Zimmer EDV GmbH

IT-Security • Netzwerke • Support

Datenschutz für Vereine

Zimmer EDV GmbH

IT-Security • Netzwerke • Support

Steffen Zimmer

IT Sicherheit sei 1997
Datenschutz Beauftragter seit 2007
ISO27001-Grundschutz Lead Auditor (BSI)
ISO 27001 Lead Auditor (TÜV Rheinland)
ISO 9001 Lead Auditor (TÜV Rheinland)
TÜV-Zertifizierter Datenschutzauditor

Zimmer EDV GmbH

IT-Security • Netzwerke • Support

Ich bin kein Jurist. Der Vortrag gibt daher meine Meinung wieder und stellt keine rechtsverbindliche Auskunft dar.

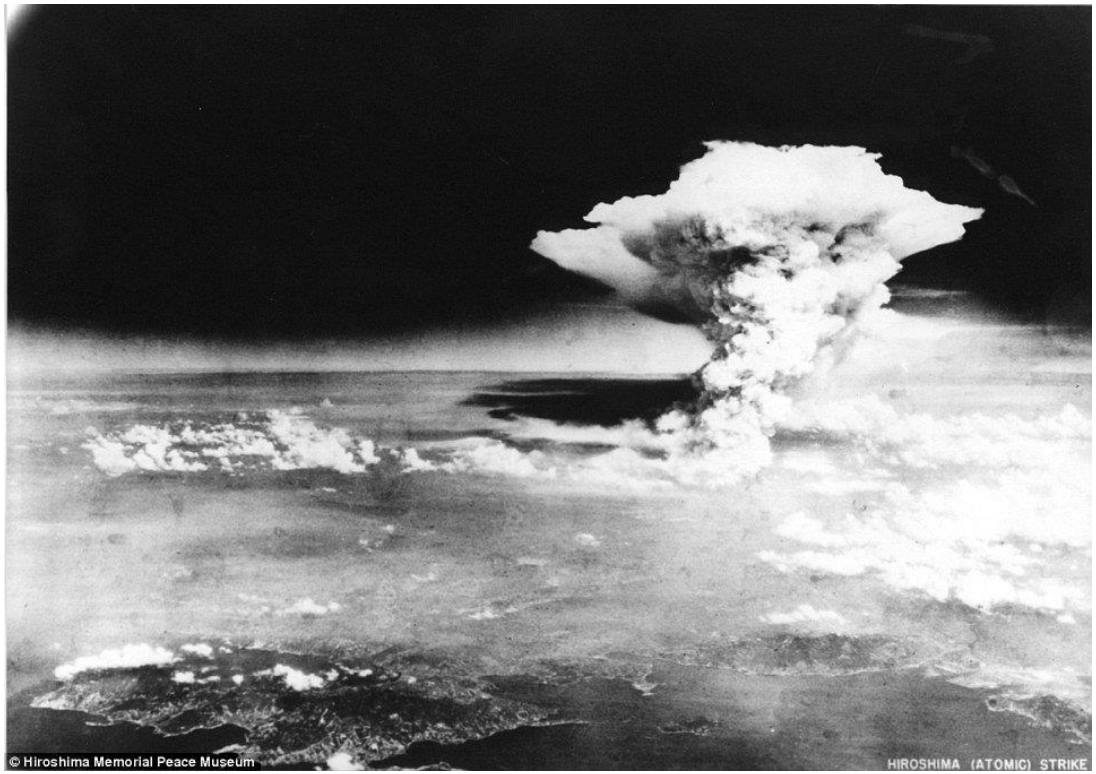
Inhalte

1. Aktuelle Situation
2. Was verlangt die DSGVO
3. Was muss ein Verein machen
4. Fragen

Inhalte

1. Aktuelle Situation
2. Was verlangt die DSGVO
3. Was muss ein Verein machen
4. Fragen

25.05.2018
Was wurde erwartet?



25.05.2018

Was ist wirklich passiert?

Nichts

(wesentliches, aber viel skurriles)

Aktuelle Situation

Los Angeles Times

Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism.

Aktuelle Situation

Aktuelle Situation

„Ich stimme der Verarbeitung meiner Daten im Rahmen der Kundenbeziehung zu“

„Ich stimme der Datenschutzerklärung und den AGB zu“

„Ich stimme der Datenverarbeitung zu Zwecken der Begründung und Durchführung des Beschäftigungsverhältnisses zu“.

„ADV-Vertrag für Erstellung eines Brandschutzkonzepts“

„Einwilligung zur DSGVO damit weiterhin Rechnungen bezahlt werden können.“

Sachlich betrachtet

Unsicherheit bei vielen Bürgern, Firmen, Vereinen

Angst vor Abmahnungen

Angst vor der Aufsichtsbehörde (Bußgelder bis zu 20.000.000 €)

Angst vor Kundenanfragen und Beschwerden

Angst vor der Privathaftung

Viel Aktionismus

Inhalte

1. Aktuelle Situation
2. Was verlangt die DSGVO
3. Was muss ein Verein machen
4. Fragen

Wesentliche Punkte der DSGVO

1. Datenschutzerklärung auf Webseiten
2. Auftragsdatenverarbeitungs-Verträge (AV-Verträge)
3. Auskunftsrecht
4. Informationspflicht
5. Verzeichnis der Verarbeitungstätigkeiten
6. Bußgelder
7. Einwilligungen

Vergleich BDSG (alt) und DSGVO

BDSG (alt)	DSGVO
Besonders schützenswerte Daten (6)	Besonders schützenswerte Daten (8)
ADV-Verträge	AV-Verträge
Auskunftsrecht	Auskunftsrecht
Verfahrensverzeichnis	Verzeichnis der Verarbeitungstätigkeiten
Anforderungen um personenbezogene Daten verarbeiten zu dürfen	Anforderungen um personenbezogene Daten verarbeiten zu dürfen
„Jedermannverzeichnis“	Erklärung über Datenverarbeitung
Bußgeld: 200.000 €	Bußgeld: 20.000.000 €
-	Datenschutzfreundliche Voreinstellungen „Datenschutz by Default“ „Datenschutz by Design“

Personenbezogene Daten

„Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“

BDSG §3

„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;
DSGVO Art.4

Was sind personenbezogene Daten?

Herr Anton Müller hat die Telefonnummer 0711-1234567

Frau Anna Müller hat für 15,-- € Seife im Supermarkt eingekauft.

Herr Anton Müller hat Grippe.

Die Kreditkartennummer von Frau Anna Müller ist 1234 5678 9012.

Frau Anna Müller hat sich eine Kette für 50000,-- € gekauft.

Herr M. hat ein monatliches Einkommen von 2000,-- €.

Herr M. geb. 01.01.1960 aus Stuttgart, Hauptstr. 13 ist in der IG Metall.

Ein Einwohner aus Stuttgart verdient durchschnittlich 2300,-- €.

Supermarkt Süd AG hat 2013 einen Gewinn von 22 Mio. € erwirtschaftet.

Elektro Müller besitzt zwei Porsche.

Natürliche und juristische Personen

Natürliche Personen:

- Kunden, Interessenten, Schüler
- Mitarbeiter (auch von einer GmbH, AG, etc.)
- Teilweise Lieferanten (falls Lieferant keine juristische Person)

Juristische Personen:

- GmbH
- AG
- Verein

Besondere Arten

Besondere Arten personenbezogener Daten:

- Rassische oder ethnische Herkunft
- Politische Meinungen
- Religiöse oder philosophische Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit
- Sexualleben
- Biometrische Daten (EU-DSGVO Art 9)
- Genetische Daten (EU-DSGVO Art. 9)
- Strafrechtliche Daten (EU-DSGVO Art 10)

BDSG §3 Abs. 9, EU-DSGVO Art 9

Automatisierte Verarbeitung

„Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.“

BDSG §3 Abs. 9

„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 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;
DSGVO Art. 4

Zulässigkeit der Datenerhebung

Wann dürfen personenbezogene Daten erhoben, verarbeitet oder genutzt werden?

1. Erlaubnis durch Gesetz oder Rechtsvorschrift
2. Regelung durch DSGVO oder BDSG (neu)
3. Einwilligung des Betroffenen

Kurzer Exkurs: Einwilligungen

Firmen holen sich derzeit massenweise die Einwilligung für den Versand von Newslettern ein. … und erhalten diese nicht!

UWG (Gesetz gegen unerlaubten Wettbewerb)

§7 Unzumutbare Belästigung

Liegt vor bei Fax, Telefon, E-Mail ohne Einwilligung

(3) Abweichend von Absatz 2 Nummer 3 ist eine unzumutbare Belästigung bei einer Werbung unter Verwendung elektronischer Post nicht anzunehmen, wenn
1. ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat,
2. der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,
3. der Kunde der Verwendung nicht widersprochen hat und
4. der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen

Kurzer Exkurs: Einwilligungen

„Hiermit willige ich der Verarbeitung meiner Personenbezogenen Daten zur Personalverwaltung und Lohnabrechnung ein.“

Kurzer Exkurs: Einwilligungen

Anforderungen an eine Einwilligung:

- Die Einwilligung muss konkret und für verschiedene Verarbeitungszwecke separat erfolgen.
- Die Nichteinwilligung darf nicht zu einer Nichterfüllung einer Leistung führen. (Koppelungsverbot).
- Das Widerrufsrecht muss eingeräumt und erklärt werden, einschließlich der Folgen des Widerrufs.
- Bei Verweigerung einer Einwilligung oder einer ungültigen Einwilligung kann man sich nicht mehr auf eine gesetzliche Grundlage berufen

Fazit: Einwilligungen sind sehr komplex und risikobehaftet. Gesetzliche Grundlagen heraussuchen sind das einfachere und wirkungsvollere Mittel

Kurzer Exkurs: Einwilligungen

Rechtsgrundlagen DSGVO

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- **die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen; (Lohnbuchhaltung, Rechnungen)**
- **die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt; (Steuerrecht)**
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen; (Notfallmedizin)
- 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; (Kommunen)
- **die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.**

Kurzer Exkurs: Einwilligungen

Rechtsgrundlagen BDSG (neu)

- Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch nichtöffentliche Stellen ist zulässig,
- wenn sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist oder
- **sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist,**
- sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.

Inhalte

1. Aktuelle Situation
2. Was verlangt die DSGVO
3. Was muss ein Verein machen
4. Fragen

Auftragsdatenverarbeitung

Datenschutz im Verein nach der Datenschutzgrundverordnung (DS-GVO)

Landesdatenschutzbeauftragter Baden-Württemberg

https://www.baden-wuerttemberg.datenschutz.de/datenschutz-im-verein/

Vereinssatzung

Die Mitgliedschaft in einem Verein ist als Vertragsverhältnis zwischen den Mitgliedern und dem Verein anzusehen, dessen Inhalt im Wesentlichen durch die Vereinssatzung und sie ergänzende Regelungen (z.B. eine Vereinsordnung) vorgegeben wird.
Eine **Vereinssatzung** bestimmt insoweit die Vereinsziele, für welche die Mitgliederdaten genutzt werden können.

Informationspflicht (auf jedem Formular)

Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters

- Kontaktdaten des Datenschutzbeauftragten
- Zwecke der Verarbeitung (bitte im Einzelnen aufzählen)
- Rechtsgrundlage der Verarbeitung
- berechtigte Interessen i.S.d. Art. 6 Abs. 1 lit. f) DS-GVO
- Empfänger oder Kategorien von Empfängern (z.B. Weitergabe personenbezogener Daten an eine Versicherung, an den Dachverband, an alle Vereinsmitglieder, im Internet)
- Absicht über Drittlandtransfer (z.B. bei Mitgliederverwaltung in der Cloud), so-wie Hinweis auf (Fehlen von) Garantien zur Datensicherheit
- Speicherdauer der personenbezogenen Daten
- Belehrung über Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht gegen Verarbeitung)
- Hinweis auf jederzeitiges Widerrufsrecht der Einwilligung
- Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde

Erhebung von Daten Dritter

Daten von Dritten die der Identifizierung dienen (Name, Vorname, Anschrift, Geburtsdatum) sind zulässig, wenn sie für Kartenverkäufe oder zur oder Verteidigung Ansprüche geht (Stadionsverbot)

Verwaltung von Vereinsdaten

- Ausreichendes Sicherheitsniveau
- Vorsicht bei Speicherung in der Cloud (insbesondere im Ausland)
- AV-Verträge bei externen Dienstleistern

Löschen, Sperre

Personenbezogene Daten müssen gelöscht werden wenn

- Ihre Speicherung unzulässig ist
- Ihre Kenntnis für die Verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

An Stelle einer Löschung tritt eine Sperrung

- Aufbewahrungsfristen einer Löschung entgegenstehen
- Durch Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt

Datenschutzbeauftragter

Ein Datenschutzbeauftragter muss bestellt werden wenn:
… mehr als 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind.
… besondere Daten nach Art. 9 verwendet werden (Selbsthilfegruppen)
… Videoüberwachung vorliegt

Wichtig: kein DSB -> Vorstand für die Einhaltung des Datenschutzes verantwortlich

Verzeichnis der Verarbeitungstätigkeiten

Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters

- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind bzw. noch offengelegt werden
- Angaben über Drittlandtransfer einschließlich Angabe des Drittlandes sowie Dokumentierung geeigneter Garantien
- wenn möglich Fristen für die Löschung der verschiedenen Datenkategorien
- wenn möglich Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO

Datenschutzfolgenabschätzung

Nur bei der Verarbeitung von Daten nach Art. 9 DSGVO

Facebook

Sehr riskant

WhatsApp

Meiner Meinung nach: No-Go!

Fragen???

Steffen Zimmer
Zimmer EDV GmbH
Esslinger Str. 69
72124 Pliezhausen

Telefon: 07127-92894-0
Fax: 07127-92894-9
E-Mail:
steffen.zimmer@zimmeredv.de