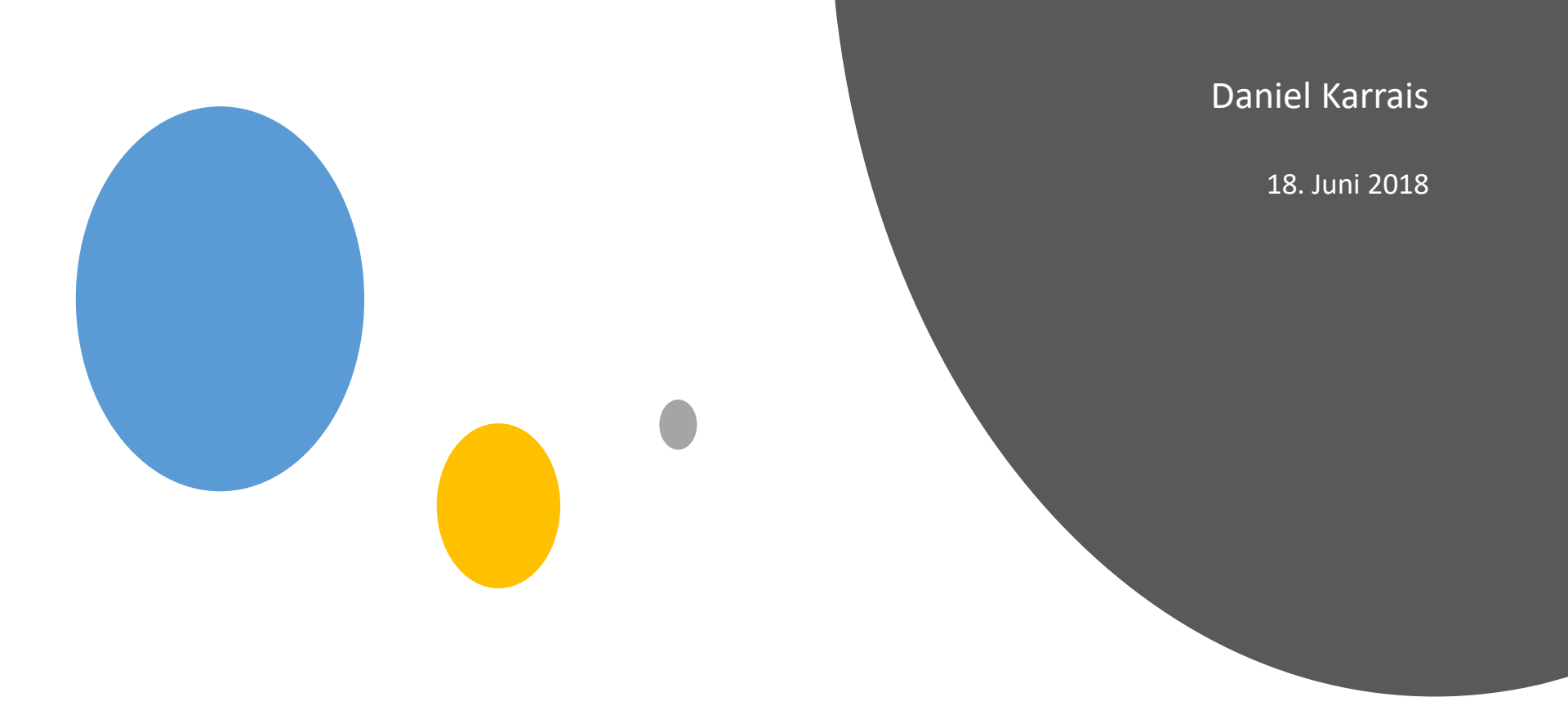




Daniel Karrais

18. Juni 2018

Datenschutz- Grundverordnung

Wichtiges Wissen
für Vereine

Hinweis

In den folgenden Folien werden Tipps und Hinweise zur Umsetzung der DSGVO in Vereinen gegeben. Diese basieren größtenteils auf Erfahrungen bei der Umsetzung der DSGVO aus der Praxis und auf diversen Leitfäden der Datenschutzbehörden und der Datenschutzkonferenz. Die Rechtsprechung und Auslegung ist ständigen Änderungen unterworfen, sodass sich die enthaltenen Informationen überholen können.

Die Folien erheben keinen Anspruch auf Vollständigkeit. Zur besseren Verständlichkeit wurden teilweise Formulierungen aus den einschlägigen Texten vereinfacht. Es gilt in letzter Konsequenz die DSGVO bzw. das BDSG sowie die Hilfen aus den offiziellen Leitfäden zur DSGVO. Die Situation in jedem Verein ist sorgfältig zu prüfen. Im Zweifel empfehlen wir für verbindliche Aussagen die Datenschutzbehörde zu kontaktieren und um Hilfe bei der Auslegung zu bitten.

Wichtige Begrifflichkeiten (Art. 4 DSGVO)

Personenbezogene Daten: Informationen über eine natürlichen Person, die zur Identifikation der Person dienen können oder Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind. (→ Mitgliederdaten, außer von Verstorbenen)

Betroffene: Identifizierte oder identifizierbare natürliche Person (→ Mitglieder)

Verantwortlicher: Natürliche oder juristische Person, Behörde oder Einrichtung, die allein oder gemeinsam über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (→ Verein, vertreten durch Vorstand)

Verarbeitung: jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang 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

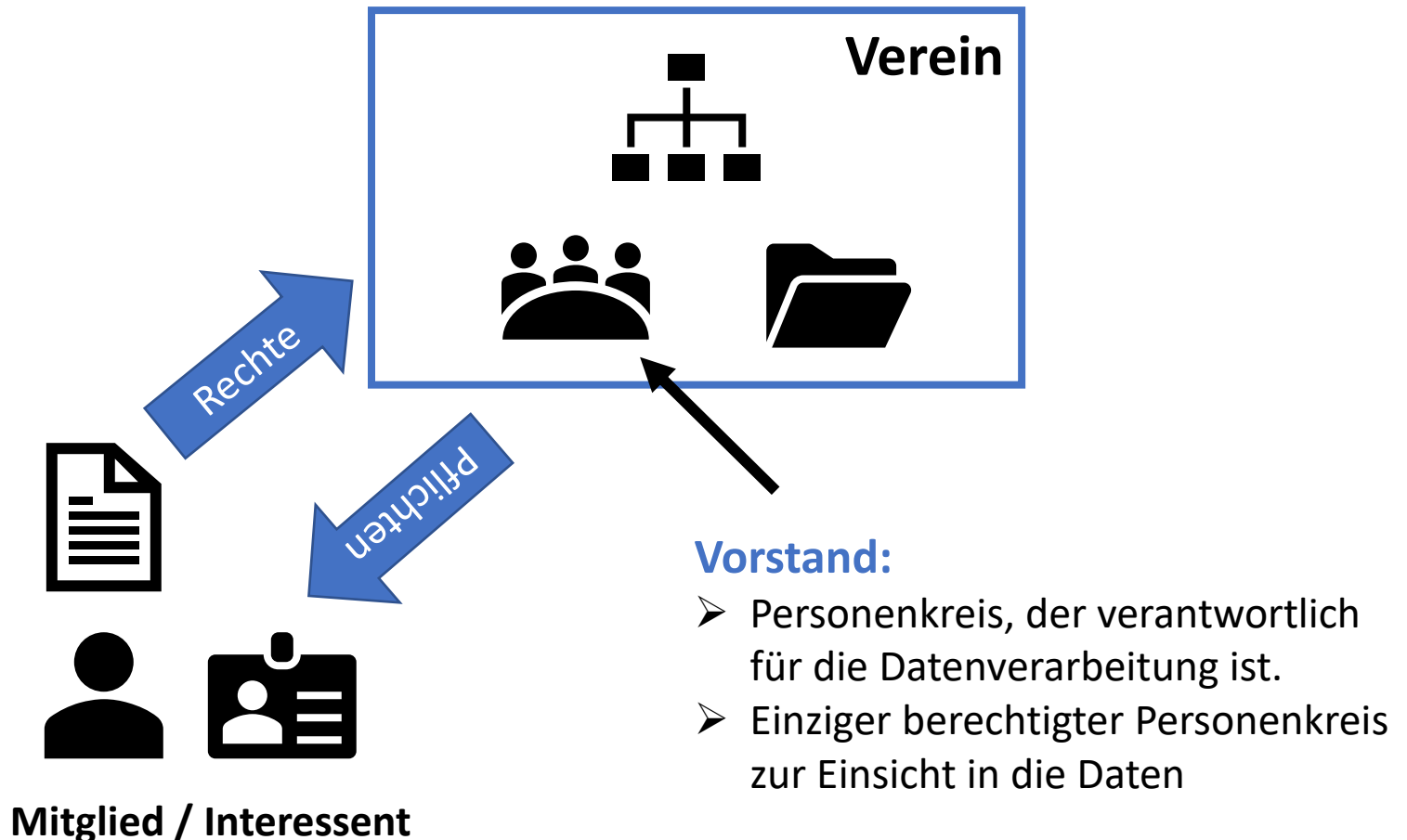
Personenbezogene Daten

Beispiele (nicht abschließend)

- Name
- Adresse
- Mail, Webseite, Social Media-Account
- Telefon, Fax, Mobilnummer
- Bankdaten
- Geburtsdatum
- Familienstand
- Spielernummer / Mitgliedsnummer / Beitrittsdatum etc.
- Familienstand, Kinder / Eltern
- Ergebnisse und Leistungen bei Wettkämpfen
- Besitzverhältnisse
- u.v.m.

Wer ist der Verantwortliche?

Verantwortlicher gegenüber dem Betroffenen ist der Verein



Rechtsgrundlage der Verarbeitung (Art. 6 Abs. 1 DSGVO)

Verarbeitung ist grundsätzlich verboten außer:



a) Nach Einwilligung durch Betroffenen

b) Zur Vertragserfüllung und –abwicklung



c) Zur Erfüllung einer rechtlichen Verpflichtung durch den Verantwortlichen



d) Zum Schutz lebenswichtiger Interessen des Betroffenen oder einer anderen natürlichen Person



e) Zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder zur Ausübung öffentlicher Gewalt



f) Zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern die Grundrechte des Betroffenen diese nicht überwiegen

Berechtigtes Interesse des Vereins

Die Vereinsziele bzw. der Vereinszweck, die Satzung und andere ordnungsgemäß festgelegten Rahmenregeln definieren die berechtigten Interessen des Vereins nach Art. 6 Abs. 1 f

Beispiel:

- Übermittlung von Spielerlisten an den Verband oder den nächsten gegnerischen Verein
- Kontaktaufnahme zur Mitgliederinformation
- Anmeldung von Mitgliedern für nächsten Wettkampf
- Veröffentlichung von Mitgliederlisten (rein intern)

Technische und organisatorische Maßnahmen und Datenminimierung

Einige Tipps für TOMs:

- Beschränkung des Datenzugriffs auf Vorsitzenden und Schatzmeister
- Datenhaltung möglichst zentral, um Inkonsistenz zu vermeiden (z.B. über eigenen ftp-Server, Vereinslaptop o.ä.)
- Keine Verwendung von Dropbox oder anderen nicht-EU-Clouddienstleistern
- Geräte, die zum Zugriff oder zur Speicherung auf die Daten verwendet werden, regelmäßig updaten und Firewall und Virens Scanner verwenden
- (Massen-)Mailversand nur noch über BCC, ggf. Verwendung eines Newsletter-Tools
- Vor Veröffentlichung von Mitglieder Daten Einwilligung des Betroffenen einholen (auch mündlich möglich)



Internetseite

Was Sie haben müssen:

- Impressum und Datenschutzerklärung mit aktuellen Informationen
- Cookie-Hinweis, idealerweise mit Opt-Out-Option
- Datenschutzerklärung mit Hinweisen zur Verwendung der Daten

Was Sie nicht (mehr) dürfen (nicht abschließend):

- Verwendung von „offenen“ Social Media Plug-Ins (Stichwort: Datenübermittlung an Nicht-EU-Land)
- Verwendung von Seiten ohne SSL-Zertifikat, sofern Daten von Ihrer Seite übermittelt werden können (Stichwort: Kontaktformular)
- Verpflichtende Angaben von mehr als der Mailadresse bei Verwendung eines Kontaktformulars → Datenminimierung
- Veröffentlichung von Namen, Bildern o.ä. ohne Einwilligung des Betroffenen (war schon immer so)

Newsletter & Mitgliederkommunikation



Newsletter sind eine Form des Direktmarketings und unterliegen einer Einwilligungspflicht

- Empfehlung: Verwendung von Newsletter-Dienstleistern zur einfachen Datenhaltung und -verwaltung
- Dokumentation der Einwilligungen in Papierform oder über Double-Opt-In-Verfahren
- Besonders bei Newsletterversand an Interessenten ist Vorsicht geboten

Sonderfall Mitglieder:

- Kommunikation mit Mitgliedern liegt im berechtigten Interesse des Vereins. Eine gesonderte Einwilligung für Newsletter-Empfang ist nicht notwendig, sofern ausschließlich Vereinsangelegenheiten kommuniziert werden



Facebook

Bei Verwendung von Facebook-Seiten

- Nach einem Urteil besteht eine gemeinsame Verantwortung bei der Verwendung von Facebook-Fanpages durch den Seiteninhaber und Facebook

Problem:

- Nach DSGVO müssten Sie einen Vertrag mit Facebook schließen
- Es wird davon ausgegangen, dass es ausreicht auf Ihrer Fanpage auf die Datenschutzerklärung von Facebook hinzuweisen



WhatsApp

WhatsApp liest das Adressbuch des Nutzers und speichert diese Daten

- Problematisch für Vorsitzende, die Mobilnummern von Mitgliedern auf dem Handy gespeichert haben

Empfehlung:

- Keine WhatsApp-Gruppen für Vereinskommunikation nutzen
- Wägen Sie für sich selbst ab, ob Sie WhatsApp nutzen wollen
- Weitere Rechtsprechung ist abzuwarten

Auftragsverarbeiter (Art. 28 DSGVO)

**Auftragsverarbeiter verarbeiten pb. Daten im Auftrag des Verantwortlichen.
Es ist eine AV-Vereinbarung zu schließen.**

Auftragsverarbeiter sind (nicht abschließend):

- Host Ihrer Internetseite und anderer Datenhaltungssysteme
- Anbieter von Newsletter-Tools
- Ggf. untergeordnete Verbände
- Lettershops, sofern Sie einen Datensatz erhalten

Keine Auftragsverarbeiter sind:

- Banken
- Internet- und Telefonie-Provider
- Mailanbieter
- Postdienstleister

Datenübermittlung an Drittstaaten

Datenübermittlung an Drittstaaten (non-EU) ist zu vermeiden!

Vorsicht ist geboten bei:

- Clouddiensten (z.B. Dropbox, Google Drive, Google Docs, Facebook etc.)
- Websitehosts, wenn diese keine Unternehmen aus der EU sind (Server-Standorte beachten)

Verarbeitungsverzeichnis (Art. 30 DSGVO)

Verantwortliche sind zum Führen eines Verarbeitungsverzeichnisses verpflichtet (Art. 30 DSGVO). Inhalte:

- Beschreibung Verarbeitungstätigkeit (High-Level)
- Kontakt operativ Verantwortlicher
- Zweck der Verarbeitung
- Kategorie der betroffenen Personen (z.B. Mitglied, Mitarbeiter, etc.)
- Kategorie der pb. Daten (z.B. Name, Alter, Adresse,...)
- Kategorie von Empfängern (z.B. Steuerberater, Lettershop, Host,...)
- Übermittlung in Drittland?
- Löschfrist der Daten
- Technische und organisatorische Maßnahmen

Datenschutzbeauftragter (Art. 37 DSGVO)

Datenschutzbeauftragter muss benannt werden, wenn

- Die Kerntätigkeit des Verantwortlichen in der Verarbeitung von pb Daten liegt
- Automatisiert Entscheidungen getroffen werden
- Mehr als 10 Personen dauerhaft mit der Verarbeitung beschäftigt sind (§38 BDSG)
- Besonders risikoreiche Verarbeitung stattfindet

Fazit: Die meisten Vereine brauchen keinen Datenschutzbeauftragten.

Informationspflichten (Art. 13 & 14 DSGVO)

Informationspflicht bei erster Datenerhebung oder bei Datenerhalt durch Dritten

Der Verantwortliche teilt dem Betroffenen folgendes mit:

- Vereinsname sowie Kontaktdaten des Vorsitzenden und ggf. DSB
- Zwecke für die pb. Daten verarbeitet werden
- Vereinszweck, der das berechtigte Interesse zur Verarbeitung darstellt
- Kategorien von Empfängern der Daten
- Ggf. Auskunft ob Daten an Drittländer der EU übertragen werden
- Speicherdauer der Daten
- Aufklärung Betroffenenrechte (Auskunft, Löschung, Einschränkung, Widerruf)
- Beschwerderecht bei einer Aufsichtsbehörde

Dokumentation

Vereine sollten:

- Eine Datenschutzrichtlinie für den Verein verabschieden, die regelt, wer auf welche Daten Zugriff erhält, wie diese verarbeitet werden und an wen diese weitergegeben werden
- Mitgliedsanträgen ein Infoblatt beifügen, das Informationen dazu bereithält, wie die Daten verarbeitet werden
- Einwilligungen für die Veröffentlichung auf Internetseiten einholen, sofern notwendig
- Ein Verarbeitungsverzeichnis erstellen
- Altbestände an Mitgliederdaten löschen

Zeit zum Nachdenken...

Haben wir eine
Datenschutzrichtlinie?

Wer sind unsere
Auftragsverarbeiter?

Wie läuft die
Mitgliederkommunikation?

Welche Daten hat unser Verein?

Sind unsere
Sicherheitsvorkehrungen gut
genug?

Welche Daten braucht der Verein?



Wer verarbeitet die Daten in
unserem Verein?

Ist unsere Internetseite DSGVO-
konform?

Bekommen Dritte Daten von
unseren Mitgliedern?

Hilfreiche Dokumente und Links

Leitfaden „Datenschutz im Verein nach der Datenschutz-Grundverordnung“
des Landesbeauftragten für Datenschutz und Informationssicherheit des
Landes Baden-Württemberg

Alle Papiere der Datenschutzkonferenz (DSK)

Hinweise für kleine Unternehmen und Vereine:
<https://www.lida.bayern.de/de/kleine-unternehmen.html>

Allgemeine Leitfäden zur DSGVO:
https://www.lida.bayern.de/de/datenschutz_eu.html

Datenschutz Wiki mit Checklisten und Tipps zu verschiedenen Themen:
www.datenschutz-wiki.de