Sparkasse Rhein-Maas

Wirtschaft
Recht
Steuern

kpp

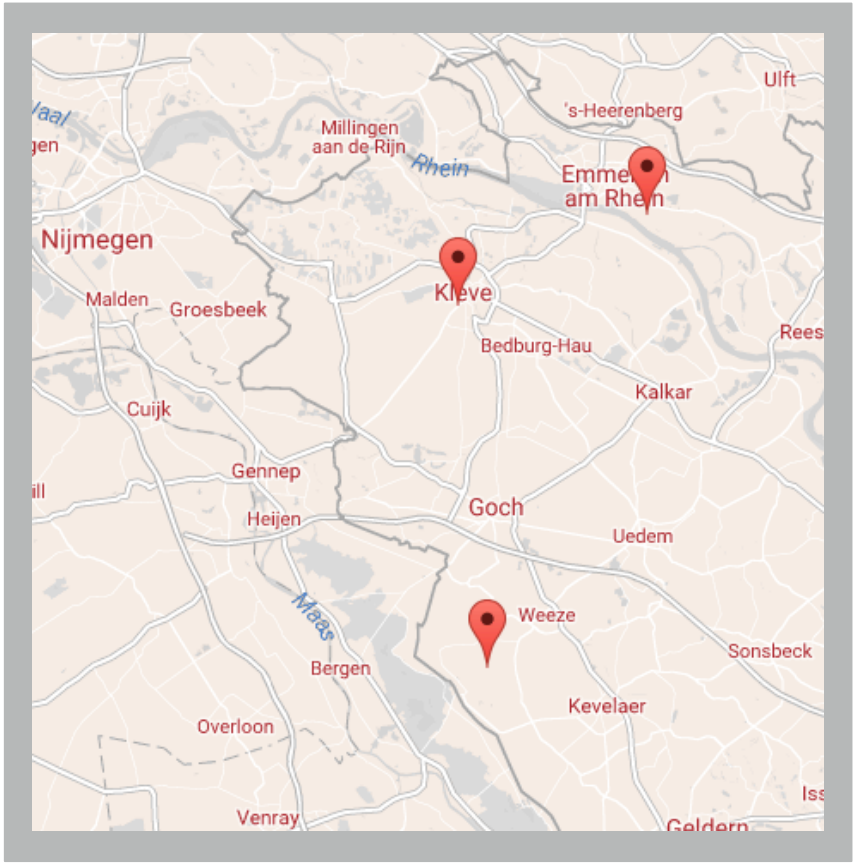
Anforderungen der Datenschutz-Grundverordnung und deren Umsetzung in Vereinen

Vortragsveranstaltung der Sparkasse Rhein-Maas
Referent: Stefan Boß, KPP Steuerberatungsgesellschaft mbH, Kleve

Inhaltsübersicht

KPP ist die führende Kanzlei für regionale sowie grenzüberschreitende Beratung

Wirtschaft
Recht
Steuern



- KPP ist die führende Kanzlei am Niederrhein für grenzüberschreitende Beratung zu den Niederlanden
- Seit Firmengründung 1995 historisch am Niederrhein verwurzelt
- Zur Zeit drei Standorte vorhanden, die die starke regionale Fokussierung untermauern
- Aktuell sind 16 Berufsträger sowie 42 qualifizierten Mitarbeiter aus betriebswirtschaftlichen, rechtswissenschaftlichen und steuerrechtlichen Bereichen beschäftigt
- Unseren Mandanten wird eine umfassende Beratung innerhalb unserer Schwerpunktthemen, die insbesondere durch eine branchenbedingte hohe Vertrauensbeziehung geprägt ist, geboten
- Wir verstehen uns als Premiumpartner aber vor allem als Team mit unseren Mandanten als integrativen Bestandteil

Vorstellung Referent

Wirtschaft
Recht
Steuern

Stefan Boß
Unternehmensberater bei der KPP Steuerberatungsgesellschaft mbH

Bankkaufmann (vormals Sparkasse Kleve)

Langjährige Tätigkeit bei der Finanz Informatik,
IT-Beratung von Sparkassen in Deutschland

Unternehmensberatung
Betriebswirtschaftliche Beratung, IT-Beratung

TÜV-zertifizierter
Datenschutzbeauftragter

Telefon: 02821 7204 733

Email: stefan.boss@kpp.de

Agenda

Wirtschaft
Recht
Steuern

1.	Vorstellung der KPP
2.	**Das neue Datenschutzrecht in Europa und Auswirkungen auf Vereine**
3.	Anregungen und Hilfsmittel zur Umsetzung in Vereinen

Die EU-Datenschutz-Grundverordnung ist seit dem 25.05.2018 in Kraft…

Wirtschaft
Recht
Steuern

kpp

Haben Sie in Ihrem Verein die Anforderungen der DS-GVO schon umgesetzt?

Was bedeutet eigentlich „Datenschutz“?

- Datenschutz? Also „Daten“ schützen?
  Nein: Nicht Daten sondern Persönlichkeitsrechte der Betroffenen schützen
- Es geht also beim Datenschutz um den Schutz der Privatsphäre von natürlichen Personen (und deren personenbezogenen Daten)
  - „Meine Daten gehören mir!“
  - Und wenn ich meine Daten an Dritte gebe, dann möchte ich, dass diese sorgfältig damit umgehen und meine Daten nur zu dem mir bekannten bzw. ausdrücklich erlaubten Zweck nutzen
- Die wesentlichen Vorgaben zum Datenschutz sind nicht neu, die gesetzlichen Anforderungen zur Beachtung (auch durch Vereine) existieren schon seit geraumer Zeit (Bundesdatenschutz-Gesetz, Recht auf informationelle Selbstbestimmung…)
  - Jetzt lediglich europaweit geregelt (und in Teilen ergänzt/geändert)
    Ziel: „Datensammel-Wut“ der Internet-Großkonzerne (Google etc.)

Was bedeutet eigentlich „Datenschutz"?

Wer ist im Verein für die Umsetzung des Datenschutzes verantwortlich?

Wirtschaft
Recht
Steuern

kpp

- Wie bisher ist der (Gesamt-)Vorstand des Vereins für die Einhaltung des Datenschutzes und die Umsetzung der DS-GVO verantwortlich
  - „Verantwortliche" Ansprechpartner sind in der Datenschutzerklärung des Vereins aufzunehmen (-> Webseite)
  - (wenn erforderlich) Benennung eines Datenschutzbeauftragten -> Webseite!
  - Rechenschaftspflichten
    - Nachweise, dass Datenschutz eingehalten wird, müssen dokumentiert sein (Beweisumkehr: Nachweis der Einwilligung erforderlich)
  - Auskunftspflicht gegenüber Mitgliedern und Aufsichtsbehörden
    - z. B. Verarbeitungsverzeichnis (siehe Musterbeispiel für Vereine)
    - Meldung von Datenschutzverletzungen an Aufsichtsbehörden (72 Stunden)
  - Löschrechte (Recht auf „Vergessenwerden", Recht auf Datenübertragbarkeit)
  - Widerspruchsrechte (z. B. gegen Nutzung für werbliche Zwecke)
  - Regelungen mit Auftragsverarbeitern (nicht aber Postdienste, Steuerberater…)

Was versteht der Gesetzgeber unter „personenbezogenen Daten“?

Wirtschaft
Recht
Steuern

kpp

- Blick ins Gesetz (Art. 4 Ziff. 1 DS-GVO):

  Im Sinne dieser Verordnung bezeichnet der Ausdruck „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“

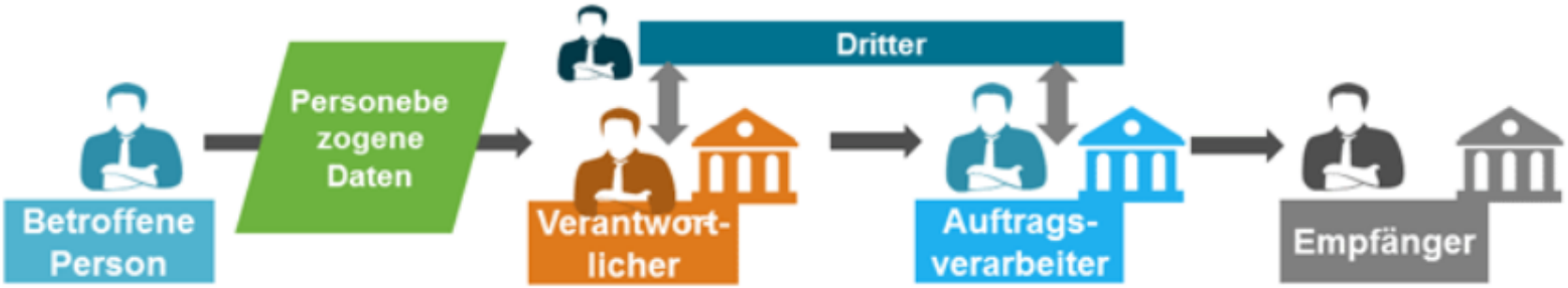
- Für Sie im Verein also z. B.
  - die in einem Mitgliederverzeichnis (Vereinssoftware aber auch Papier-Akten) aufgeführten Personendaten wie Name, Anschrift, Geburtsdatum, Mitgliederkennung, E-Mailadresse…
  - erfasst sind hiervon aber auch z. B. (Einzel-)Bilder oder Namen von Mitgliedern auf Webseiten des Vereins oder auch z. B. Wettkampf-/Leistungsergebnisse

Begriffsbezeichnungen der Datenschutz-Grundverordnung

Wirtschaft
Recht
Steuern

kpp

Relevante Rollen im Rahmen der DSGVO



Was ist bei der Verarbeitung von personenbezogenen Daten zu beachten? (1/2)

Wirtschaft
Recht
Steuern

kpp

- Die DS-GVO fordert, dass personenbezogene Daten nach folgenden Grundsätzen verarbeitet werden müssen:
  - „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz"
    - Darf ich die Daten verarbeiten, gibt es eine Rechtsgrundlage (Mitgliedsantrag) und was mache ich mit den Daten (Verarbeitungsvereichnis)?
  - „Zweckbindung"
    - Ich nutze die Daten nur für den vom Betroffenen gewollten Zweck (also z. B. keine Weitergabe an Dritte für Werbezwecke)
  - „Datenminimierung" und „Speicherbegrenzung"
    - Nur Daten erheben, die für die Zweck erforderlich sind (z. B. keine Daten zur Religionszugehörigkeit); Löschkonzept für Daten (alte Wettkampfdaten)
  - Richtigkeit
    - Nur „korrekte" Daten / Korrektur-Recht der Betroffenen
  - Integrität und Vertraulichkeit

Was ist bei der Verarbeitung von personenbezogenen Daten zu beachten? (2/2)

Wirtschaft
Recht
Steuern

- Löschkonzept für personenbezogene Daten erstellen:

  Grund für Löschanforderung

  - Zweck ist entfallen
  - Widerruf der betroffenen Person
  - Widerspruch gegen Verarbeitung
  - Einwilligung widerrufen
  - unrechtmäßige Verarbeitung

  Löschkonzept muss beschreiben, wie Daten gelöscht werden:

  - Wer, wann, wie?

  Weitergehende Informationen:
  https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/08/DSK_KPNr_11_Recht-auf-Vergessenwerden.pdf

Wann „darf" ein Verein überhaupt personenbezogene Daten verarbeiten?

Wirtschaft
Recht
Steuern

kpp

- Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn z. B. eine der folgenden Bedingungen erfüllt ist:
  - Eine wirksame „Einwilligungserklärung" der betroffenen Person liegt vor, dass z. B. (Einzel)-Fotos der Person auf die Webseite gestellt werden dürfen
    - Einzel-Foto vom Trainer mit Namensangabe
  - Die Verarbeitung dient der Erfüllung eines Vertrages auf Initiative der betroffenen Person
    - Mitglieder beantragen die Mitgliedschaft im Verein (Name, Bankdaten…)
      - Datenminimierung beachten:
        Daten nur im Umfang erheben wie es für den Zweck erforderlich ist
    - Mitglieder bestellen Vereins-Trikots mit Namen, Größen, Bankdaten etc.
      - Löschpflichten beachten:
        Daten löschen, wenn der Zweck erfüllt ist (evtl. Verlängerung wg. Rücksendung…)
- Die Kern-Herausforderung wird die Erfüllung der Informationspflichten darstellen, die der Verein bei der Erhebung der Daten gegenüber den betroffenen Personen zu beachten hat.

Informationspflichten (z. B. über Datenschutzrichtlinie des Vereins)

Wirtschaft
Recht
Steuern

kpp

- Name und Kontaktdaten des Verantwortlichen (Vorstand, Vereins-E-Mail)
- Kontaktdaten des Datenschutzbeauftragten (DSB), wenn benannt
  - Ein DSB (intern/extern) ist vom Verein zu benennen, wenn im Verein mindestens 10 Personen ständig mit der automatisierten Verarbeitung von personenbezogenen Daten betraut sind
- Zwecke der Datenverarbeitung und Rechtsgrundlage bzw. berechtigtes Interesse (Verarbeitung ist für Mitgliedsantrag erforderlich)
- Empfänger oder Kategorien von Empfängern (wer erhält die Daten?)
  - Trainer für Mannschaftslisten, Meldung an Sportbund etc., Wettkampfteilnahme
- Bei einer Datenübermittlung in ein Drittland (nicht EU, auch Schweiz)
  - Cloud-Dienste mit Serverstandorten außerhalb der EU (Dropbox USA)
- Angaben über die Dauer der Speicherung und die Löschung von Daten
- Information über die Rechte der Betroffenen (siehe Folgeseite)

Rechte der „Betroffenen“

- Recht auf Einschränkung der Verarbeitung einzelner Daten*)
- Auskunftsrecht der Betroffenen
- Recht auf Berichtigung von Daten
- Widerspruchsrecht gegen Verarbeitung *)
- Recht auf Löschung /
  Recht des Betroffenen auf das „Vergessenwerden“
- Beschwerderecht beider zuständigen Aufsichtsbehörde (NRW)

**) Informationspflicht über die „Folgen der Nichtbereitstellung“ z. B. bei Widerspruch*

Anpassungen auf Vereinswebseite - Abmahnungen vermeiden!

Wirtschaft
Recht
Steuern

kpp

- Wichtig im Zusammenhang mit den gesetzlichen Anforderungen ist die Anpassung bzw. Ergänzung der **Vereins-Webseiten** (Abmahn-Gefahr!):
  - Die Landesdatenschutzbehörden haben erklärt, die Einhaltung der DS-GVO bei Vereinen „mit Augenmaß" zu prüfen; problematischer ist an dieser Stelle jedoch die Gefahr von kostenpflichtigen Abmahnungen von dritter Seite (also zum Beispiel spezialisierten Abmahn-Anwälten, die ihr Geschäftsmodell hierauf ausgerichtet haben).
  - Neben der internen Umsetzung der DS-GVO im Verein gilt es daher, „von außen" nicht angreifbar zu sein. Daher sollte der Vorstand unbedingt die Webseitengestaltung prüfen und eine DS-GVO-konforme Datenschutzerklärung, welche von jeder Webseite mit einem Klick zu erreichen ist, aufnehmen
    - Kostenlose Datenschutzhinweis-Generatoren im Internet, z. B. https://www.activemind.de/datenschutz/datenschutzhinweis-generator/ (hier auch „Impressum"-Generator") -> Datenschutzrichtlinie beschließen
    - Vorsicht bei Kontakt-Formularen auf Webseite, Facebook-Like-Buttons…
    - Newsletter-Anmeldungen via „Double-Opt-In" (Bestätigungs-E-Mail)

IT-Sicherheit (Technik-Sicherheit) - Technisch organisatorische Maßnahmen

Wirtschaft
Recht
Steuern

kpp

- Der Verantwortliche (Vereinsvorstand) trifft geeignete technische und organisatorische Maßnahmen, welche dafür sorgen, dass die Anforderungen an den Datenschutz wirksam umgesetzt werden
  - „Einbrecher stiehlt den Vereins-PC" - Wie sind die personenbezogenen Daten gesichert?
    - Verschlüsselung, Zugangsdaten, Kennwörter…
  - Papierakten
    - Abschließbarer Schrank etc.
  - Technische bzw. organisatorische Beschränkung der Personen, welche auf personenbezogene Daten zugreifen können (Minimalprinzip)
    - Benutzerkonzept bei Arbeitsteilung (Kassierer vs. Beisitzer)
    - Grundsätzlich nur Daten erheben, welche für den Verarbeitungszweck benötigt werden (Verarbeitungsverzeichnis erstellen, Datenminimierung)
    - Speicherfrist / Löschkonzept (wann werden Daten gelöscht?)
    - Verpflichtungserklärung zum Datenschutz für Vereins-Funktionsträger

Agenda

Wirtschaft
Recht
Steuern

kpp

1.	Vorstellung der KPP
2.	Das neue Datenschutzrecht in Europa und Auswirkungen auf Vereine
3.	**Anregungen und Hilfsmittel zur Umsetzung in Vereinen**

Anregungen und Hilfsmittel zur Umsetzung der DS-GVO in Vereinen (1/3)

Wirtschaft
Recht
Steuern

kpp

- Datenschutz im Vorstand zum Thema machen („Verantwortlicher“)
- Webseite überprüfen („nicht angreifbar machen gegen Abmahnungen“)
- Verzeichnis von Verarbeitungstätigkeiten erstellen
  - Muster: https://www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf
- Prüfung, ob ein Datenschutzbeauftragter zu benennen ist
  - Mindestens 10 Personen sind „ständig“ mit der Verarbeitung von personenbezogenen Daten betraut oder unabhängig von der Personenanzahl
  - wenn Verarbeitungen durchgeführt werden, die eine Datenschutzfolgen-Abschätzung erfordern (Weitergabe der Daten an Dritte zu Werbezwecken)
  - oder wenn eine geschäftsmäßige Verarbeitung zum Zweck der anonymisierten Übermittlung oder zum Zweck Markt- und Meinungsforschung vorliegt
  - Entscheidung treffen: Interner oder externer Datenschutzbeauftragter (Kontaktdaten auf Webseite angeben); Verantwortlich bleibt der Vorstand!
- Datenschutzrichtlinie beschließen (und Angabe auf Webseite)

Anregungen und Hilfsmittel zur Umsetzung der DS-GVO in Vereinen (2/3)

Wirtschaft
Recht
Steuern

kpp

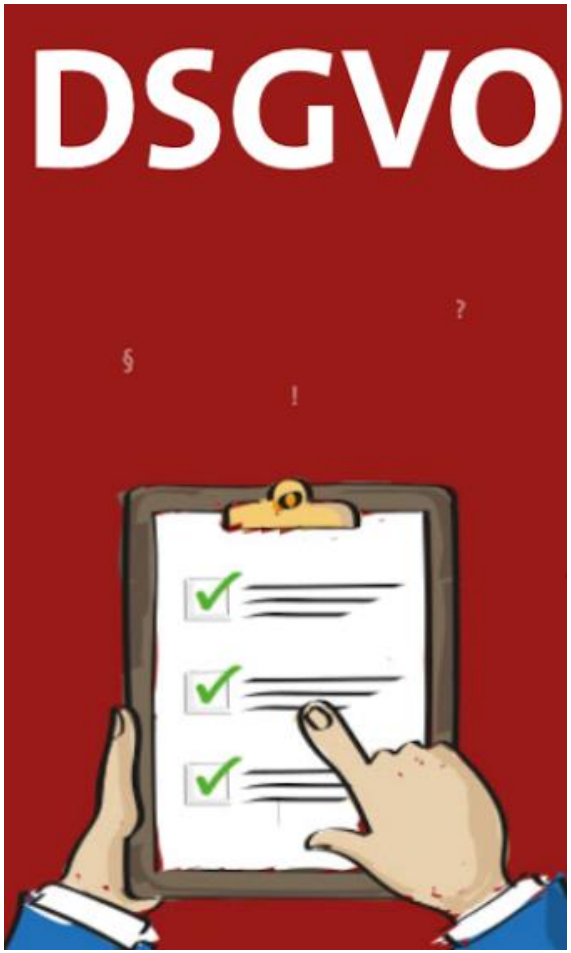
- Technisch organisatorische Maßnahmen dokumentieren
  - Vorhandene Maßnahmen prüfen, ob Datenschutz hinreichend gewährleistet werden kann
    - Falls nicht: Maßnahmen anpassen und umsetzen (Zugriffschutz, Löschkonzept, Newsletter-Anmeldeprozess etc.)
- Vereinbarungen mit „Auftragsverarbeitern" schließen, wenn personenbezogene Daten an Dritte weitergegeben werden
  - Hinweis: Gemäß „Kurzpapier 13" der Datenschutzkonferenz sind z. B. Steuerberater, Rechtsanwälte oder Postdienstleister per Definition keine Auftragsverarbeiter (somit keine gesonderte Vereinbarung erforderlich) (https://www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf)
- Einwilligungsformulare prüfen (gesonderte Erklärung)
  - Muster: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf (Formularmuster auf der letzten Seite)

Anregungen und Hilfsmittel zur Umsetzung der DS-GVO in Vereinen (3/3)

Wirtschaft
Recht
Steuern

kpp

- „Aufräumen“
  - Alt-Daten löschen, sofern diese nicht für gesetzliche Anforderungen benötigt werden (Aufbewahrungsfristen, Spendenbescheinigungen, Kontoauszüge…)
- Und wie geht es weiter?
  - Es ist sinnvoll, die Einhaltung der DS-GVO im Verein regelmäßig zu überprüfen
    - Aktualität des Verarbeitungsverzeichnisses
    - Technisch organisatorische Maßnahmen
    - Verschwiegenheitsverpflichtung für Funktionsträger (Neuwahlen Vorstand…)
    - Vereinbarungen „Auftragsverarbeiter“ vollständig? (neue Dienstleister?)
    - Datenschutzdokumentation vollständig?
      - Datenschutzerklärung noch aktuell (Webseite, Facebook-Like-Buttons…)
    - Ist ein Datenschutzbeauftragter zu benennen? (jetzt > 10 Personen?)
  - Kommende ePrivacy-Verordnung (vermutlich 2019/2020) könnte erneut Anforderungen an Webseitengestaltung mit sich bringen (Wiedervorlage)



KPP Steuerberatungsgesellschaft mbH
Telefon 02821 / 72 04 0
E-Mail info@kpp.de
Internet www.kpp.de