scope & focus
Service-Gesellschaft mbH

Datenschutz-Anforderungen an Vereine

Dipl.-Ök. Stephan Rehfeld

1

scope & focus
Service-Gesellschaft mbH

Verantwortlichkeit – Art. 4 Nr. 7 DSGVO

„Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

2

scope & focus
Service-Gesellschaft mbH

Vereine und KMUs müssen die DSGVO und das BDSG-neu vollumfänglich beachten!

Es gibt (fast) keine Erleichterungen für Vereine und KMUs!

3

scope & focus
Service-Gesellschaft mbH

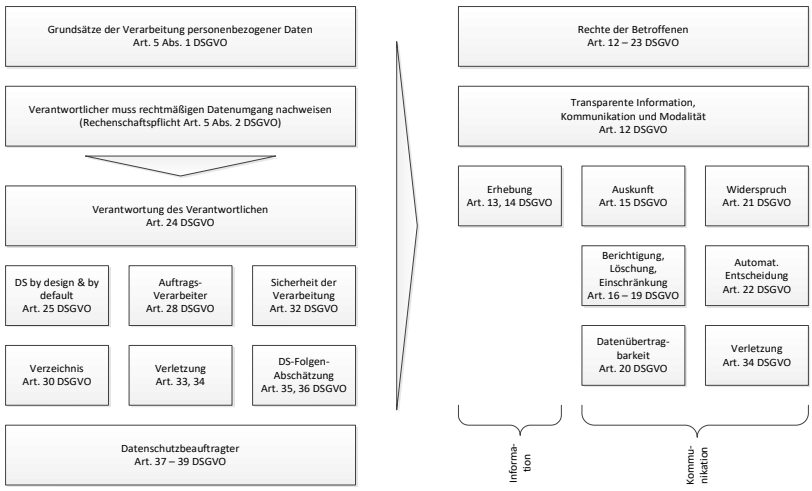
Personenbezogene Daten

„personenbezogene Daten“ 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;

4

scope & focus Service-Gesellschaft mbH

Beispiel: Mitgliederverwaltung



Kranig, Sachs, Gierschmann, Datenschutz-Compliance nach der DS-GVO, 2017, S. 25

5

scope & focus Service-Gesellschaft mbH

Datenschutz-Grundsätze

Abs. 1: Personenbezogene Daten müssen

a) auf rechtmäßige Weise … („Rechtmäßigkeit, Transparenz“);
b) für festgelegte, eindeutige und legitime Zwecke … („Zweckbindung“);
c) dem Zweck angemessen und erheblich … („Datenminimierung“);
d) sachlich richtig und erforderlichenfalls … („Richtigkeit“);
e) in einer Form gespeichert werden, die die Identifizierung … („Speicherbegrenzung“);
f) in einer Weise verarbeitet werden, … („Integrität und Vertraulichkeit“);

Abs. 2: Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

6

scope & focus
Service-Gesellschaft mbH

PRAKTISCHE UMSETZUNG

7

scope & focus
Service-Gesellschaft mbH

Praktische Umsetzung

Was ist zu tun?

- https://www.lfd.niedersachsen.de/download/131993/Checkliste_fuer_die_Umstellung_kleinerer_Unternehmen_auf_die_Datenschutzgrundverordnung.pdf

Grundregulierung - Muster zur GDD-Praxishilfe DS-GVO VIII

- https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_8.docx

8

scope & focus Service-Gesellschaft mbH

Literaturtipp

Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf

Hilfe zur Umsetzung für KMUs und Vereine:
https://www.lfd.niedersachsen.de/download/131993/Checkliste_fuer_die_Umstellung_kleinerer_Unternehmen_auf_die_Datenschutzgrundverordnung.pdf

Datenschutz im Verein nach der Daten-schutzgrundverordnung (DS-GVO)

Informationen über die datenschutzrechtlichen Rahmenbedingungen beim Umgang mit personenbezogenen Daten in der Vereinsarbeit

9

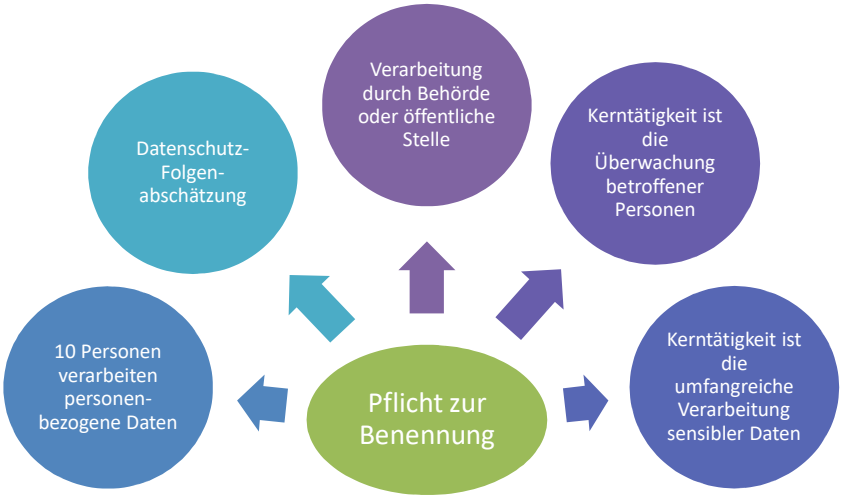
scope & focus Service-Gesellschaft mbH

Datenschutzbeauftragter

A Datenschutzbeauftragter (DSB)
Muss ein DSB vom Verein benannt werden?
☐ ja
☒ nein (weniger als 10 Personen im regelmäßigen Umgang mit personenbezogenen Daten)

10

Pflicht zur Benennung eines DSB



11

Datenschutzbeauftragter

DSK-Kurzpapier Nr. 12

- https://www.lfd.niedersachsen.de/download/126341

GDD-Praxishilfe DS-GVO I

- https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_1.pdf

Meldeformular

- https://nds.dsb-meldung.de/

12

Verzeichnis der Verarbeitungstätigkeiten (VVT)

B Verzeichnis von Verarbeitungstätigkeiten

Ist ein solches Verzeichnis erforderlich?

☒ ja (wegen der regelmäßigen Verarbeitung personenbezogener Daten)

☐ nein

13

Verzeichnis der Verarbeitungstätigkeiten (VVT)

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	28.02.2018	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
...	...	...	...	...	...	...	...	...	...

14

Verzeichnis der Verarbeitungstätigkeiten (VVT)

Hinweise und Formulare:

- https://www.lfd.niedersachsen.de/themen/wirtschaft/verfahrensverzeicnis_und_verfahrensregister_nach_bdsg/verfahrensregister-und-verfahrensbeschreibung-fuer-den-nicht-oeffentlichen-bereich-56247.html

Musterverzeichnis (LDA Bayern):

- https://www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf

15

Verpflichtung von Beschäftigten

C Datenschutz-Verpflichtung von Beschäftigten
Ist eine solche Verpflichtung durchzuführen?
☒ ja (da alle Mitarbeiter mit personenbezogenen Daten umgehen)
☐ nein

16

Verpflichtung von Beschäftigten

DSK-Kurzpapier Nr. 19 mit Muster (kann auch für Funktionäre verwendet werden)

- https://www.lfd.niedersachsen.de/download/131285

GDD-Praxishilfe DS-GVO XI

- https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_11.pdf

Muster

- https://www.gdd.de/downloads/praxishilfen/Muster_Verpflichtung_auf_Vertraulichkeit_v1.4.docx

17

Informations- und Auskunftspflichten

D Information- und Auskunftspflichten

Bestehen irgendwelche Informationspflichten?

☒ ja (insb. in der Vereinssatzung sowie auf der Webseite in der Datenschutzerklärung)

☐ nein

18

Neuer „Beipackzettel“ bei Datenerhebung (Direkterhebung und Erhebung durch Dritte)

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
- wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln
- die Dauer, für die die personenbezogenen Daten gespeichert werden;
- das Bestehen eines Rechts auf Auskunft, auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- wenn die Verarbeitung auf einer Einwilligung beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling

Prüfbogen zur Erfüllung der Informationspflichten

- https://www.bstbk.de/de/ressourcen/Dokumente/04_presse/publikationen/02_steuerrecht_rechnungslegung/2018-04-27_Arbeitshilfe_Informationspflichten.docx

20

Betroffenenrechte

- Recht auf Auskunft
  - https://www.bstbk.de/de/ressourcen/Dokumente/04_presse/publikationen/02_steuerrecht_rechnungslegung/2018-04-27_Arbeitshilfe_Auskunftspflichten.docx
- Recht auf Berichtigung
- Recht auf Einschränkung
- Recht auf Löschung
- Recht auf Widerspruch

- Recht auf Datenportabilität
- Automatisierte Einzelfallentscheidung (Profiling)

21

Datenschutzerklärung auf der Webseite

Generator, z. B.

- https://datenschutz-generator.de/

Mustertext, z. B.

- https://www.uni-muenster.de/Jura.itm/hoeren/lehre/materialien/musterdatenschutzerklaerung

Beim Impressum gab es keine Änderungen

22

Exkurs: Social Media

EuGH Urteil vom 05.06.2018 (Facebook-Urteil)

- Achtung: Social Media-Auftritte sind Joint Controllerships, es müssen entsprechende Vereinbarungen abgeschlossen werden.
- Auf jeden Social Media-Auftritt gehören auch eine Datenschutz-erklärung und ein Impressum (Abmahngefahr).

23

Exkurs: Cookies

Beschluss der Datenschutzkonferenz „Zur Anwendbarkeit des Telemediengesetzes (TMG) für nicht öffentliche Stellen ab dem 25. Mai 2018“:

- Marketing-Cookies dürfen nur mit einer informierten Einwilligung der betroffenen Person gesetzt werden.

24

Löschen von personenbezogenen Daten

E Löschen von Daten

Gibt es eine Anforderung zur Datenlöschung?

☒ ja (aber erst nach Ablauf gesetzlicher Aufbewahrungspflichten)

☐ nein

25

Löschen von personenbezogenen Daten

DSK Kurzpapier Nr. 11

- https://www.lfd.niedersachsen.de/download/122114

Übersicht über die relevanten Aufbewahrungsfristen (Achtung, Werbung!)

- https://www.reisswolf.com/service/aufbewahrungsfristen/

26

scope & focus Service-Gesellschaft mbH

Informationssicherheit

F Sicherheit

Müssen die Daten besonders gesichert werden?

☐ ja

☒ nein (etablierte Standardmaßnahmen sind ausreichend, um die Daten effektiv zu schützen)

27

scope & focus Service-Gesellschaft mbH

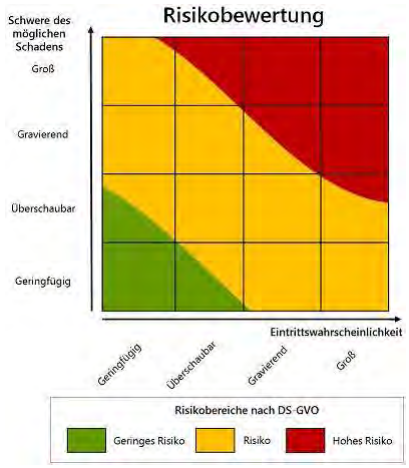
Risikoorientierte Informationssicherheit

PDCA-Zyklus…

…risikobasierter Ansatz…

scope & focus Service-Gesellschaft mbH

Informationssicherheit



https://www.lda.bayern.de/de/dsfa.html

29

scope & focus Service-Gesellschaft mbH

Infromationssicherheit

Geringes Risiko

Ein geringes Risiko bedeutet, dass weder die mögliche Schwere des Schadens für den Betroffenen noch die Eintrittswahrscheinlichkeit hoch sind und in Kombination weder mittel noch hoch.
Bei einem geringen Risiko ergeben sich in der DS-GVO für den Verantwortlichen gewisse Ausnahmen verschiedener Verpflichtungen, so dass manche Maßnahmen nicht durchgeführt werden müssen:

- Bei einer Datenschutzverletzung ohne Risiko (z. B. harmloser Fehlversand innerhalb einer Organisation) muss die Datenschutzaufsichtsbehörde nicht informiert werden.
- Ein Verzeichnis der Verarbeitungstätigkeiten ist (unter Berücksichtigung anderer Faktoren wie z. B. unregelmäßige Verarbeitung) bei geringem Risiko nicht zu erstellen.

Risiko ("Normal")

Auch bei einer rechtmäßigen Verarbeitung personenbezogener Daten entstehen Risiken für die betroffenen Personen, z. B. bei der Verarbeitung von Adresslisten, Einkaufsverhalten, der Kommunikation am Arbeitsplatz oder von Mitgliederlisten eines Sportvereins. Dort kann also die Schwere des Schadens und die Eintrittswahrscheinlichkeit in Kombination ein mittleres Niveau für das Risiko des Betroffenen erreichen.
Bei der Verarbeitung besonderer Arten personenbezogener Daten, d.h. sensibler Daten, ist das Risiko nicht immer gleich als hoch einzustufen. Die Risiko-Stufe „normal" kann also dort auch erreicht werden wie z. B. bei Angaben zur Religionszugehörigkeit „Römisch-Katholisch" in Bayern oder der Diagnose eines „Schnupfens" beim Hausarzt.

Hohes Risiko

Ein hohes Risiko umfasst dagegen potentielle Schäden, deren Ausmaß für die Rechte und Freiheiten von Betroffenen gravierend und/oder ziemlich wahrscheinlich sind. Unter der DS-GVO wird dieses Risiko-Level im Verhältnis aller Verarbeitungen eher selten vorkommen. Da ein hohes Risiko aber wesentliche Rechtsfolgen für den Verantwortlichen hat, muss das mögliche Vorkommen eines hohen Risikos zwangsläufig im Blick behalten werden.

Informationssicherheit

DSK-Kurzpapier Nr. 19

- https://www.lfd.niedersachsen.de/download/130405

31

Auftragsverarbeitung

G Auftragsverarbeitung

Ist ein Vertrag zur Auftragsverarbeitung notwendig?

☒ ja (sowohl mit dem Hosting-Anbieter als auch mit dem externen Lohnabrechner)

☐ nein

32

scope & focus Service-Gesellschaft mbH

DSK-Kurzpapier Nr. 13 - Auftragsverarbeitung
- https://www.lfd.niedersachsen.de/download/126580

DSK-Kurzpapier Nr. 16 – Gemeinsame Verantwortliche
- https://www.lfd.niedersachsen.de/download/128878

Mustervertrag
- BITKOM: https://www.bitkom.org/Bitkom/Publikationen/Mustervertragsanlage.html
- GDD: https://www.gdd.de/downloads/praxishilfen/Mustervertrag_zur_Auftragsverarbeitung_DS-GVO.docx

33

scope & focus Service-Gesellschaft mbH

Datenschutzverletzungen

H Datenschutzverletzungen
Müssen bestimmte Vorfälle gemeldet werden?
☒ ja (aber nur bei relevanten Risiken – eine einfache Online-Meldung beim BayLDA ist möglich)
☐ nein

34

scope & focus Service-Gesellschaft mbH

Datenschutzverletzungen

Voraussetzung

- Verletzung des Schutzes von personenbezogener Daten
- **Risiko** für die Rechte und Freiheiten der betroffenen Person

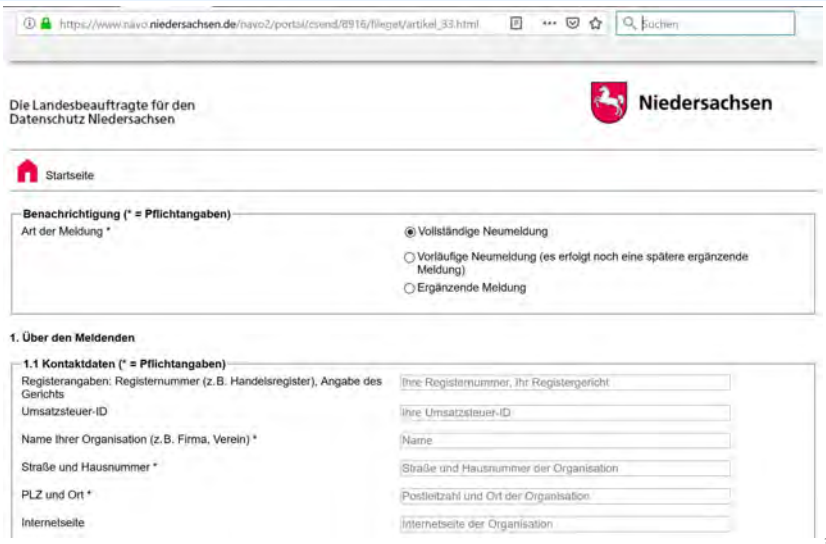
Folge

- **Meldung an die Aufsichtsbehörde** innerhalb von 72 Stunden
- Meldungsinhalt ist definiert

35

scope & focus Service-Gesellschaft mbH

Datenschutzverletzungen



36

scope & focus Service-Gesellschaft mbH

Datenschutz-Folgeabschätzung

I **Datenschutz-Folgeabschätzung (DSFA)**
Muss eine DSFA vom Verein durchgeführt werden?
☐ ja
☒ nein (da kein hohes Risiko bei der Daten-verarbeitung im Verein besteht)

37

scope & focus Service-Gesellschaft mbH

Datenschutz-Folgeabschätzung

Wird in der Regel nicht einschlägig sein für Vereine, Ausnahme kann der Betrieb einer Videoüberwachungsanlage sein

38

Datenschutz-Folgenabschätzung

DSK-Kurzpapier Nr. 5

- https://www.lfd.niedersachsen.de/download/120917

Ausführliche Beschreibung

- https://www.bitkom.org/Bitkom/Publikationen/Risk-Assessment-Datenschutz-Folgenabschaetzung.html

Musterrechnung

- https://www.lda.bayern.de/de/dsfa.html

39

Videoüberwachung

J **Videoüberwachung (VÜ)**
Besteht eine Ausschilderungspflicht bezüglich VÜ?
☐ ja
☒ nein (da keine Videoüberwachung im Verein durchgeführt wird)

40

scope & focus Service-Gesellschaft mbH

Videoüberwachung

DSK-Kurzpapier Nr. 15

- https://www.lfd.niedersachsen.de/download/126258

Beispielbeschilderung

- https://www.lfd.niedersachsen.de/startseite/themen/videoueberwachung/transparenzanforderungen_bei_einer_videoueberwachung_nach_dsgvo/transparenzanforderungen-und-hinweisbeschilderung-bei-einer-videoueberwachung-nach-der-ds-gvo-158959.html

41

scope & focus Service-Gesellschaft mbH

SPEZIALPROBLEME

42

scope & focus Service-Gesellschaft mbH

Spezialprobleme

- Fotos auf Vereinsveranstaltungen
  - https://www.lfd.niedersachsen.de/startseite/datenschutzreform/dsgvo/anfertigung_und_veroeffentlichung_von_personenfotografien/anfertigung-und-veroeffentlichung-von-personenfotografien-nach-dem-25-mai-2018-166008.html
- Datenübermittlung an Vereinsmitglieder
- Bekanntgabe zur Wahrnehmung satzungsmäßiger Mitgliederrechte
- Mitteilungen in Aushängen und Vereinspublikationen
- Datenübermittlung an Dachverbände und andere Vereine
- Datenübermittlung an Sponsoren und Firmen zu Werbezwecken
- Veröffentlichungen im Internet
- Veröffentlichungen im Intranet
- Personenbezogene Auskünfte an die Presse und sonstige Massenmedien

43

scope & focus Service-Gesellschaft mbH

FRAGEN AUS DEM AUDITORIUM

44

Fragen aus dem Auditorium

- WhatsApp Gruppen mit Vereinsmitgliedern, um sie über Ausfälle etc. zu informieren - dürften laut DSGVO ja der absolute Obergau sein - kann man sich da eine Erlaubnis einholen oder muss man sich eine Alternative suchen oder gänzlich darauf verzichten?
- https://www.lfd.niedersachsen.de/startseite/datenschutzreform/dsgvo/nutzung_von_whatsapp_im_unternehmen/merkblatt-fuer-die-nutzung-von-whatsapp-in-unternehmen-166297.html

45

Fragen aus dem Auditorium

- Ich betreue die Homepage der SG. Ein Impressum und die Datenschutzerklärung (bei uns vom Anbieter Jimdo) sind Bestandteil. Über Spiele/Sportaktionen kann auf der Homepage berichtet werden, da öffentliches Interesse besteht. So dürfen auch Bilder eines Spieles gezeigt werden. Ich denke auch die der Zuschauer/Besucher....
  Wie ist es aber bei Jugendmannschaften beim Fotografieren der Spiele oder einstellen von Mannschafts-/Einzelfotos. Kann man vom Einverständnis der Eltern ausgehen? Ist diese mit Eintritt des Vereins gegeben?
- https://www.lfd.niedersachsen.de/startseite/datenschutzreform/dsgvo/anfertigung_und_veroeffentlichung_von_personenfotografien/anfertigung-und-veroeffentlichung-von-personenfotografien-nach-dem-25-mai-2018-166008.html

46

scope & focus Service-Gesellschaft mbH

Fragen aus dem Auditorium

- Muss ich von jedem einzelnen Mitglied eines Vereins oder auch Elternvertreter einer Schule ein schriftliches Einverständnis für die Datensammlung haben? Was sollte auf einem Vordruck unbedingt draufstehen?
- Nein, die Rechtmäßigkeitsnorm ist Art. 6 Abs. 1 lit. B) DSGVO (Vertrag)
- Beim E-Mail Kontakt zu Mitgliedern oder Elternvertretern, was gibt es da Datenschutzrechtlich zu beachten? Wie sicher ist der E-Mail Verkehr?
- …
- Was gibt es bei Whatsapp Gruppen zu beachten?
  Braucht man dafür extra ein schriftliches Einverständnis? Ist das datenschutzrechtlich überhaupt noch erlaubt?
- Illegal

47

scope & focus Service-Gesellschaft mbH

SANKTIONEN


scope & focus
Service-Gesellschaft mbH
Geldbußen von bis zu 10 000 000 EUR oder 2 % seines gesamten weltweit erzielten Jahresumsatzes
Privacy by Design und by Default
Einwilligung eines Kindes
Informations-sicherheit
Auftrags-verarbeitung
Anzeigepflicht bei Datenabfluss
Benachrichtigung einer Person bei Datenabfluss
Datenschutz-beauftragter
Datenschutz-Folgenabschätzung


scope & focus
Service-Gesellschaft mbH
Geldbußen von bis zu 20 000 000 EUR oder 4 % seines gesamten weltweit erzielten Jahresumsatzes
Datenschutz-grundsätze
Verstoß gegen die Rechtmäßigkeit
Einwilligung
Verarbeitung sensibler Daten
Informationspflicht
Betroffenenrechte
Datenübermittlung in Drittstaaten
Nichtbefolgung der Anweisung der Aufsichtsbehörde

scope & focus
Service-Gesellschaft mbH

scope & focus

Ihre Daten - mit Sicherheit!

Leonhardtstr. 2
30175 Hannover
T: 0511 | 364 221-0
F: 0511 | 364 221-99

Hoerneckestr. 19-21
28217 Bremen
T: 0421 | 369 3530-0
F: 0421 | 369 3530-99

www.scope-and-focus.com
information@scope-and-focus.com

Dipl.-Ök. Stephan Rehfeld
Dipl.-Wirt.-Ing. Ulrike Hauser

51