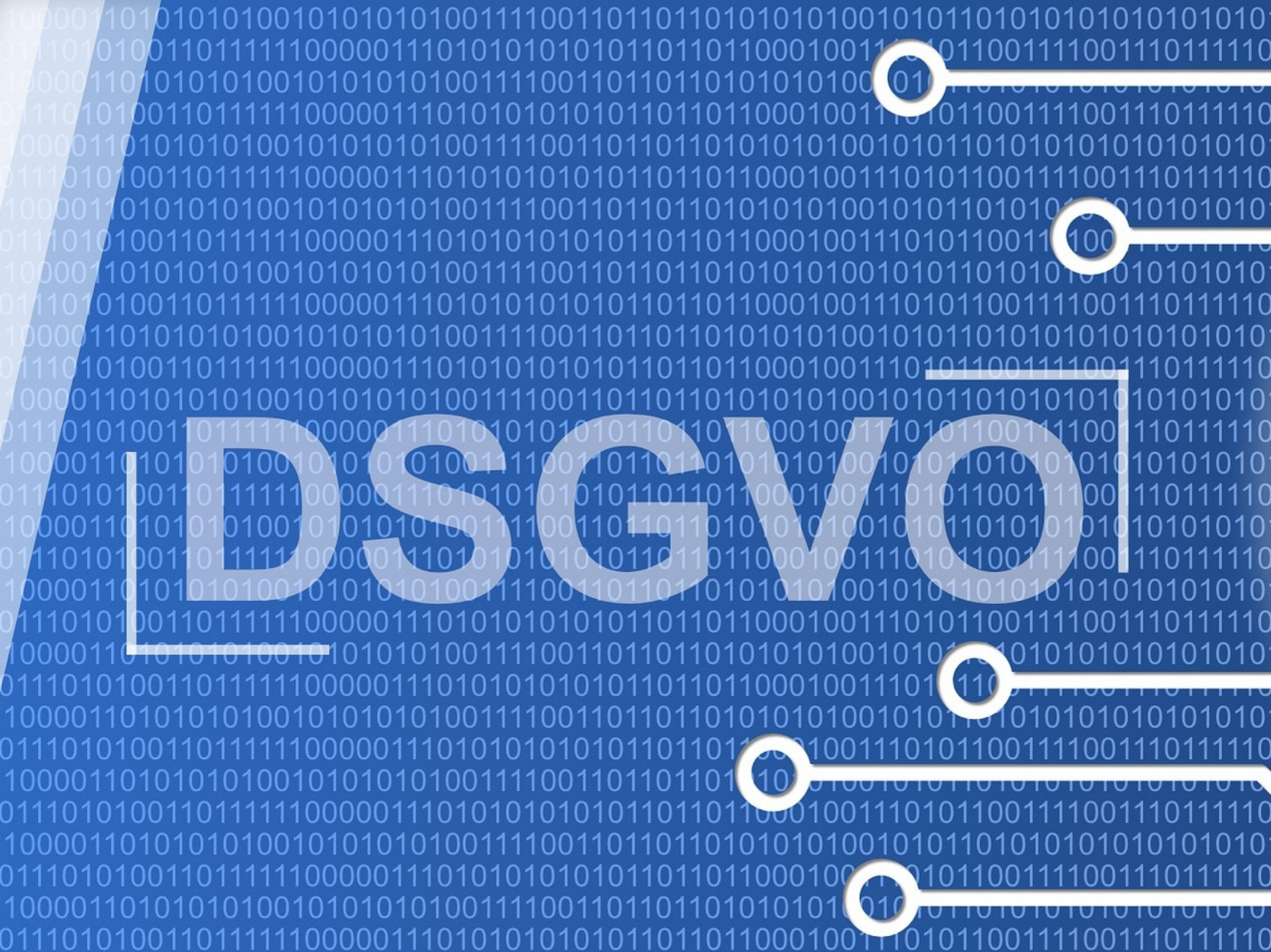

DSGVO


DSGVO

Die EU-DSGVO im Verein

Maßgeschneiderte und praxisorientierte Seminare helfen Ihnen, Schritt zu halten:

Workshop - Schlau in 2 x 360 Minuten / 9 - 16 Uhr

Datenschutz: Die neue EU-DSGVO und ihre Umsetzung

960,- €

Nicht bei uns... hier gehts jetzt „all inklusive“ weiter...

Die EU-DSGVO im Verein

Eine Betrachtung der Änderungen und Aufgaben

nach dem 25.5.2018 für Vereine in Mecklenburg-Vorpommern

Erstellt in Zusammenarbeit mit dem

Landesdatenschutzbeauftragten des Landes Mecklenburg-Vorpommern

und der SELBSTHILFE MV e.V. *

Für die Vereine der

SELBSTHILFE Mecklenburg-Vorpommern e.V. Rostock

Referent: Christian Engelen

Teilnehmer der Allianz für Cyber-Sicherheit

*Trotz größter Sorgfalt bei der Erstellung der vorliegenden Übersicht kann keine Gewähr für die inhaltliche Richtigkeit und Vollständigkeit übernommen werden. STAND: Juni 2018

Die Situation vor dem 25.5.18

Datenschutz galt schon immer…

So auch ein Großteil der in der DSGVO enthaltenen Vorgaben!

Jetzt dreht sich die Beweislast…

Von: „Beweist mir mal, das ich was falsch gemacht habe...“
zu „Ok, Das hier sind meine Dokumente, die beweisen, dass alles richtig gelaufen ist.“

Mit dem Ergebnis von mehr Arbeit für alle.

Die EU-DSGVO im Verein

Diese Punkte werden wir heute näher besprechen

1. **Brauchen wir einen Datenschutzbeauftragten?**
2. **Was für Bußgelder müssen wir bei Verstößen befürchten?**
3. **Welche Maßnahmen müssen wir ergreifen?**
    1. **Auf unserer Website**
    2. **In unseren Anträgen, Infomaterial etc.**
    3. **Beim Zugriff auf unsere Daten**
    4. **Bei der Sicherheit der Mitgliederdaten**
    5. **Bei der Dokumentation / Aussendarstellung unserer Vereinsarbeit**
    6. **Weitere wichtige Vorsorgemaßnahmen**
4. **Neue Interne Abläufe / Dokumentationen**
5. **Diskussion / Fragen**

Brauchen wir einen Datenschutzbeauftragen?

Radio Eriwan vermeldet dazu: Jein

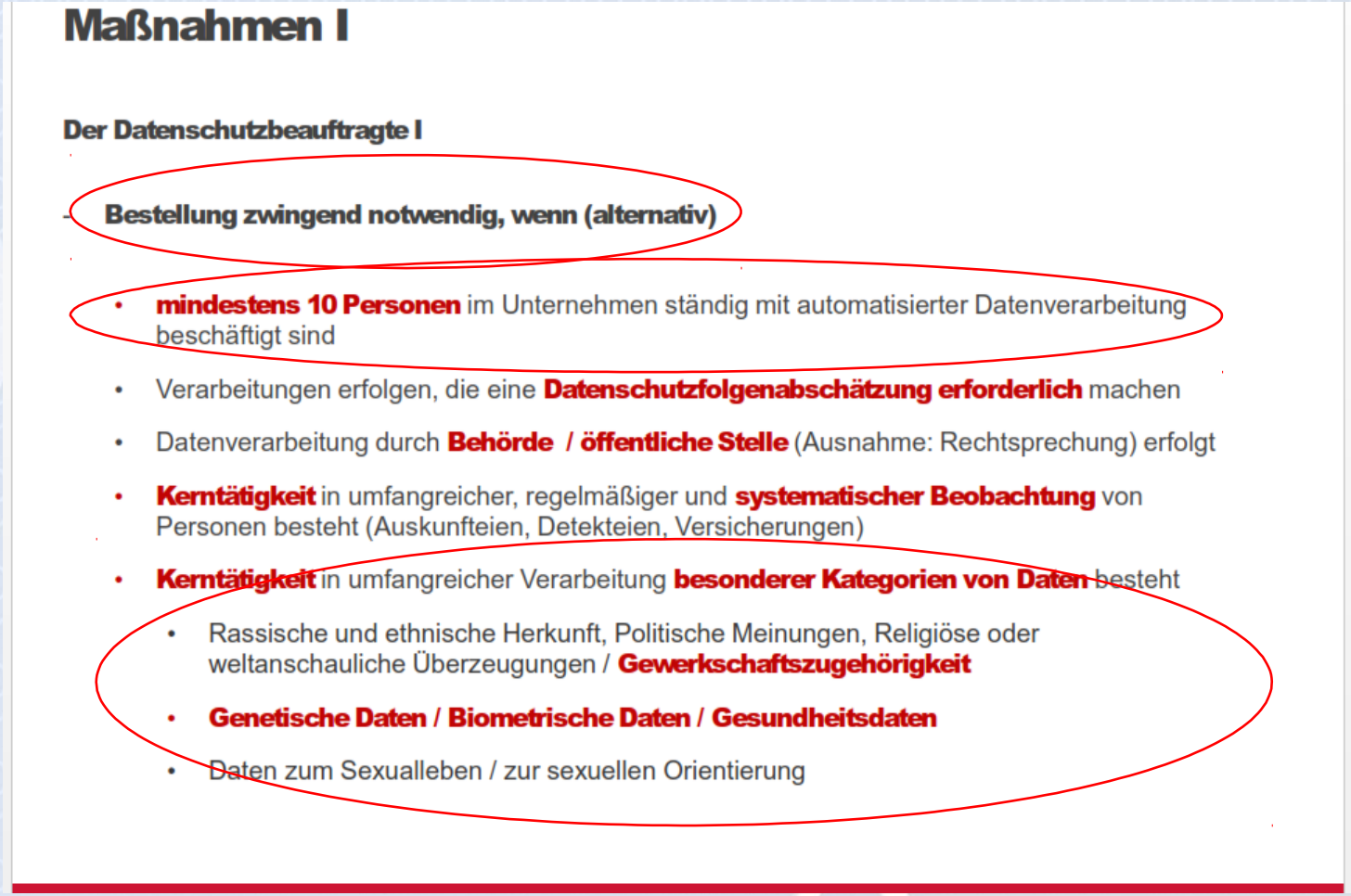
Die EU-DSGVO stellt in Art. 37 Abs. 1 folgende Voraussetzungen für die verpflichtende Bestellung eines Datenschutzbeauftragten:

(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn […]

c) die **Kerntätigkeit** des Verantwortlichen oder Auftragsverarbeiters **in der umfangsreichen Verarbeitung besonderer Kategorien von Daten** gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.“

Brauchen wir einen Datenschutzbeauftragen?

Das sagen bisherige Schulungen zu dem Thema (Ausschnitt aus Begleitmaterial)



Maßnahmen I

Der Datenschutzbeauftragte I

- **Bestellung zwingend notwendig, wenn (alternativ)**
  - **mindestens 10 Personen** im Unternehmen ständig mit automatisierter Datenverarbeitung beschäftigt sind
  - Verarbeitungen erfolgen, die eine **Datenschutzfolgenabschätzung erforderlich** machen
  - Datenverarbeitung durch **Behörde / öffentliche Stelle** (Ausnahme: Rechtsprechung) erfolgt
  - **Kerntätigkeit** in umfangreicher, regelmäßiger und **systematischer Beobachtung** von Personen besteht (Auskunfteien, Detekteien, Versicherungen)
  - **Kerntätigkeit** in umfangreicher Verarbeitung **besonderer Kategorien von Daten** besteht
    - Rassische und ethnische Herkunft, Politische Meinungen, Religiöse oder weltanschauliche Überzeugungen / **Gewerkschaftszugehörigkeit**
    - **Genetische Daten / Biometrische Daten / Gesundheitsdaten**
    - Daten zum Sexualleben / zur sexuellen Orientierung

Brauchen wir einen Datenschutzbeauftragen?

Die meisten Informationsveranstaltungen zum Thema DSGVO stellen die Situation derart dar, daß selbst die Speicherung von Krankheitsdaten oder Informationen zu spezifischen Krankheitsfeldern automatisch die Bestellung eines Datenschutzbeauftragten nach sich zieht.

Die Erwägungsgründe (EG) zur DSGVO sind Erläuterungen zum besseren Verständnis, die die EU herausgegeben hat. In EG 91, Satz 4 stellt die EU folgendes klar:

- *Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt.*

Wer jetzt vergleicht, wieviele sensible Daten ein normaler Hausarzt / Anwalt im Vergleich zu Ihrem Verein erhebt und verwaltet, sind aus dieser Analogie die ehrenamtlichen Strukturen NICHT verpflichtet, durch die Erhebung von z.B. spezifischen Daten zur Erkrankung eines Mitglieds einen Datenschutzbeauftragten zu bestellen.

Dies wurde auch so vom Landesdatenschutzbeauftragten MV bestätigt.

Brauchen wir einen Datenschutzbeauftragen?

Damit bleibt noch die Klärung, ob mehr als neun Personen regelmäßig mit den Daten der Mitglieder arbeiten.

Die DSGVO schreibt folgendes als einen Grund zur Bestellung eines DB vor:

- ***Es sind regelmäßig mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt***

Auch der Begriff der Verarbeitung wird definiert. Die Verarbeitung umfasst nach Art. 4 Nr. 2 DSGVO dabei

(…) 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 oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Hierzu zählt jeder, der mindestens wöchentlich umfangreich mit den Daten zu tun hat, egal ob Vorstand, Kassenwart, einfaches Mitglied oder Praktikant.

Umfangreich bedeutet jetzt aber nicht, daß ein Gruppenleiter eine Teilnehmerliste mit Adressen oder Anwesenheitsdaten führt bzw. ein Mailing erstellt und versandt wird.

Brauchen wir einen Datenschutzbeauftragen?

Also müssen Sie folgendes intern abklären:

- Wer braucht umfassenden Zugriff auf die vorhandenen Daten?
- Lässt sich dieser Personenkreis einschränken?
- Dokumentieren Sie die Personen im Verfahrensverzeichnis

Immer mit der Maßgabe, nicht über neun Personen regelmäßig mit den Daten hantieren zu lassen.

Müssen wir Bußgelder befürchten?

Bisherige Schulungen zeigten erschreckende Szenarien, wie hoch Bußgelder angeblich sein werden

Änderungen zum BDSG IV

Bußgelder II

- **Höhe**
  - bis zu € 20.000.000 oder
  - bis zu 4% des gesamten, weltweit erzielten Jahresumsatzes
  - je nachdem, welcher der Beträge höher ist

- **Bei Verstößen gegen**
  - Grundsätze für die Verarbeitung, einschließlich Einwilligu
  - Rechte der betroffenen Personen
  - Übermittlung personenbezogener Daten an einen Empfä internationale Organisation
  - Alle Pflichten gemäß den Rechtsvorschriften der Mitglie Öffnungsklausel erlassen wurden (bspw. Bestellung eine
  - Nichtbefolgen einer Anweisung der Aufsichtsbehörde
  - Nichtgewährung des Zugangs für die Aufsichtsbehörde

Bußgelder III

→ Neue Faustregel der Aufsichtsbehörden: Faktor 66,6?

- Übermittlung personenbezogener Daten in die USA
  - Adobe (Acrobat Reader) € 8.000
  - Unilever € 11.000
  - Punica € 9.000

- Keinen Datenschutzbeauftragten bestellt / Fragen nach Krankheitsgrund
  - Drogerie Müller € 137.500

- Ankauf von Listen mit Daten und datenschutzwidrige Nutzung
  - DEBEKA € 1,3 Mio. Bußgeld zzgl. € 600.000,00 Zustiftung

- Videoüberwachung der Mitarbeiter
  - Lidl € 1,46 Mio.
    (Einzelbußgelder zwischen € 10.000 und € 310.000)

Müssen wir Bußgelder befürchten?

Unsere Recherchen zu diesem Thema, die insbesondere auf direkten Gesprächen mit dem Landesdatenschutzbeauftragten basieren, zeigen folgendes:

Der Landesdatenschutzbeauftragte wird auch mit Anwendung der DSGVO seine bisherige Arbeitsweise nicht ändern.

Diese sieht im Falle von Verstößen folgende Vorgehensweise vor:

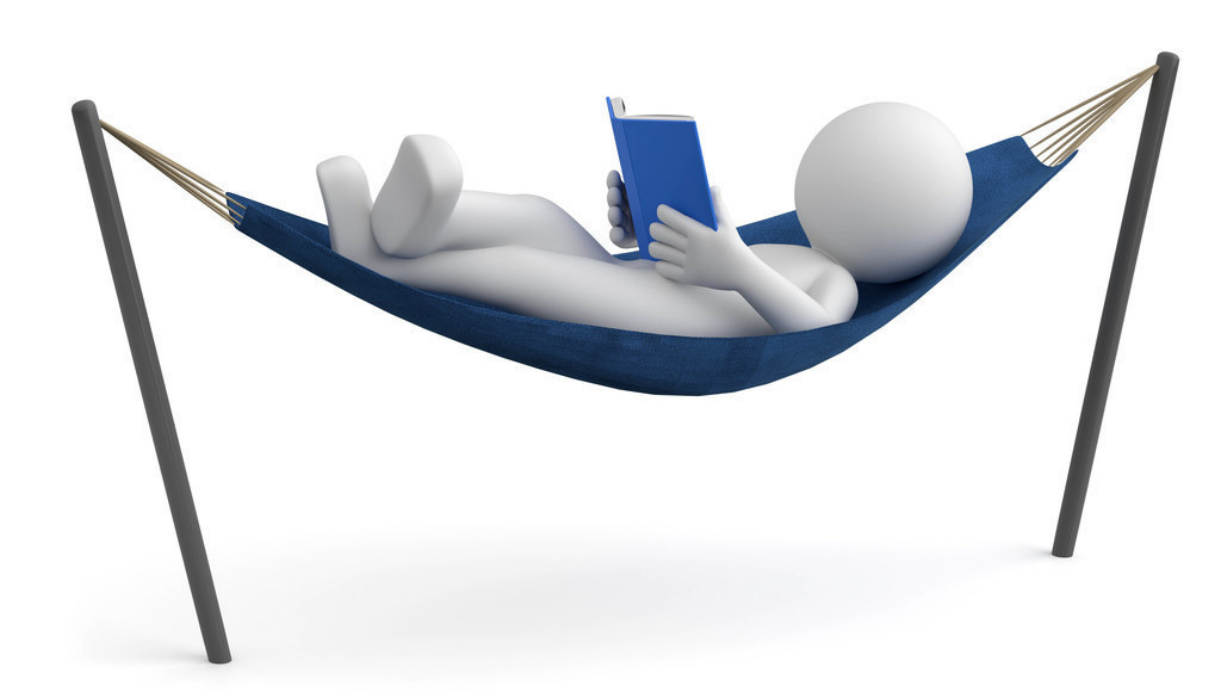
1. **Aufklärung der Situation und Belehrung des Verursachers/Verantwortlichen mit Fristsetzung zur Behebung.**
2. **Falls nichts bzw. nicht ausreichend reagiert wird, erfolgt eine behördliche Anordnung mit Fristsetzung, die Mißstände abzustellen.**
3. **Erst wenn diese zwei Aufforderungen ins Leere laufen, kommen Bußgelder in Betracht.**

Allerdings greift im letzteren Fall die Maxime, daß „**Bußgelder angemessen und verhältnismäßig sein sollen**“. Daraus folgt, daß ein kleiner Verein, der ausschließlich ehrenamtlich geführt wird auch immer nach seiner Leistungsfähigkeit im Bezug auf die Erbringung eines zu verhängenden Bußgeldes beurteilt wird.

Merksatz: **Lasst es gar nicht erst zu Stufe drei kommen !!!**

Müssen wir Bußgelder befürchten?

Eher nicht, nur eine kleine Pause ...



Maßnahmenkatalog

Thema: Website / Internetauftritt

Gerade die öffentlich zugänglichen Medien (Website, Broschüren, Flyer etc.) sind Für die unrühmliche Gilde der Abmahner Angriffsziele, da diese sich leicht automatisiert abrufen und auswerten lassen und dann eventuell zu einer Abmahnung führen können.

Ganz wichtig: **Sollten Sie eine Abmahnung bekommen:**

Sofort rechtlichen oder fachlich kompetenten Beistand suchen. Rufen Sie in der Geschäftsstelle an. **Nicht zahlen oder irgendetwas unterschreiben !!!**

In den meisten derzeit bekannten Fällen ist die Abmahnung nicht rechtssicher, also angreifbar da der Abmahnende meist nur vorgeschobene Gründe wie das Wettbewerbsrecht angibt. Dies zieht in unserem Geschäftsfeld nicht und kann abgewendet werden.

Maßnahmenkatalog

Thema: Website / Internetauftritt

Ihre Internetseite sollte folgendes aufweisen:

1) Einen auf der Startseite auffällig plazierten Link/Menüpunkt zu Ihrer
2) DSGVO konformen Datenschutzerklärung
3) Ein eventuell vorhandenes Kontaktformular sollte eine ausführliche Datenschutzbelehrung, zumindest aber einen zwingenderweise zu bestätigenden Haken besitzen, der bestätigt, das der Kontaktsuchende VOR dem Absenden die Datenschutzerklärung gelesen und verstanden hat.
4) Sozial Media Links wie facebook/Twitter/usw. MÜSSEN so eingebunden werden, daß in keinem Fall unbemerkt und unerlaubt Daten irgendeiner Art an diese Dienste übertragen werden. (Beispiel: „c´t shariff“ Script)
5) Auswertungsdienste wie Google Analytics oder die Google Webfonts sind weitere Kandidaten, zu deren Einsatz Sie eine ausdrückliche Zustimmung der Besucher benötigen.

Maßnahmenkatalog

Thema: Anträge/Infomaterial

Ihre Aufnahmeanträge müssen seit Mai entweder eine Datenschutzerklärung enthalten oder einen Auszug derselben mit Verweis auf Ihre Internetseite mit der kompletten Erklärung.

Ebenso gilt dies für Flyer, die ein Rückmeldungsformular enthalten oder ähnliches.

Dokumente, die der Außendarstellung dienen, sollten nur Bildmaterial enthalten, dessen Herkunft geklärt und genehmigt ist.

Maßnahmenkatalog

Thema: Zugriff auf Daten

Natürlich muß ein Verein mit den erhobenen Daten arbeiten. Allerdings sollte sichergestellt werden, daß ein Unbefugter -also Besucher, Praktikant oder Mitglied- keinen absichtlichen oder versehentlich Einblick in schützenswerte Daten erhält.

Es ist wichtig, alle Geräte und Materialien, die Daten von Mitgliedern enthalten, jederzeit verschlossen und unzugänglich aufzubewahren.

Maßnahmenkatalog

Thema: Zugriff auf Daten

Es genügt normalerweise, wenn z.B. die Mitgliedsdaten in verschlossenen Aktenschränken verwahrt werden, zu denen nur der Vorstand Zugriff hat.

Elektronische Verarbeitungsgeräte (kurz PC, Tablet oder ähnliches) müssen mindestens mit einem Passwort und einem kurzzeitig (z.B. nach 5 Min.) aktiviertem Bildschirmschoner mit Passwortabfrage geschützt werden.

Wichtig ist dies auch, damit sichergestellt werden kann, daß nicht mehr als die erlaubten neuen Mitarbeiter mit den Daten arbeiten können.

Maßnahmenkatalog

Thema: Sicherheit der Mitgliedsdaten

Ergänzend zu den vorgenannten Punkten betrifft dies die IT-Sicherheit. Auch diese wird jetzt strikt gefordert.

Einige von Ihnen haben bereits Erfahrungen mit defekten Computern aller Art machen müssen. Da ist auf einmal die jahrelang zuverlässige Festplatte nicht mehr ansprechbar, da löscht jemand unbedacht den falschen Ordner auf der Festplatte oder ein Virus macht Daten unbrauchbar.

Gegen alle diese und ähnliche Schwierigkeiten muss man heute vorbereitet sein. Was allerdings nicht schwer oder teuer sein muß.

Beispiel: Die Vereinsverwaltung wird auf einem PC im Büro gemacht. Dieser Raum ist verschließbar. Von den Daten wird jede Woche per Software eine Sicherung der veränderten Daten gemacht und einmal im Monat eine Komplettsicherung. Diese Sicherung erfolgt auf eine externe Festplatte, die dann bei einem Vorstandsmitglied (nicht im Büro) verschlossen wird.
Damit sind schon mehr als 90 % der oben genannten Probleme gelöst.
Kosten: Externe Festplatte ca. 70 Euro, Zeit und etwas Hirnschmalz.

Maßnahmenkatalog

Thema: Dokumentation/Außendarstellung

Einiges hierzu hatten wir bereits vorher angesprochen. Jetzt geht es um das aktuell kontrovers diskutierte Problem: **Was ist mit Film und Fotomaßnahmen?**

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat einen **Vermerk** herausgegeben, der sich der Problematik des Fotografierens in der Öffentlichkeit widmet. Hierbei geht es nicht um Aufnahmen zu journalistischen oder rein privaten Zwecken. Letztere unterfallen gem. Art. 2 Abs. 2 lit. c ohnehin nicht der DSGVO. Vielmehr geht es um das Fotografieren einer unüberschaubaren Anzahl von Menschen oder von solchen, die als Beiwerk auf einem Foto zu erkennen sind. Der für jeden Smartphone-Besitzer relevante Fall.

IV. Ergebnis
Die derzeitige Rechtslage in Bezug auf Fotografien einer unüberschaubaren Anzahl von Menschen oder von Menschen als Beiwerk anderer Motive ist überwiegend unsicher. Dies beruht insbesondere darauf, dass der deutsche Gesetzgeber bisher keinen ausdrücklichen Gebrauch von der Öffnungsklausel des Art. 85 Abs. 2 DSGVO gemacht hat. Dies wäre aber im Sinne der Rechtssicherheit nötig.
Bis dahin ist es möglich, die Datenerhebung in den meisten Fällen über Art. 6 Abs. 1 lit. f DSGVO zu rechtfertigen. ***Eine Informationspflicht gegenüber den Abgelichteten besteht nicht. Dies ergibt sich aus Art. 11 Abs. 1 DSGVO, hilfsweise aus Art. 14 Abs. 5 lit. b DSGVO.***

Maßnahmenkatalog

Thema: Dokumentation/Außendarstellung

Das Oberlandesgericht (OLG) Köln hat sich als offenbar erstes deutsches Gericht zu der aktuell sehr umstrittenen Frage geäußert, ob das Kunsturhebergesetz (KUG) auch nach Geltung der Datenschutzgrundverordnung (DSGVO) anwendbar ist.

Erfreulicherweise hat das Gericht diese Frage bejaht (OLG Köln, Beschl. v. 18.06.2018, Az. 15 W 27/18).

Zumindest im journalistischen Bereich schließe die DSGVO die Anwendung des KUG nicht aus. Denn das KUG erlaube eine umfassende Abwägung der betroffenen Grundrechte.

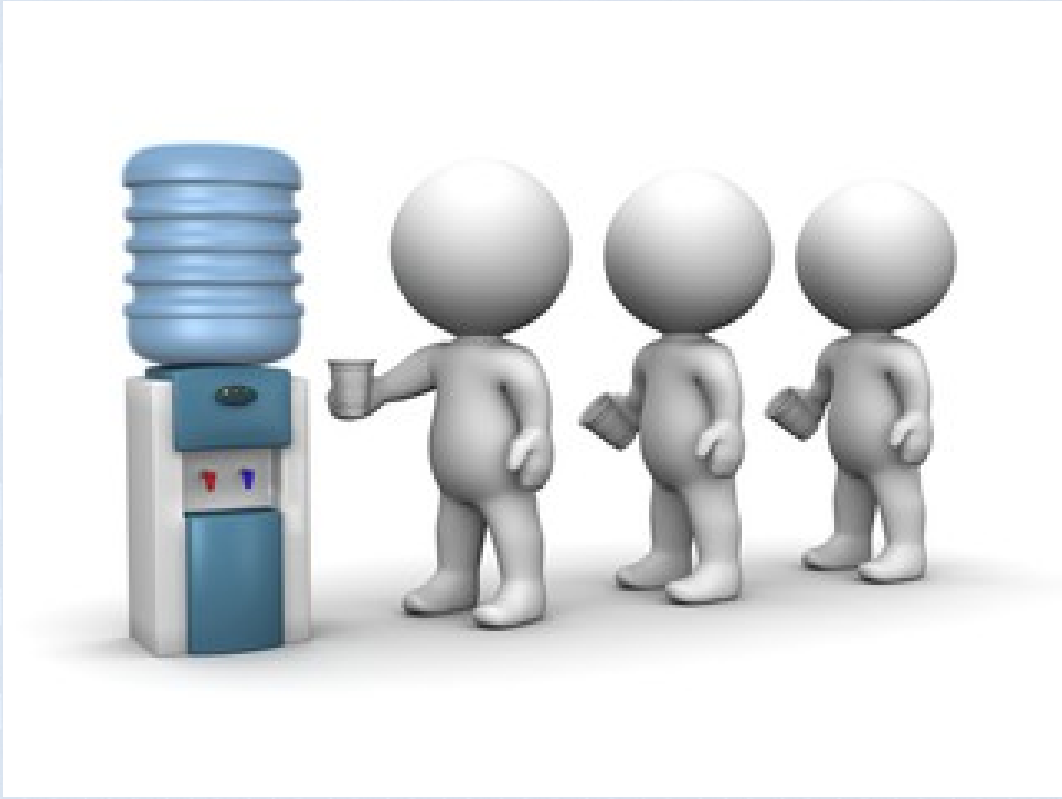
KUG § 23 (Auszug)

(1) Ohne die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:

1. Bildnisse aus dem Bereiche der Zeitgeschichte;
2. Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
3. Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;

Maßnahmen...

Eine kleine Pause wäre vielleicht sinnvoll?



Dokumentation

Thema: Dokumentationspflicht

Auch den Vereinen der Selbsthilfe wird ein Mindestmaß an Dokumentation abverlangt. Hierzu gehören:

1) Verfahrensverzeichnis
2) IT-Sicherheitskonzept
3) Verpflichtung der Mitarbeiter
4) sowie der beteiligten Unternehmen und eventuell
5) Vorbereitungen für Externe Anfragen

Dokumentation

Thema: Verfahrensverzeichnis

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

Bayerisches Landesamt für Datenschutzaufsicht

Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

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

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

Vorstand: Dieter Eckbauer-Düppels, geb. 03.12.1952

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

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virenscanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder

Dokumentation

Thema: IT-Sicherheitskonzept

Technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)
1. Pseudonymisierung
2. Verschlüsselung
3. Gewährleistung der Vertraulichkeit
4. Gewährleistung der Integrität
5. Gewährleistung der Verfügbarkeit
6. Gewährleistung der Belastbarkeit der Systeme
7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall
8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Es liegen schriftlich vor

- ☐ interne Verhaltensregeln
- ☐ Risikoanalyse
- ☐ allgemeine Datensicherheitsbeschreibung
- ☐ umfassendes Datensicherheitskonzept
- ☐ Wiederanlaufkonzept
- ☐ Zertifikat:
  Zertifizierungsstelle:
- ☐ Sonstiges:

Dokumentation

Thema: Mitarbeiter

Verpflichtung auf die Vertraulichkeit

Die einschlägigen gesetzlichen Vorschriften verlangen, dass personenbezogene Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden. Daher ist es Ihnen auch nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der Ihnen übertragenen Aufgaben erforderlich ist.

Nach diesen Vorschriften ist es untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugter Offenlegung oder unbefugtem Zugang führt.

Verstöße gegen die Datenschutzvorschriften können ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden. Entsteht der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen.

Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt einen Verstoß gegen arbeitsvertragliche Pflichten dar, der entsprechend geahndet werden kann.

Optional – Ihre Tätigkeit berührt das Fernmeldegeheimnis. Sie dürfen sich nicht über das erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation verschaffen. Sie dürfen derartige Kenntnisse grundsätzlich nicht an Dritte weitergeben.

Optional – Ihre Tätigkeit berührt das Sozialgeheimnis. Sofern Daten verarbeitet werden, die dem Sozialgeheimnis unterliegen, haben Sie diese im gleichen Umfang geheim zu halten, wie die ursprünglich übermittelnde Stelle.

Optional – Ihre Tätigkeit berührt die [anwaltliche/ärztliche/etc.] Schweigepflicht. Sie wirken an der beruflichen oder dienstlichen Tätigkeit eines Berufsgeheimnisträgers mit, soweit dies erforderlich ist. Es ist Ihnen untersagt, fremde Geheimnisse, namentlich zum persönlichen Lebensbereich gehörende Geheimnisse oder Betriebs- oder Geschäftsgeheimnisse unbefugt zu offenbaren.

Die Verpflichtung auf die Vertraulichkeit besteht auch nach der Beendigung des Beschäftigungsverhältnisses fort.

Frau/Herr _____ Abteilung/Tätigkeit _____

erklärt, in Bezug auf die Vertraulichkeit und Integrität personenbezogener Daten die Vorgaben der geltenden Datenschutzvorschriften einzuhalten.

Mit Ihrer Unterschrift bestätigen Sie zugleich den Empfang einer Kopie dieser Niederschrift nebst Anlage.

_____, _____ _____

Ort Datum Verpflichtete(r)

Anlage zur Verpflichtung auf die Vertraulichkeit

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim betrieblichen Datenschutzbeauftragten.

Begrifflichkeiten

Art. 4 Nr. 1 DS-GVO: „**Personenbezogene Daten**" [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Art. 4 Nr. 2 DS-GVO: „**Verarbeitung**" [meint] 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 oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Grundsätze der Verarbeitung

Art. 5 Abs. 1 lit. a DS-GVO: Personenbezogene Daten müssen [...] auf **rechtmäßige Weise**, nach Treu und Glauben und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz").

Art. 5 Abs. 1 lit. f DS-GVO: Personenbezogene Daten müssen [...] in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor **unbefugter oder unrechtmäßiger Verarbeitung** und vor unbeabsichtigtem **Verlust**, unbeabsichtigter **Zerstörung** oder unbeabsichtigter **Schädigung** durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

Art. 29 DS-GVO: Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten **ausschließlich auf Weisung** des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Art. 32 Abs. 2 DS-GVO: Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch **Vernichtung**, **Verlust** oder **Veränderung**, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte **Offenlegung** von beziehungsweise unbefugten **Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Art. 33 Abs. 1 Satz 1 DS-GVO: Im Falle einer **Verletzung** des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der [...] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Dokumentation

Thema: Auftragsdatenverarbeiter

Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

[Stand: Mai 2017]

Vereinbarung

zwischen dem/der

.....

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

.....

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

[ggf.: Vertreter gemäß Art. 27 DS-GVO:

.....]

Hinweis

„Die einzelnen Festlegungen nach Art. 28 Abs. 3 DS-GVO sollten vollständig in die Vereinbarung übernommen und wie eine Checkliste abgearbeitet werden. Die für das konkrete Dienstleistungsverhältnis zutreffenden Alternativen sollten angekreuzt werden. Leerfelder sind ggf. entsprechend des konkreten Auftrags auszufüllen. Vergütungs- und Haftungsregelungen zu den einzelnen Leistungen des Auftragnehmers sollten im Hauptvertrag vereinbart werden."

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/SLA/..... vom ....., auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: ..... (Definition der Aufgaben)

(2) Dauer

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum .....

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von ..... zum ..... gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom .....

oder

☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: .....

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in .....

- ☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);
- ☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);
- ☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);
- ☐ wird hergestellt durch genehmigte Verhaltensregeln (Artt 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);
- ☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).
- ☐ wird hergestellt durch sonstige Maßnahmen: ..... (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DS-GVO)

(2) Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

Dokumentation

Thema: Auskunftspflichterfüllung

Datenschutzrechtliche Selbstauskunft nach DSGVO

Betr: Name, Adresse, Sonstige Identifikationsmöglichkeit (z.B. Kundennummer, verwendete E-Mail-Adresse)

Sehr geehrte Damen und Herren,

nach Art. 15 DSGVO habe ich das Recht, von Ihnen eine Bestätigung darüber zu verlangen, ob Sie personenbezogene Daten über meine Person gespeichert haben. Sofern dies der Fall ist, so habe ich ein Recht auf Auskunft über diese Daten.

1. Auskunft über meine bei Ihnen gespeicherten Daten

Ich darf Sie in diesem Fall bitten, mir gemäß Art. 15 Abs. 1 DSGVO folgende Informationen mitzuteilen:

a) Welche Daten über meine Person konkret bei Ihnen gespeichert oder verarbeitet werden (z.B. Name, Vorname, Anschrift, Geburtsdatum, Beruf, medizinische Befunde).

b) Weiterhin wollen Sie mich bitte über die Verarbeitungszwecke meiner Daten ebenso informieren wie über

c) die Kategorien personenbezogener Daten, die bezüglich meiner Person verarbeitet werden;

d) die Empfänger oder Kategorien von Empfängern, die meine Daten bereits erhalten haben oder künftig noch erhalten werden;

e) die geplante Dauer für die Speicherung meiner Daten, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

f) über das Bestehen meiner Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung meiner Daten, ebenso wie über mein Widerspruchsrecht gegen diese Verarbeitung nach Art. 21 DSGVO und mein Beschwerderecht bei der zuständigen Aufsichtsbehörde.

g) Sofern die Daten nicht bei mir erhoben werden, fordere ich Sie auf, mir alle verfügbaren Informationen über die Herkunft der Daten mitzuteilen; sowie

h) mir darzulegen, ob eine automatisierte Entscheidungsfindung einschließlich Profiling gemäß Art. 22 DSGVO besteht. In diesem Fall wollen Sie mir bitte aussagekräftige Informationen über die involvierte Logik und die angestrebten Auswirkungen einer derartigen Verarbeitung für meine Person mitteilen.

i) Wurden meine personenbezogenen Daten an ein Drittland oder an eine internationale Organisation übermittelt, wollen Sie mir bitte mitteilen, welche geeigneten Garantien gemäß Art. 46 DSGVO im Zusammenhang mit der Übermittlung vorgesehen sind.

Bitte stellen Sie mir kostenfrei eine Kopie meiner bei Ihnen gespeicherten personenbezogenen Daten zur Verfügung. Sofern ich diesen Antrag elektronisch stelle und nichts anderes vermerke, so sind mir die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen.

2. Löschung meiner Daten

Weiterhin verlange ich nach Art. 17 DSGVO die **unverzügliche Löschung** meiner bei Ihnen verarbeiteten personenbezogenen Daten.

Die Voraussetzungen des Art. 17 DSGVO liegen nach meiner Ansicht vor. Sofern ich eine Einwilligung zur Verarbeitung meiner Daten erteilt habe, widerrufe ich diese hiermit, bzw. lege gemäß Art. 21 DSGVO Widerspruch gegen die Verarbeitung ein. Dies gilt ebenso für das Profiling gemäß Art. 22 DSGVO. Lehnen Sie die Löschung ab, so haben Sie dies mir gegenüber zu begründen.

Sofern Sie meine personenbezogenen Daten öffentlich zugänglich gemacht haben und gemäß Art. 17 Abs. 1 DSGVO zu deren Löschung verpflichtet sind, haben Sie angemessene Maßnahmen zu ergreifen, um sämtliche Empfänger meiner Daten darüber gemäß Art. 19 DSGVO zu informieren, dass ich die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien dieser personenbezogenen Daten verlangt habe.

3. Fristen und Rechtsfolgen

Auskunftserteilungen müssen gemäß Art. 12 Abs. 3 DSGVO unverzüglich erfolgen, spätestens aber innerhalb eines Monats. Sollte ich innerhalb dieser Frist keine Auskunft von Ihnen erhalten, so werde ich mich an die zuständige Aufsichtsbehörde wenden. Ich mache darauf aufmerksam, dass unterlassene oder nicht vollständige Auskunftserteilungen nach Art. 83 Abs. 5 DSGVO mit einer hohen Geldbuße bedroht sind.

Mit freundlichen Grüßen

Seminar

Thema: Weitere Fragen