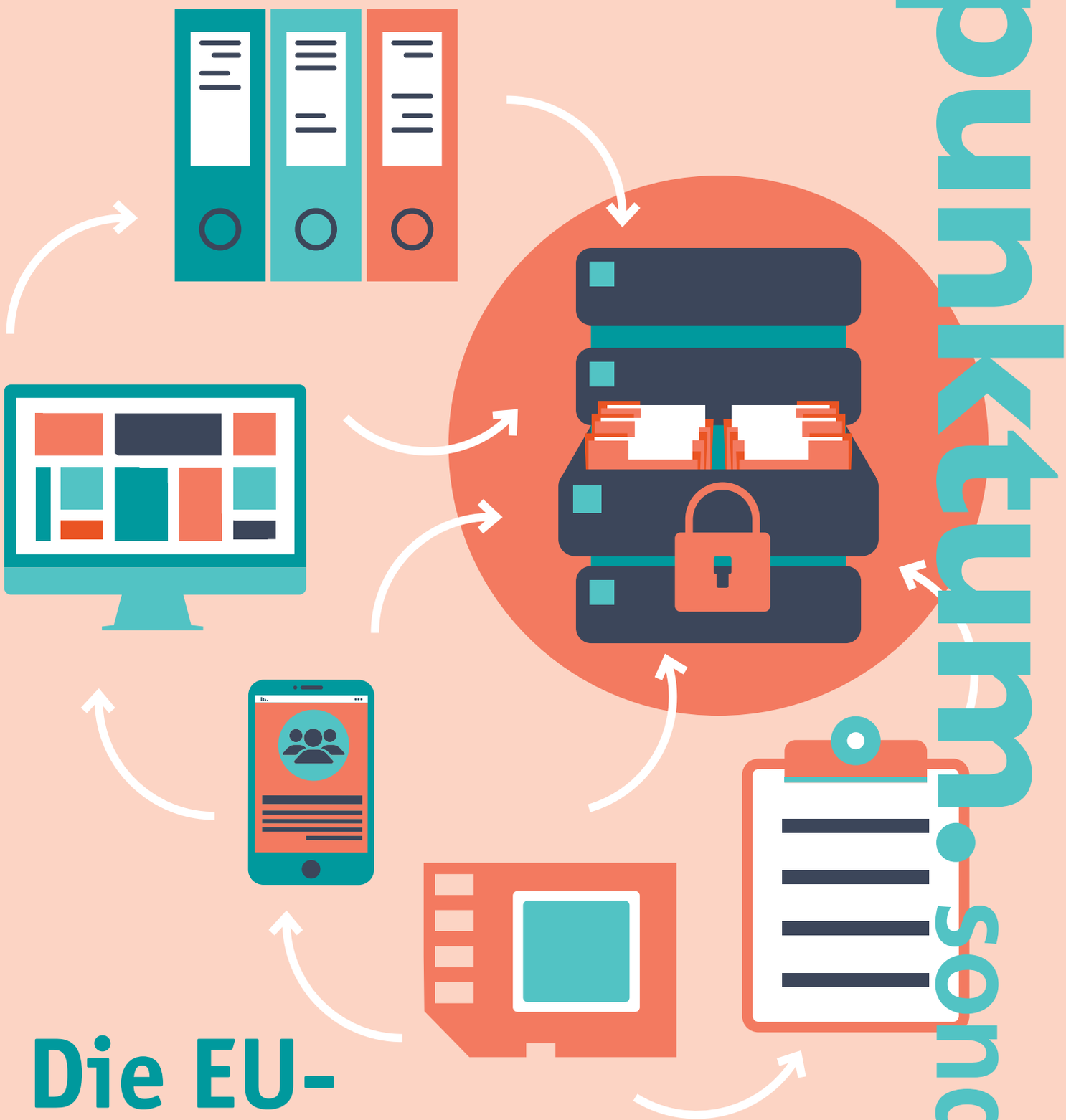
punkt4fun-sonderheft



Die EU-Datenschutz-Grundverordnung

Eine Arbeitshilfe für Jugendverbände

Intro

Dieses punktum-Sonderheft zur EU-Datenschutzgrundverordnung ist als Arbeitshilfe für Jugendverbände konzipiert. In seiner Gliederung folgt es daher nicht den Paragrafen der Verordnung, sondern beschreibt anhand von Praxisfeldern der Jugendverbände jene Maßnahmen, die für einen datenschutzkonformen Umgang mit persönlichen Daten erforderlich sind. Wo immer es geht, verzichtet die Autorin, Rechtsanwältin Sascha Lotzkat, auf formal-juristische Erläuterungen, um ein besseres Verständnis für Datenschutzbelange zu ermöglichen. Daher sind im Heft auch keine Paragrafentexte der DSGVO abgedruckt. An passender Textstelle finden sich aber Hinweise in der Seitenspalte, die auf den einschlägigen Gesetzestext verweisen.

Nicht erst seit der EU-Datenschutzgrundverordnung steht der verantwortungsbewusste Umgang mit Medien und Daten auf der Agenda von Jugendverbänden. Stichwort Medienkompetenz: Junge Menschen werden dabei unterstützt, kritisch mit Medien und sorgsam mit (ihren und fremden) Daten umzugehen. Einzelne Aspekte der DSGVO bedeuten für Jugendverbände jedoch einen Bürokratiezuwachs und zusätzliche Kosten. Diese wiegen im weitestgehend ehrenamtlich organisierten Jugendverbandsbereich besonders schwer. Wenn die DSGVO beispielsweise aktuelle Betriebssysteme (und damit entsprechende Hardware) zur Datensicherheit im IT-Bereich vorschreibt, dann entstehen zusätzliche Kosten. Wenn die Rechtmäßigkeit der Datenverarbeitung zu belegen ist oder Einwilligungen zum Fotografieren zu archivieren sind, dann entsteht zusätzlicher bürokratischer Aufwand. Immer wieder sind es staatliche Verordnungen – wie aktuell die DSGVO –, die ein ehrenamtliches Engagement junger Menschen komplizierter werden lassen. Zumindest die zusätzlichen Kosten sollten bei der Förderung der Jugendverbände mit eingepreist werden. (jg)

Die Autorin

Sascha Lotzkat ist seit 20 Jahren als Rechtsanwältin tätig. Sie führt eine eigene Kanzlei in einer Bürogemeinschaft in Hamburg. Ihre Schwerpunkte sind Arbeitsrecht und Datenschutz. Als externe Datenschutzbeauftragte ist sie für Einrichtungen und Vereine im sozialen, kirchlichen und medizinischen Bereich tätig. Wichtig ist ihr, dem Datenschutz den Schrecken zu nehmen und in Einrichtungen und Vereinen lebbar zu gestalten.

Kontakt: Waitzstr. 8 | 22607 Hamburg | T. (040) 325 98 94 - 0 | info@ra-slotzkat.eu | www.ra-slotzkat.eu

Inhalt

3 Die Grundideen des Datenschutzes

6 Datenschutz in der Geschäftsstelle

11 Website

17 Soziale Medien

19 Publikationen

21 Fotos

25 Veranstaltungen und Freienfreizeiten

28 Hilfen

Impressum

Dieses Heft ist eine Sonderausgabe der vierteljährlichen Publikation **punktum** vom Landesjugendring Hamburg e.V.

Die Redaktion behält es sich vor, Beiträge zu kürzen.

Namentlich gekennzeichnete Beiträge geben die Meinung des Autors, aber nicht unbedingt die Meinung des Vorstandes wieder.

Redaktion: Jürgen Garbers

Layout und Gestaltung: Rebekka Posselt

V.i.S.d.P.: Laura Vanselow c/o LJR, Güntherstraße 34, 22087 Hamburg. Preis im Mitgliedsbeitrag inbegriffen.

Verlag: Landesjugendring Hamburg e.V.; Güntherstr. 34, 22087 Hamburg; Tel.: (040) 31 79 61 14; Fax: (040) 31 79 61 80; info@ljr-hh.de; www.ljr-hh.de.

Auflage: 300 Exemplare

punktum wird gefördert mit Mitteln der Freien und Hansestadt Hamburg, Behörde für Arbeit, Soziales, Familie und Integration.

Druck: eurodruck, Schnackenburgallee 158, 22525 Hamburg; gedruckt auf umweltfreundlichem Papier.

Die Grundideen des Datenschutzes

Aus unserem Alltag sind analoge und digitale Informationen nicht mehr wegzudenken. Wir sind umgeben von Geräten, die unsere Daten erheben, verarbeiten, speichern und weiterleiten. Täglich nehmen uns Überwachungskameras (S-Bahn, Bus, Kreuzung) auf. Apps auf unseren Smartphones bieten zahllose Möglichkeiten, Informationen über uns und unser Verhalten zu sammeln, zu speichern und weiterzuleiten. Per GPS kann unser monentaner Standort bestimmt, mit anderen Daten verknüpft und ausgewertet werden. Viele Berechtigungen von Smartphone-Apps geben Dritten zudem Zugriff auf unsere Bilder, Kontakte und Sprachnachrichten. Auch beim Surfen im Internet hinterlassen wir bewusst oder unbewusst Spuren. Wir posten in Sozialen Netzwerken oder werden beim Surfen über Internetseiten hinweg weiterverfolgt (tracking). Ohne Datenschutz droht eine umfassende Überwachung des Bürgers, die seine Freiheit bedroht und sein Recht auf informationelle Selbstbestimmung aushölt.

Die **Datenschutzgrundverordnung der EU** soll Verbraucher vor umfassender Überwachung schützen. Firmen, Geschäftsleute, Vereine und sonstige Institutionen, die mit persönlichen Daten hantieren, müssen gewisse Standards einhalten, um die Datensicherheit zu gewährleisten. Dabei soll unter anderem Datenverlust, -manipulation und unberechtigter Zugriff verhindert werden. Dies soll dadurch gewährleistet werden, dass Zweckbindung, Transparenz, Datensparsamkeit, Richtigkeit, Speicherbegrenzung (Recht auf Löschen), Integrität und Vertraulichkeit beim Umgang mit personenbezogenen Daten einzuhalten sind.

Rechtliche Grundlagen: EU-Datenschutzgrundverordnung (DSGVO): https://dsgvo-gesetz.de/art-1-dsgvo | Bundesdatenschutzgesetz (BDSG): www.gesetze-im-internet.de/bdsg_2018/index.html | ePrivacy: https://www.datenschutz-bayern.de/0/eprivacyV0.html

Grundlage ist das Recht auf informationelle Selbstbestimmung, welches im Grundgesetz, der Europäischen Menschenrechtskonvention und der Allgemeinen Erklärung der Menschenrechte (Art. 12) verankert ist.

Art. 1 und 2 GG, Art. 10 EMK, Art. 12 AEMR

Die Datenschutzgrundverordnung wird ergänzt durch das Bundesdatenschutzgesetz (BDSG). Dieses Gesetz gilt im Wesentlichen für öffentliche Stellen (Verwaltung) und im privaten Bereich (natürliche und juristische Personen, z.B. Vereine), bei ganz oder teilweiser automatisierter Verarbeitung und außerdem für Beschäftigtendaten. Das BDSG ergänzt die Regeln der DSGVO, weshalb nachfolgend überwiegend die Vorschriften der DSGVO dargestellt werden.

Bundesdatenschutzgesetz

Die **ePrivacy-Verordnung** soll Vorgaben für datenschutzfreundliche Software-Technik in der elektronischen Kommunikation unterbreiten und die Datenschutzgrundverordnung ergänzen. Die bisher geltende ePrivacy-Richtlinie (2002/58/EG) und die ergänzende Cookie-Richtlinie (2009/136/EG) sollten abgelöst werden. Die Verordnung ist jedoch nicht am 25.5.2018 in Kraft getreten, so dass weiter auf die bisherigen Vorschriften und Gesetze (BDSG, TMG, StGB u. DSGVO) zurückgegriffen werden muss.

ePrivacy (Stand 28.02.2019)

1. Begriffe, die immer wieder vorkommen, kurz erklärt:

Art. 4 DSGVO

Personenbezogene Daten

Alle Informationen, die es ermöglichen natürliche Personen zu identifizieren oder identifizierbar zu machen, werden als **personenbezogene Daten** bezeichnet. Neben Namen und Geburtsdatum gehören dazu auch besondere Merkmale wie Geschlecht, kulturelle oder wirtschaftliche Informationen.

Verarbeitung

Als **Verarbeitung** werden alle Arbeiten wie das Erheben, Erfassen, Ordnen, Anpassen, Verändern, Auslesen und Abfragen etc. von Daten bezeichnet. Die Verarbeitung umfasst digitale wie ebenso handschriftlich gemachte Vorgänge.

Verantwortliche Stelle

Verantwortliche Stelle sind die Personen, Vereine, Behörden, Einrichtungen oder andere Stellen, die allein oder mit anderen zusammen über die Zwecke und die Mittel der Verarbeitung der Daten entscheiden.

Art. 6 DSGVO

Rechtmäßigkeit der Verarbeitung

Um Daten zu verarbeiten, muss eine Berechtigung vorliegen: Die Verarbeitung muss einen Grund haben. Juristen nennen das **Rechtmäßigkeit der Datenverarbeitung** bzw. Rechtsgrundlage. Die DSGVO benennt in Art. 6 mehrere Gründe, nach der die Datenverarbeitung berechtigt ist. Liegt keiner der genannten Gründe vor, dürfen Daten nicht verarbeitet werden. Für Jugendverbände gibt es im Wesentlichen drei Rechtsgrundlagen: die Erfüllung des **Vertrages** (Mitgliedschaft), dessen Anbahnung, das **berechtigte Interesse** und die **Einwilligung**.

Zweckbindung

Daten dürfen nur für den **Zweck** verwendet werden, für den sie erhoben wurden. Bei Jugendverbänden gibt die Satzung den Zweck vor. Der Inhalt des zwischen Mitgliedern und Jugendverband geschlossenen **Vertrag** bestimmt sich nach der Satzung und evtl. weiteren Regeln wie der Geschäftsordnung.
Dadurch ist auch der Zweck, für den die Daten erhoben werden, klar umrissen. Damit dürfen alle Daten erhoben werden, die zur Verfolgung der Verbandsziele und für die Betreuung und Verwaltung der Mitglieder (wie etwa Name, Anschrift, in der Regel auch das Geburtsdatum und die Bankverbindung) notwendig sind. Für andere als den Vereinszweck dürfen die Daten nicht – bzw. nur mit anderer Rechtsgrundlage – genutzt werden.

Datenminimierung

Es dürfen nur die Daten erhoben werden, die angemessen und erheblich sind. Die Datenmenge ist auf das **notwendige Maß** zu beschränken. Wichtig ist darauf zu achten, dass bereits bei der Datenerhebung (Anmeldebögen, Fragebögen etc.) nur die Daten abgefragt werden, die tatsächlich für die Arbeit benötigt werden. Immer wenn Sie denken, das könnte ich mal gebrauchen, sind die Daten zum jetzigen Zeitpunkt nicht notwendig. Häufig wird vorgeschlagen, die erhobenen Daten zu anonymisieren oder zu pseudonymisieren. Das macht im Bereich von Forschung und Analyse Sinn. In der Jugendverbandsarbeit sollen Personen jedoch konkret angesprochen und daher Daten zugeordnet werden können.

Richtigkeit

Die erhobenen und verarbeiteten Daten müssen immer sachlich richtig und auf dem neuesten Stand sein. Es sind angemessene Maßnahmen zu treffen, damit unrichtige Daten **aktualisiert** werden.

Speicherbegrenzung

Recht auf Löschung: Daten, die der Identifikation von Personen dienen, dürfen nur solange gespeichert werden, wie dies erforderlich ist. »Wir könnten die Informationen mal gebrauchen« oder »die Neueingabe ist unbequem« sind keine ausreichenden Gründe, Daten länger als notwendig zu speichern. Näheres dazu beschreibt der Abschnitt »Veranstaltungen und Ferienfreizeiten« auf Seite 25 in diesem Heft.

Integrität und Vertraulichkeit

Es muss gewährleistet werden, dass es **Unbefugten** nicht möglich ist, Daten zu verändern oder die Daten zur Kenntnis zunehmen. Um die Integrität und Vertraulichkeit zu gewährleisten, sind geeignete organisatorische und technische Maßnahmen zu treffen. Siehe dazu den Abschnitt »Datenschutz in der Geschäftsstelle« auf Seite 6 in diesem Heft.

Privacy by design und Privacy by default

Zum Schutz der personenbezogenen Daten setzt die DSGVO auf zwei weitere Grundsätze. Die Verantwortlichen sollen interne Strategien festlegen und Maßnahmen ergreifen, durch die personenbezogene Daten geschützt werden können. Dies kann durch technische Maßnahmen (Privacy by design) und durch datenschutzfreundliche Voreinstellungen (Privacy by default) geschehen.
Privacy by design bezieht sich auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen (Software), Diensten und Produkten. Anwendungen und Produkte sollen bereits technisch die Möglichkeit bieten, den Datenschutz zu gewährleisten, wenn z.B. in Formularen nur notwendige Daten eingegeben werden können.
Durch **Privacy by default** sollen IT-Anwender auch ohne besondere technische Kenntnisse in die Lage versetzt werden, ihren Datenabfluss zu überwachen. So werden Voreinstellungen in IT-Geräten datenschutzfreundlich eingerichtet, z.B. Ortungsfunktionen im Smartphone ausgeschaltet.

2. Schutz von Minderjährigen in der DSGVO

Minderjährige

Die DSGVO gewährleistet Minderjährigen bis zur Vollendung des 16. Lebensjahres einen besonderen Schutz. Die allgemeine Regel, dass die Volljährigkeit mit Vollendung des 18. Lebensjahres eintritt, bleibt bestehen. Der Wille der Erziehungsberechtigten – meist der Eltern – ist daher bindend, auch wenn die Jugendlichen einen anderen Wunsch geäußert haben.

Berechtigte Interessen

Basiert die Verarbeitung der Daten auf einer Interessenabwägung, so überwiegen bei Kindern und Personen unter 16 Jahren regelmäßig die schutzwürdigen Interessen der Kinder. **Im Alter zwischen 16 und 18 Jahren** kann hingegen die Abwägung ergeben, dass die eigenen berechtigten Interessen des Jugendverbandes überwiegen.

Einwilligung

Bis zur Vollendung des 16. Lebensjahres können Kinder und Jugendliche nur bedingt eine Einwilligung in die Verarbeitung der personenbezogenen Daten geben. Ist eine Einwilligung erforderlich (z.B. Anmeldung zur Ferienfahrt per Kontaktformular), müssen Jugendverbände besondere Vorkehrungen treffen, um sich zu vergewissern, dass die Einwilligung durch die Erziehungsberechtigten für das Kind oder mit dessen Zustimmung erteilt wurde.

Datenschutz in der Geschäftsstelle

1. Anforderungen an die Struktur der Geschäfftsstelle

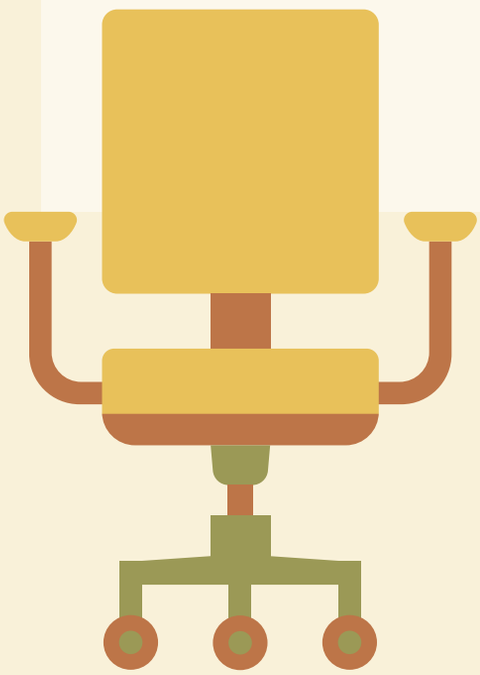
Die Geschäftsstelle ist die Einrichtung, welche neben dem Vorstand die Aufgaben des Datenschutzes für den Jugendverband (Verantwortliche) wahrnimmt. Es sind geeignete und wirksame Maßnahmen zum Schutz der Daten zu treffen. Die getroffenen Maßnahmen müssen nachgewiesen werden. **Zu dokumentieren sind folgende Punkte der Datenverarbeitung:** die Rechtmäßigkeit der Datenverarbeitung, welche Personen und Daten betroffen sind, wann Daten gelöscht werden und ob eine Übermittlung an Dritte stattfindet. Außerdem sind die getroffenen Technisch-Organisatorischen-Maßnahmen (TOM) zu dokumentieren. Die DSGVO stellt im wesentlichen zwei Instrumente zur Verfügung, um der Dokumentationspflicht nachzukommen: das Verzeichnis der Verarbeitungstätigkeiten und die TOM.

2. Rechtmäßigkeit der Datenverarbeitung

Um Daten zu verarbeiten, muss eine Berechtigung vorliegen, die Verarbeitung muss einen Grund haben. Juristen nennen das Rechtmäßigkeit der Datenverarbeitung bzw. Rechtsgrundlage. Die DSGVO gibt in Art. 6 mehrere Gründe an, nach der die Datenverarbeitung berechtigt ist. Liegt keiner der genannten Gründe vor, dürfen Daten nicht verarbeitet werden. Für Jugendverbände gibt es im Wesentlichen drei Rechtsgrundlagen: Vertrag durch Mitgliedschaft, berechtigtes Interesse und Einwilligung. Sie werden nachfolgend erläutert.

Vertrag
Art. 6 I S 1 lit b) DSGVO

Junge Menschen treten einem Jugendverband bei, werden dadurch Vereinsmitglieder und zahlen Mitgliedsbeiträge. In der Satzung sind Ziele und Zwecke des Jugendverbandes beschrieben. Somit haben der Verein und seine Mitglieder einen **Vertrag** geschlossen, dessen Inhalt sich aus der Satzung und evtl. weiteren Regeln wie etwa einer Geschäftsordnung ergibt.
Dadurch ist auch der Zweck, für den die Daten der Mitglieder erhoben werden, klar umrissen. Es dürfen alle Daten erhoben werden, die zur Verfolgung der Vereinsziele



und für die Betreuung und Verwaltung der Mitglieder (wie etwa Name, Anschrift, in der Regel auch das Geburtsdatum und die Bankverbindung) notwendig sind. Für andere als für den Vereinszweck dürfen die Daten nicht – bzw. nur mit anderer Rechtsgrundlage – genutzt werden.
Beispiel: Der Abschluss von Versicherungsverträgen zugunsten des Jugendverbandes oder seiner Mitglieder ist beispielsweise vom Vereinszweck gedeckt, soweit Risiken bestehen, gegen die sich der Jugendverband nicht zuletzt aus Fürsorgegründen versichern muss. Die Daten, die dafür erforderlich sind, dürfen erhoben werden. Grundsätzlich nicht erforderlich ist dagegen die Frage nach der früheren Mitgliedschaft des Beitrittswilligen in einer konkurrierenden Organisation.

Berechtigtes Interesse
Art. 6 I S 1 lit f) DSGVO

Für einen anderen Zweck als zur Verfolgung der Vereinsziele, der Mitgliederbetreuung und -verwaltung dürfen personenbezogene Daten erhoben werden, wenn der Verein ein **berechtigtes Interesse** nachweisen kann. Dabei ist zwischen dem Interesse des Vereins und der Mitglieder abzuwägen. Der Datenschutz als Ausfluss des Persönlichkeitsrechts ist ein hohes Schutzgut des Betroffenen.
Das berechtigte Interesse des Vereins an der Datennutzung überwiegt, wenn die Privat-, Intims- und Vertraulichkeitssphäre des Mitglieds gewahrt wird oder zurücktreten muss.
Für den Verein sind es häufig öffentlichkeitswirksame und wirtschaftliche Belange, die den Wunsch des Betroffenen, seine Privatsphäre zu wahren, zurücktreten lässt.
Beabsichtigt der Verein eine Datenverarbeitung, die nicht direkt vom Vereinszweck umfasst ist (z.B. für Öffentlichkeitsarbeit), kann er die Mitglieder bitten, ihren Wunsch auf Schutz ihrer Privatsphäre vorzubringen. Dann kann eine Abwägung an Hand der konkret genannten berechtigten Interessen erfolgen.
Der Verein sollte in einer Datenschutzordnung regeln, auf welchem Weg die Betroffenen ihre schutzwürdigen Interessen geltend machen können.

Bei Kindern und Jugendlichen unter 16 Jahren überwiegen regelmäßig die schutzwürdigen Interessen der Betroffenen. Im Alter zwischen 16 und 18 Jahren kann hingegen die Abwägung ergeben, dass die vereinseigenen berechtigten Interessen überwiegen.

Einwilligung Art. 6 I S 1 lit a) DSGVO

Eine **Einwilligung** in die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist dann erforderlich, wenn der Jugendverband diese in weitergehendem Maße verarbeitet. Es empfiehlt sich nicht, Einwilligungen für Datenverarbeitungen einzuholen, die bereits aufgrund einer der obigen Rechtsgrundlagen oder einer gesetzlichen Erlaubnis möglich sind. Denn dadurch wird beim Betroffenen der Eindruck erweckt, er könne mit der Verweigerung der Einwilligung oder ihrem späterem Widerruf die Datenverarbeitung verhindern. Hat der Jugendverband aber von vornherein die Absicht, im Falle der Verweigerung des Einverständnisses auf die gesetzliche Verarbeitungsbefugnis zurückzugreifen, wird der Betroffene getäuscht. Erst fragen sie ihn nach seiner ausdrücklichen Einwilligung, dann wird diese »ignoriert« und doch auf gesetzliche Ermächtigungen oder den Vereinszweck zurückgegriffen.

3. Hinweispflicht, Datenerhebung, Anfragen an Mitgliedschaft, neue Mitglieder

Unterrichtung
Art. 13 I und II DSGVO

Erfolgt eine Erhebung personenbezogener Daten direkt bei der betroffenen Person, so hat der Jugendverband zum Zeitpunkt der Datenerhebung eine entsprechende datenschutzrechtliche Unterrichtung vorzunehmen (Transparenzgebot). Daraus folgt, dass der Jugendverband in jedem Formular, das er zur Erhebung personenbezogener Daten nutzt, auf Folgendes hinweisen muss:

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters,
- Kontaktdaten des Datenschutzbeauftragten (sofern notwendig),
- Zwecke der Verarbeitung (bitte im Einzelnen aufzählen),
- Rechtsgrundlage der Verarbeitung,
- Empfänger oder Kategorien von Empfängern (z.B. Weitergabe personenbezogener Daten an eine Versicherung, an den Dachverband, an alle Vereinsmitglieder, Publikation im Internet),
- Absicht über Drittlandtransfer (z.B. bei Mitgliederverwaltung in der Cloud), sowie Hinweis auf Garantien zur Datensicherheit (resp. auf ihr Fehlen),
- Speicherdauer der personenbezogenen Daten,
- Belehrung über Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht gegen Verarbeitung),
- Hinweis auf jederzeitiges Widerrufsrecht einer Einwilligung,
- Hinweis auf das Beschwerderecht bei einer Aufsichtsbehörde.

Art. 14 I und II DSGVO

Werden personenbezogene Datei auf andere Weise als bei der betroffenen Person erhoben (z.B. gekauft), so sind Betroffene ebenfalls zu unterrichten. Diese Form dürfte bei Jugendverbänden selten vorkommen. Denn sie gilt nicht für allgemein öffentlich zugängliche Daten, wie z.B. die Kontaktadressen der an der Jugendarbeit Interessierten einer Partei, einer Behörde etc..

4. Verzeichnis von Verarbeitungstätigkeiten

Notwendig in jeder Geschäftsstelle: Erarbeitung eines Verzeichnisses von Datenverarbeitungstätigkeiten – egal, ob analog oder digital. Muster dafür finden sich bei den Aufsichtsbehörden für den Datenschutz (siehe Links auf der Rückseite des Heftes).

Ein Verzeichnis von Verarbeitungstätigkeiten soll innerhalb eines Jugendverbandes darlegen, welche Daten erhoben und wie diese verarbeitet werden. Die DSGVO schreibt ein solches Verzeichnis vor, es muss zwingend folgende Angaben enthalten:

- Name und Kontaktdaten des Verantwortlichen sowie ggfs. seines Vertreters,
- Zwecke der Verarbeitung (z.B. Verwaltung der Vereinstätigkeiten),
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (z.B. Mitglieder: Name, Adresse, etc.),
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind bzw. noch offengelegt werden (z.B. externe Dienstleister, Veranstalter, Trainer, ...),
- Angaben über einen Drittlandtransfer der Daten einschließlich der Angabe des Drittlandes sowie der Dokumentation geeigneter Garantien (meist keine, u.U. bei einer Cloud-Speicherung der Daten),
- wenn möglich: Fristen für die Löschung der verschiedenen Datenkategorien,
- wenn möglich: Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO.

5. Löschen von Daten

Personenbezogene Daten dürfen nicht mehr unbegrenzt aufgehoben werden.

Durch die DSGVO ist das Löschen von Daten in den Fokus der Öffentlichkeit gelangt. Personenbezogene Daten müssen irgendwann gelöscht werden. Früher wurden Mitgliederverzeichnisse in Papierform vernichtet, sobald die Regale oder die Kellerräume voll waren. Bei digitalen Informationen wird das Platzproblem zumeist dadurch behoben, dass mehr Festplattenspeicherplatz angeschafft wird.

Seit Mai 2018 ist das Löschen von Daten nicht mehr nur die Lösung eines Platzproblems. Personenbezogene Daten dürfen nicht mehr unbegrenzt aufgehoben werden. Auch dann nicht, wenn es »praktisch« oder »arbeitserleichternd« ist. Jede Geschäftsstelle muss festlegen, welche personenbezogene Daten sie wann löscht. So können Teilnehmerlisten einer Veranstaltung sofort gelöscht werden, wenn sie nicht wegen der Abrechnung gegenüber der BASFI oder aus steuerlichen Gründen länger aufzubewahren sind.

6. Technisch-Organisatorische-Maßnahmen

Technische und organisatorische Vorsichtsmaßnahmen zum Schutz von Daten

Technisch-Organisatorische-Maßnahmen (TOM) spielen eine zentrale Rolle, um personenbezogene Daten zu schützen. Die TOMs beziehen sich überwiegend – aber nicht nur – auf die IT-Sicherheit. Dabei ist jeweils der Stand der IT-Technik einzuhalten. Um Mitgliederdaten zu schützen, müssen Standardsicherheitsmaßnahmen angewandt werden. Dazu gehören der Einsatz aktueller Betriebssysteme, Passwortschutz und Backups. Die Programm- und Browserversionen sind stets aktuell zu halten. Virenschutzprogramme (einschließlich Firewall) sind regelmäßig zu aktualisieren.
Damit Unbefugte nicht an die schutzwürdigen Daten herankommen, sind Datenbanken mit personenbezogenen Daten entsprechend abzusichern.

7. Auftragsverarbeitung

Datenverarbeitung durch Dritte vertraglich absichern

Erbringen andere Stellen weisungsgebundene Dienstleistungen in Bezug auf die Verarbeitung personenbezogener Daten eines Jugendverbandes (z.B. Drucken von Vereinspost für die Mitglieder, Administrieren von Systemen durch IT-Dienstleister, Bereitstellung von Speicherplatz oder ganzer Anwendungen z.B. durch Cloud-Dienste), so müssen Regelungen zur Auftragsverarbeitung beachtet werden. In diesen Fällen bedarf es eines schriftlichen Vertrags zwischen dem Jugendverband als Auftraggeber und dem Dienstleister als Auftragnehmer mit einem verpflichtenden Inhalt. Der Dienstleister muss zuvor sorgfältig vom Verein ausgewählt werden. Der Dienstleister muss die Gewähr dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen nach der DSGVO erfolgt. Er muss bei seiner Tätigkeit den Schutz der Rechte der betroffenen Personen gewährleisten. Grundsätzlich verantwortlich bleibt aber der Verein. Er muss sicherstellen, dass der Dienstleister die datenschutzrechtlichen Vorgaben einhält.

8. Persönliche Daten zu Hause

Zuhause mit Vereinsdaten arbeiten?

Häufig werden Jugendleiter und Betreuer zu Hause personenbezogene Daten verarbeiten, z.B. beim Erstellen oder Versenden von Teilnehmendenlisten. Um den Anforderungen des Datenschutzes zu genügen, sind auch zu Hause technische und organisatorische Maßnahmen zu treffen. Ehrenamtliche sollten darauf hingewiesen werden, dass sie deshalb alle Informationen mit personenbezogenen Daten (z.B. Notizzettel, Karteikarten, USB-Sticks) stets sicher und verschlossen aufbewahren müssen, damit ein unbefugter Zugriff Dritter nach Möglichkeit ausgeschlossen ist.
Falls personenbezogene Daten auf privaten Endgeräten (z.B. Laptop, Smartphone,

Tablet) gespeichert werden, ist sicherzustellen, dass alle rechtlichen und technischen Vorgaben eingehalten werden. Dabei sollten die Ehrenamtlichen auf die Mindeststandards wie Benutzerkennung, Passwortschutz und Datensicherung hingewiesen werden. Insbesondere ist darauf zu achten, dass Familienangehörige oder andere Personen keinen Zugriff auf die Daten haben.

9. Schweigepflicht von Mitarbeitenden und Ehrenamtlichen

Erklärung zur Schweigepflicht dokumentieren

Sowohl Mitarbeitende der Geschäftsstelle als auch Ehrenamtliche sind auf das Datengeheimnis, also zur Verschwiegenheit zu verpflichten. Dass eine Verpflichtung stattgefunden hat, ist zu dokumentieren. Sinnvoll aber nicht notwendig ist die schriftliche Verpflichtung.

10. Datenschutzbeauftragter (DSB)

Wer zählt mit zur Anzahl der Datenverarbeitenden?

Für viele Jugendverbände wird es keine Pflicht sein, einen DSB zu benennen. Ein DSB ist erst zu benennen, wenn in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.
Werden von einem Jugendleiter nur Listen seiner Gruppenmitglieder geführt, so sind diese nicht mitzuzählen. Bei Unsicherheit kann immer der Hamburgische Beauftragte für Datenschutz und Informationssicherheit befragt werden.

11. Datenschutzvorfall

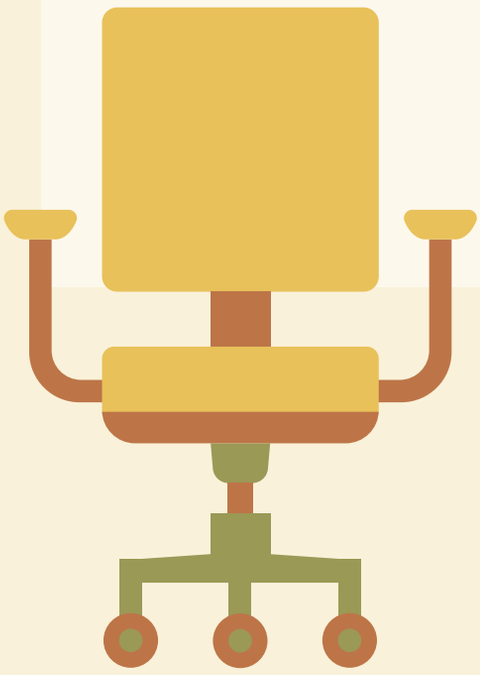
Wenn etwas vorgefallen ist …

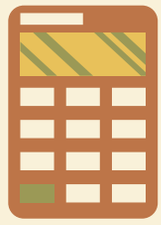
Wurde ein Speicherstick oder ein Laptop verloren oder ein Mail-Konto gehackt, können persönliche Daten verloren gehen. Sie können auch Unbefugten zur Kenntnis gelangen. Nichts verschweigen! Handeln Sie zügig. Bei einem Datenschutzvorfall ist die Aufsichtsbehörde (Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit) innerhalb von 72 Stunden zu informieren. Ansonsten können empfindliche Busgelder drohen.
Dies gilt nicht bei sehr geringfügiger Persönlichkeitsrechtsverletzung.

12. Dokumentation der Einsichtnahme in erweiterte Führungszeugnisse (gemäß § 72a SGB VIII)

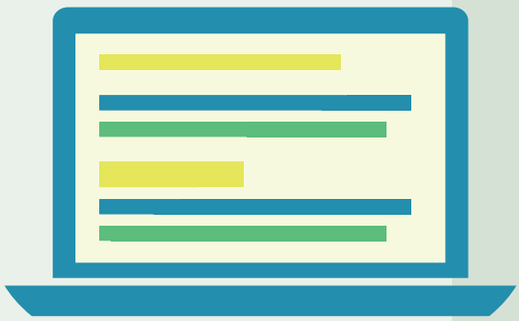
www.ljr-hh.de/politisches-und-rechtliches/rechtliches

Bei Personen, die Umgang mit Kindern und Jugendlichen im Jugendverband haben, ist das erweiterte Führungszeugnis einzusehen, um einschlägig vorbestrafte Personen aus der Jugendverbandsarbeit auszuschließen. Der Paragraf 72a Absatz 5 SGB Vlll hält genau fest, was zu notieren ist. Als Prüfungsergebnis müssen folgende Daten schriftlich festgehalten werden: Name der betroffenen Person, Ausstellungsdatum des erweiterten Führungszeugnisses und Ergebnis der Einsichtnahme. Die Führungszeugnisse selbst sind nicht aufzubewahren, nur die Einsichtnahme ist zu dokumentieren. Wichtig: Diese Daten werden entweder sofort gelöscht, wenn die Person nicht tätig wird, oder spätestens nach drei Monaten, nachdem die Personen ihre Tätigkeit beendet hat. Außerdem ist sicherzustellen, dass keine Unbefugten Zugriff auf diese Daten haben.





Website



Durch eine Website können viele verschiedene personenbezogene Daten erhoben und gespeichert werden. Jeder Jugendverband, der eine Webseite betreibt, muss prüfen, welche personenbezogenen Daten er darüber erhebt, nutzt, speichert und ob dies überhaupt gewünscht ist.
Neben den Pflichtangaben im Impressum (Ziffer 1) sind Pflichtangaben zur Datenschutzerklärung zu erarbeiten (Ziffer 2). Der Abschnitt 3 erläutert verschiedene technische Aspekte, die beim Website-Betrieb zu beachten sind. Es folgen Hinweise zu speziellen Beispielen unter Ziffer 4.

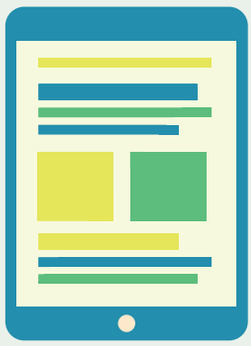
1. Impressum

1-Klick-Regel

Das Impressum muss mit einem Klick von der Startseite aus erreichbar sein. Die Datenschutzerklärung darf nicht im Impressum »versteckt« werden. Eine Ausnahme kann bei eindeutigem Hinweis auf beide Punkte (»Datenschutz & Impressum«) gelten.
Das Impressum muss die folgenden, notwendigen Angaben enthalten (Ein Kontaktformular allein reicht nicht!):

Ladungsfähige Anschrift!

- Name der Jugendverbandes (vollständig) sowie Angabe der Rechtsform,
- Anschrift,
- Telefon- und Mail-Adresse,
- Fax (sofern vorhanden),
- Vertretungsberechtigte,
- das Vereins- oder Genossenschaftsregistergericht und die entsprechende Registernummer,
- Falls vorhanden, kann eine Umsatzsteueridentifikationsnummer angegeben werden. (Achtung: Nie sollte die Steuernummer angeben werden, da sonst unter ungünstigen Umständen Steuergeheimnisse ermittelt werden können.)
- Alle Verantwortlichen einer Webseite müssen angeben, ob sie einer Verbraucherschlichtungsstelle unterliegen und bereit sind, am Schlichtungsverfahren teilzunehmen. Die Verpflichtung entfällt, wenn weniger als 10 Personen beschäftigt sind.
- Name und Anschrift des Verantwortlichen für journalistisch-redaktionelle Inhalte.



Haftung für Inhalte und Links

Als Websitebetreiber sind Jugendverbände für eigene Inhalte auf den Seiten verantwortlich. Sie sollten darauf hinweisen, dass sie nicht verpflichtet sind, übermittelte oder gespeicherte fremde Informationen zu überwachen oder nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen.
Enthält die Webseite »externe Links« (Verlinkungen) zu anderen Webseiten, auf deren Inhalt sie keinen Einfluss haben, kann für diese Inhalte auch keine Gewähr übernommen werden. Für die Inhalte und Richtigkeit der bereitgestellten Informationen ist der jeweilige Anbieter der verlinkten Webseite verantwortlich. Darauf ist ebenfalls hinzuweisen.

2. Datenschutzerklärung

1-Klick-Regel

- Die Datenschutzerklärung muss von der Startseite aus mit einem Klick erreichbar sein.
- Notwendig ist mitzuteilen, wer die verantwortliche Stelle für die Verarbeitung der personenbezogenen Daten ist. Meist wird es der Jugendverband oder die sonstige Körperschaft sein, der oder die verantwortlich ist.

- Es sind Angaben zu machen, wie Kontakt aufgenommen werden kann. Hier ist eine Mail-Adresse oder ein Kontaktformular ausreichend.
- Name und Kontaktdaten der Datenschutzbeauftragten sind zu benennen. Notwendig ist ein Datenschutzbeauftragter, wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Werden von einem Jugendleiter nur Listen der Gruppenmitglieder verwaltet, dann sind sie nicht mitzuzählen. Sinnvoll kann der Hinweis sein, dass auf Grund der Größe kein Datenschutzbeauftragter benötigt wird.
- Die zuständige Datenschutzbehörde ist zu benennen. Diese ergibt sich aus dem jeweiligen Bundesland, in dem der Träger seinen Sitz hat. Für Hamburg ist dies der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Ludwig-Erhard-Str 22 (7. OG), 20459 Hamburg, T. (040) 428 54 – 4040, Fax: (040) 428 54 – 4000, mailbox@datenschutz.hamburg.de. Den betroffenen Personen steht die Möglichkeit zu, sich direkt an die Aufsichtsbehörde zu wenden. Sie müssen sich nicht erst an die Verantwortlichen (im Jugendverband) wenden.

Verständliche und klare Sprache

- Die Datenschutzerklärung ist in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Datenschutzerklärungen mit verschachtelten Sätzen oder mit zahllosen Seiten erfüllen diese Voraussetzung nicht.

Verwendungszwecke + Rechtsgrundlage

- Der Umfang der Datenerhebung ist zu nennen. D.h.: Welche Daten werden erhoben? Wie werden sie weiter verarbeitet? Ebenso ist der Zweck anzugeben, für den die Daten erhoben werden (z.B. zur Verbesserung des Verbandsangebotes oder um die Website technisch betreiben zu können). Es kann in der allgemeinen Datenschutzerklärung auch darauf verwiesen werden, dass die Angaben der Verarbeitungszwecke an den entsprechenden Stellen auf der Websites erfolgen. Kurz zu erwähnen ist, ob eine Weitergabe der Daten an Dritte erfolgt. Denken Sie dabei an Web-Hoster, Social Media und ähnliches.

Art. 6 DSGVO

- Zu nennen ist außerdem die Rechtsgrundlage der Datenverarbeitung. Es können drei Gründe sowie andere in der DSGVO genannten Gründe vorliegen: Der Vertrag, das berechtigte Interesse und die Einwilligung sind die zumeist vorliegenden Gründe. Sollten diese nicht passen, lassen Sie sich beraten.

Speicherdauer von personenbezogenen Daten

- Es muss ein Hinweis darauf erfolgen, für welchen Zeitraum personenbezogene Daten gespeichert werden. Bereits die IP-Adresse, durch die sich die Computer untereinander identifizieren, ist ein personenbezogenes Datum. Das gilt auch für dynamische IP-Adressen. Falls die Speicherdauer nicht konkret zu bestimmen ist, müssen die Kriterien für die Festlegung dieser Dauer genannt werden.

Rechte der betroffenen Person

3. Auskunftspflichten und Rechte der Besucher

Personen, die die Webseite besuchen, stehen gewisse Auskunftsrechte zu. Auf diese ist hinzuweisen:

Art. 15 DSGVO

- Bestätigung: Der Verantwortliche oder der Jugendverband hat auf Nachfrage zu bestätigen, ob personenbezogene Daten verarbeitet werden.

Art. 15 DSGVO

- Auskunft: Der Verein hat jederzeit Auskunft zu erteilen. Anzugeben ist, welche Daten über den Anfragenden gespeichert werden, einschließlich der Herkunft und Empfänger der Daten sowie dem Zweck der Datenverarbeitung.

Folgende Auskünfte sind an Anfragende unentgeltlich zu geben:

- die Verarbeitungszwecke,
- die Kategorien personenbezogener Daten, die verarbeitet werden,
- der Empfänger oder die Kategorien von Empfängern,
- die geplante Speicherdauer der personenbezogenen Daten bzw. Kriterien ihrer Festlegung,

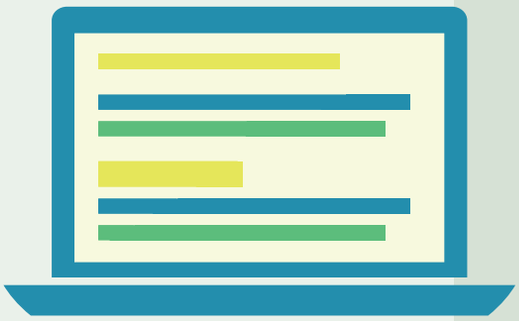
- das Bestehen des Rechts auf Berichtigung, Löschung oder Einschränkung der erhobenen Daten und des Widerspruchs zur Verarbeitung der personenbezogenen Daten sowie des Beschwerderechts bei der zuständigen Aufsichtsbehörde,
- Soweit die personenbezogenen Daten nicht beim Anfragenden erhoben wurden, ist die Herkunft der Daten zu nennen.
- Falls zutreffend: das Bestehen einer automatisierten Entscheidungsfindung einschl. Profiling gem. Art. 22 Abs. 1, Abs. 4 DSGVO.

Darüber hinaus gehende Angaben dürfen für den Anfragenden kostenpflichtig gemacht werden.

Rechte der Besucher in Bezug auf ihre erhobenen Daten

- **Berichtigung**: Wenn die verarbeiteten personenbezogenen Daten, die den Anfragenden betreffen, unrichtig oder unvollständig sind, dann sind diese zu berichtigen und/oder zu vervollständigen.
- **Löschung:** Es besteht dass Recht darauf, dass personenbezogene Daten gelöscht werden. — Art. 16 DSGVO
- **Einschränkung:** Die Einschränkung der Verarbeitung der personenbezogenen Daten kann verlangt werden. — Art. 17 DSGVO
- **Widerspruch:** Der Verarbeitung personenbezogener Daten kann widersprochen werden. Dies gilt nur unter bestimmten Voraussetzungen: Einschlägig ist hier im Wesentlichen die Datenverarbeitung auf Grund des berechtigten Interesses des Jugendverbandes. — Art. 18 DSGVO, Art. 21 DSGVO
- **Widerruf einer Einwilligung:** Ferner haben Betroffene das Recht, eine gegebene Einwilligung jederzeit zu widerrufen. Der Widerruf gilt für die Zukunft. — Art. 13 DSGVO
- **Datenübertragung:** Werden personenbezogene Daten zur Verfügung gestellt, so müssen diese in einem strukturierten, gängigen und maschinenlesbaren Format ausgehändigt oder an Dritte übermittelt werden. Dazu gehört auch die direkte Übermittlung an einen anderen Verantwortlichen. Das muss kein Jugendverband sein. — Art. 20 DSGVO

Sinnvoll ist es abschließend zu erwähnen, wie und bei wem diese Rechte geltend gemacht werden können. Es kann eine konkrete Person oder ein Funktionträger (z.B. datenschutzrecht@[jugendverbandsname].de) benannt werden.

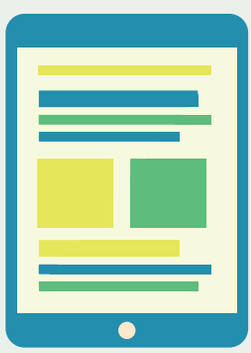


3. Technisches: Drittanbieter, Facebook, Google Analytics, Cookies und Co.

Durch Plugins oder Social Media werden personenbezogene Daten übermittelt und durch die jeweiligen Anbieter gespeichert. Dies gilt insbesondere dann, wenn Plugin-Funktionen kostenlos angeboten werden.

Plugins: Beispiel Facebook

Besonders problematisch ist das Plugin von Facebook, das auf vielen Websites als Button eingebettet ist. Wenn der Nutzer auf »Gefällt mir« klickt oder einen Kommentar abgibt, wird die entsprechende Information vom Browser direkt an Facebook übermittelt und dort gespeichert. Diese Vorlieben werden gesammelt und an Facebook-Freunde weiter gegeben. Wer beim Surfen zugleich bei Facebook eingeloggt ist, ermöglicht es Facebook, die Chronik aller aufgerufenen Websites mitzulesen und dem Facebook-Konto des Websitebesuchers direkt zuzuordnen. Auch wer nicht eingeloggt ist oder gar kein Facebook-Konto besitzt, wird über Websites, die ein Facebook-Plugin nutzen, von Facebook miterfasst (Surf-Chronik, IP-Adresse). Zwar können sich User durch die Implementierung eines Plugins, z.B. mit dem »Facebook Blocker« gegen diese Überwachung schützen, doch Jugendverbände sollten sich fragen, ob eine Implementierung eines Facebook-Buttons auf ihrer Website notwendig ist und, wenn dies gewünscht ist, wie dieser datenschutzkonform eingebettet werden kann. Denn jeder Website-Betreiber ist nach der DSGVO



verpflichtet, den Websitebesuchern die Datenübermittlung zu verdeutlichen und verständlich zu machen, wie eine Einwilligung erteilt bzw. wie ohne Datenübermittlung gesurft werden kann.

Zwei-Klick-Social-Media-Button mit Protokollierung nutzen!

Die Lösung: Nach bisheriger Rechtslage ist es empfehlenswert, derlei Social-Media-Plugins wie Facebook, Instagram oder Twitter nur im Rahmen einer »Zwei-Klick-Lösung« zu nutzen. Damit werden die Daten des Website-Besuchers erst nach explizit erteilter Einwilligung an Dritte übermittelt.

Verwendung von Cookies

Viele Websites nutzen **Cookies**, sei es um technische Funktionen bereit zu stellen oder, wie bei den meisten kommerziellen Websites, um den User auszuspionieren.

ePrivacy-Richtlinie von 2002/58/EG

Nach noch gültigem Recht (ePrivacy-Richtlinie) hat jeder Nutzer die Möglichkeit, seinen Browser bezüglich Cookies einschlägig zu konfigurieren und die Annahme von Cookies zu unterbinden oder zu begrenzen. Die kommende ePrivacy-Verordnung wird voraussichtlich eine Richtlinie zur Einwilligungslösung bieten.

Empfehlenswert ist es daher, schon jetzt einen **Banner** auf die Website zu setzen, der auf die Verwendung von Cookies hinweist und darüber informiert, dass beim weiteren Besuch der Webseite von der Einwilligung zur Verwendung von Cookies ausgegangen wird.

Cookies skalieren

Zudem gibt es die Möglichkeit, Cookies zu »skalieren«. Dabei kann der Nutzer wählen, ob die Webseite zusätzlich zu den für die Nutzerfreundlichkeit der Webseite erforderlichen Cookies auch anderweitige Cookies (z.B. für Marketingszwecke) einsetzen darf. Für selbst eingesetzte Cookies und für Logfiles sollte die Speicherdauer angegeben werden.

Tracking-Zweck erläutern

Viele Betreiber einer Website setzen **Tools zur Website-Analyse** ein, um die Aufrufe der einzelnen Webpages statistisch aufzuschlüsseln. Bekannte Anbieter dieser Web-Trackingtools sind u.a. Google Analytics, Matomo (ehemals Piwik) oder eTracker. Die Webanwendung Matomo kann auf einem eigenen Server betrieben werden. Dadurch bietet sie bei der Speicherung datenschutzrechtlich sensibler Logdaten mehr Nutzerprivatsphäre, da die Daten nicht automatisch mit Dritten geteilt werden. Beim Einsatz von Google Analytics hingegen wandern diese personenbezogenen Daten in die USA. Noch rechtfertigt das »Privacy Shield«-Abkommen die Datenübermittlung in die USA. Das kann sich jedoch bald ändern. Daher ist von einem Einsatz dieser Software abzuraten.

Disclaimer

Noch ist es beim Einsatz von Trackingtools ausreichend, wenn Usern erklärt wird, wie sie das Tracking verhindern können (Opt-Out). Dies könnte sich ändern! Nach der DSGVO ist Tracking zulässig, soweit die Interessen und Umstände im Einzelfall berücksichtigt werden (Bsp.: auf den Nutzer abgestimmte Werbung). Die kommende ePrivacy-Verordnung könnte zudem verlangen, dass vom Nutzer eine eindeutig bestätigende Einwilligung eingeholt werden muss (Opt-In).

Weitergabe personenbezogener Daten an Dritte

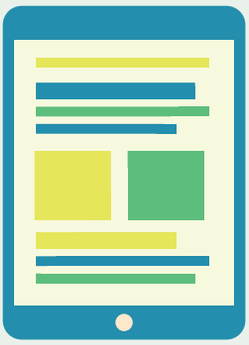
Grundsätzlich gilt: Werden auf der Website andere Dienstleister – wie Social-Media-Plugins oder Analysedienste – eingebettet, so ist in der Datenschutzerklärung darauf hinzuweisen, dass personenbezogene Daten zur Verarbeitung an Dritte weitergegeben werden. Gängige Dienstleister sind u.a. ...

- Bezahldienste,
- Third-Party-Cookies,
- Social-Media-Plugins wie Facebook, Instgram, Twitter, Youtube, etc.
- Google Maps, Google Fonts, ReCaptcha von Google,
- Websiteanalysedienste (z.B. Google Analytics),
- Anzeigen und Marketing-Dienste (z.B. Google AdSense).

Alternativen suchen

Wenn solche Dienste genutzt werden sollen, ist zu überlegen, ob technische Lösungen realisiert werden können, die eine datenschutzfreundliche Nutzung ermöglichen: Beispielsweise können Webfonts auf dem eigenen Server eingebettet statt vom Googleserver nachgeladen werden. Youtube-Videos hingegen sollten nicht

eingebettet werden, sondern als Link den Nutzer direkt auf die Youtube-Website verweisen. Anstelle von ReCaptcha (Google) zur Spamvermeidung bei Formularfeldern können eigene Alternativlösungen programmiert werden. Diese und andere technische Lösungen (Zwei-Klick-Social-Media-Button; s.o.) helfen, die eigene Website datenschutzfreundlich – Privacy by design – zu gestalten. Ist eine Nutzung von externen Dienstleistern unumgänglich, so sind die Besucher der Website auf deren Einbettung einerseits hinzuweisen und ihnen ist andererseits zu erläutern, wie sie die Datenübertragung unterbinden können. Zudem sind in der eigenen Datenschutzerklärung Links zu den jeweiligen Datenschutzerklärungen der genutzten Drittanbieter mit aufzunehmen und regelmäßig zu kontrollieren.



Newsletter

Wird ein **Newsletter** zur Verfügung gestellt, so werden die Daten in der jeweiligen Eingabemaske an den für die Verarbeitung Verantwortlichen übermittelt. Bei der Anmeldung zum Newsletter werden die IP-Adresse des Nutzers sowie Datum und Uhrzeit der Registrierung gespeichert. Die Besteller müssen die Anmeldung in einer zweiten Mail bestätigen. Dies dient dazu, einen Missbrauch der Dienste oder der Mail-Adresse der betroffenen Person zu verhindern. Die Bestellenden sind auf die Weitergabe der Daten an Dritte, Verwendungszweck, Kündigungsmöglichkeit und Widerrufsmöglichkeit hinzuweisen.
Ein entsprechender Link für eine Kündigung ist in jedem Newsletter einzubauen.

Einwilligung im double-opt-in-Verfahren

Kontaktformular

Wenn ein **Kontaktformular** auf der Website zur Verfügung gestellt wird, ist die Website dringend im https-Modus zu betreiben! Denn eine Datenübertragung via Internet erfordert eine Verschlüsselung der Website. Zudem muss der Grundsatz der Datensparsamkeit gewahrt werden! So sollten Pflichtangaben und freiwillige Angaben entsprechend gekennzeichnet werden.

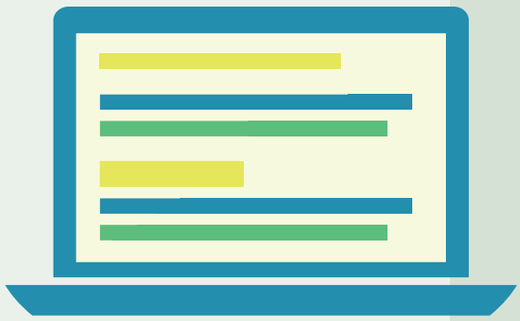
AV-Vertrag mit dem Webhoster

Wird die Website über einen Anbieter (Webhoster) ins Internet geladen, so hat dieser Anbieter Zugriff auf personenbezogene Daten (wie IP-Adressen der Besucher). Mit dem Webhoster ist daher ein **Vertrag zur Auftragsverarbeitung** abzuschließen. Dieser AV-Vertrag regelt die Handhabung der personenbezogenen Daten. Der Webhoster darf nur auf Weisung handeln. Er muss garantieren, geeignete technische und organisatorische Maßnahmen einzuhalten. Auch die Kontrollbefugnis des Jugendverbandes sowie die wechselseitigen Informationspflichten sind in dem AV-Vertrag zu regeln. Die meisten Anbieter stellen vorformulierte Verträge zur Verfügung.

4. Einzelne Beispiele

Veröffentlichung von Funktionsträgerdaten

Die Veröffentlichung von Name, ausgeübter Funktion und der vereinsbezogenen Erreichbarkeit (z.B. Telefonnummer oder Mail-Adresse) von Funktionsträgern eines Jugendverbandes (z.B. Vorstand, Jugendleiter) ist aufgrund einer Interessenabwägung zugunsten des Jugendverbandes datenschutzrechtlich zulässig. Denn ein Verein hat ein berechtigtes Interesse daran, konkrete Ansprechpartner nach außen zu benennen, um eine Kontaktaufnahme zu ermöglichen. Die Interessen oder Grundrechte der betroffenen Funktionsträger stehen gegenüber diesem berechtigten Interesse nach, zumal die Veröffentlichung der zuvor genannten vereinsbezogenen Daten einen verhältnismäßig geringfügigen Eingriff in das Persönlichkeitsrecht der betroffenen Personen darstellen.
Etwas anderes gilt aber für darüber hinausgehende personenbezogene Daten, z.B. die Privatanschrift oder eine private Telefonnummer. In diesen Fällen überwiegen regelmäßig die Interessen der betroffenen Personen. Die Veröffentlichung bedarf dann einer expliziten Einwilligungserklärung der betroffenen Personen.



Fotos

Vor einer **Veröffentlichung von Fotos** einzelner Personen im Internet sind grundsätzlich Einwilligungserklärungen der fotografierten Personen einzuholen. Ausnahmsweise kann die Veröffentlichung von Fotos im Internet auch ohne Einwilligung gerechtfertigt sein. Sie bestehen dann, wenn es sich um Bilder handelt, bei denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen, oder wenn es Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen (Beispiel: Vereinsfest) sind, an denen die dargestellten Personen teilgenommen haben. Ausführliche Informationen befinden sich im Kapitel Fotos (auf S. 21).

Protokolle von Gremiensitzungen

Protokolle der Jugendverbandsgremien beinhalten in der Regel personenbezogene Funktionsträger- und Mitgliedsdaten. Ohne Einwilligung der betroffenen Personen ist eine Veröffentlichung im Internet regelmäßig unzulässig. Hier überwiegen die Interessen der betroffenen Person am Schutz ihrer personenbezogenen Daten das grundsätzlich berechtigte Interesse des Vereins an einer Internetveröffentlichung zur Information Dritter.

Etwas anderes kann aber dann gelten, wenn ein benutzerbeschränktes Vereinsforum im Internet angeboten wird, auf das nur Vereinsmitglieder Zugriff nehmen können und die Protokolle nur in diesem zur Verfügung gestellt werden.

Sofern ein Verein die Veröffentlichung von Sitzungsprotokollen im Internet – ohne Benutzerbeschränkung und ohne Einholung von Einwilligungserklärungen der betroffenen Personen – vornehmen möchte, sollten die personenbezogenen Angaben in den Protokollen vor der Veröffentlichung unkenntlich gemacht resp. geschwärzt werden.

Publikation von Namen auf Wettkampfslisten

Ein schwieriges Feld ist die **Internet-Veröffentlichung von Starter- und Ergebnislisten** bei Sport- oder anderen Wettkämpfen. In der Regel ist eine Veröffentlichung durch einen Jugendverband nur mit Einwilligung der betroffenen Personen zulässig. Bei Minderjährigen ist grundsätzlich eine Einwilligung der Sorgeberechtigten einzuholen. Bei über 16-jährigen ist außerdem die Einwilligung der Jugendlichen selbst erforderlich. Für Minderjährige im Alter zwischen 14 und 16 Jahren kommt es auf die Einsichtsfähigkeit an. Es empfiehlt sich, bereits Jugendliche ab 14 Jahre um eine Einwilligung zu bitten.

Soziale Medien

Soziale Medien und die DSGVO

Soziale Medien wie Facebook und Instagram oder Messenger-Dienste wie WhatsApp und Snapchat sind aus der Kommunikation unter Jugendlichen kaum mehr wegzudenken. Eine Chat-Gruppe gibt es fast immer. Fehlende Netiquette und mangelnde Zeit- oder Themenbegrenzungen führen in Chatgruppen häufig zu Problemen wie Cyber-Mobbing oder Überforderung. Der Umgang im Chat kann auch das Gruppenklima negativ beeinflussen.
Die Nutzung beliebter Dienste wie Instagram oder WhatsApp ist mit Altersbeschränkungen durch die Anbieter verbunden. Diese sind in den jeweiligen AGB nachzulesen. Für jüngere Nutzer sind in diesen Diensten keine ausreichenden Sicherheitsvorkehrungen vorhanden.
Die Frage für Jugendverbände lautet: Welche Sozialen Medien können sie unter dem Aspekt des Datenschutes verantwortungsbewusst nutzen? Von welchen sind die Finger zu lassen?

Problemlagen

Die auf dem Markt angebotenen Messenger-Dienste verarbeiten personenbezogene Daten in sehr unterschiedlicher Weise. Die Frage nach dem datenschutzkonformen Einsatz einzelner Messenger-Dienste zur Kommunikation kann deswegen nicht einheitlich beantwortet werden. Ein datenschutzkonformer Einsatz von Messenger-Dienste ist stets vor dem Hintergrund der DSGVO zu bewerten.
Werden Messenger-Dienste eingesetzt, die personenbezogene Daten ihrer Nutzer kommerziell verwerten, verstoßen Jugendverbände gegen den datenschutzrechtlichen Grundsatz der zweckgebundenen Datenverarbeitung. Ein weiteres Problem liegt im standardmäßigen Auslesen der auf dem Endgerät des Nutzers gespeicherten Kontaktdaten und deren anschließendem Abgleich mit allen vom Anbieter gespeicherten Bestandsdaten.
Es sollte daher die Frage geklärt werden, ob der Einsatz von Messenger-Dienste zur Erledigung der Aufgaben im Jugendverband überhaupt erforderlich ist.

Prüfkriterien

Zur Bestimmung eines datenschutzkonformen Messenger-Dienstes sind insbesondere die folgenden Kriterien heranzuziehen:

- Eine Ende-zu-Ende-Verschlüsselung der über den Messenger-Dienst ausgetauschten personenbezogenen Daten muss gewährleistet sein.
- Der Anbieter nutzt die empfangenen personenbezogenen Daten ausschließlich für Zwecke der Übertragung der Inhalte zwischen den Teilnehmenden einer Unterhaltung.

No-Go's und Alternativen

Vor diesem Hintergrund können mit Blick auf den Einsatz folgende allgemeine Hinweise zu einzelnen Messenger-Diensten gegeben werden:

- Gegen den Einsatz von **WhatsApp** und **Telegram** gibt es erhebliche Datenschutzbedenken. Vom Einsatz dieser Messenger-Dienste wird deswegen abgeraten.
- Auch beim Einsatz von **Signal** verbleiben Datenschutzbedenken, weil dieser Dienst personenbezogene Daten seiner Nutzer außerhalb des Geltungsbereichs der DSGVO verarbeitet. Der Gebrauch dieses Messenger-Dienstes kann daher nicht empfohlen werden.
- Gegen den Einsatz von Messenger-Diensten wie **SIMSme** und **Threema**, die auf Servern in Deutschland bzw. der Schweiz gehostet werden, bestehen zur Zeit keine Datenschutzbedenken.

Speziell auf eine dienstliche Nutzung zugeschnitten sind **SIMSme Business** und **Threema Work**. Es muss sichergestellt werden, dass der Anbieter des verwendeten Messenger-Dienstes aufgrund der Nutzungsbedingungen den dienstlichen Einsatz gestattet.

- Die Entwicklung sowie der Einsatz und Betrieb eines eigenen Messenger-Dienstes wäre die beste Alternative.

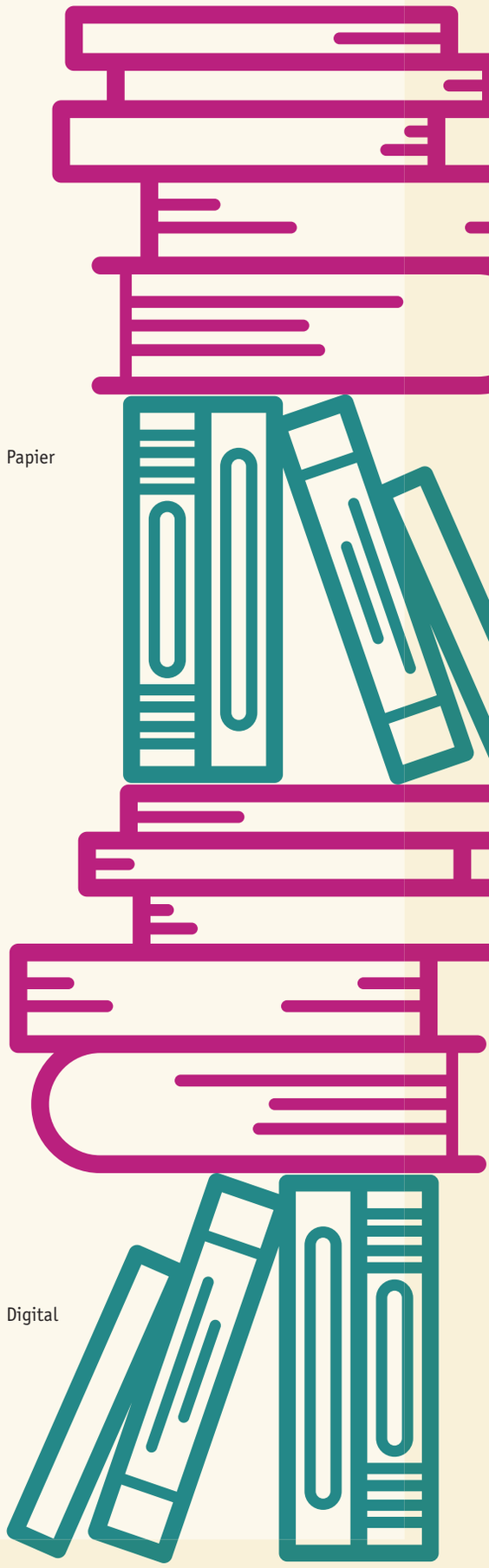
Die Nutzung von Messenger-Diensten unterliegt einer ständigen Veränderung. Die Art und Weise wie Messenger-Dienste mit den Daten der Nutzer umgehen, kann sich grundsätzlich bei allen Anbietern jederzeit ändern. Beim Einsatz eines Messenger-Dienstes sind Jugendverbände daher verpflichtet, sich über die Verarbeitungsbedingungen des genutzten Dienstes auf dem Laufenden zu halten und zu prüfen, ob die datenschutzrechtlichen Anforderungen beständig erfüllt werden. Verlässliche Informationen veröffentlichen die jeweilige Aufsichtsbehörde der verschiedenen Bundesländer, die Aufsichtsbehörden der Kirchen (Landeskirchen) und die Datenschutzkonferenz. Zudem finden sich im Netz viele hilfreiche Seiten, die über die Risiken einzelner Apps aufklären (siehe Hinweise in der Spalte).
Unabhängig von diesen allgemeinen Hinweisen ist bei der Einführung von Messenger-Diensten immer auch die konkrete Situation im Einzelfall zu berücksichtigen.

Jugendverbände sind gefodert, Alternativen zu überlegen und zu fördern. Dies hängt auch mit dem Auftrag der Jugend(verbands)arbeit zusammen, die Entwicklung von Jugendlichen zu selbstbewussten und selbstständigen Menschen zu fördern.

Mehr auf:
www.jugendschutz.net
www.surfen-ohne-risiko.net
www.chatten-ohne-risiko.net/kompass/
www.kompass-social.media

Publikationen

Eine Verbandszeitschrift kann in unterschiedlicher Form verbreitet werden. Sie kann papierbasiert als Zeitung oder digital als Newsletter versendet werden. Sie kann allgemein ausliegen oder nur an Vereinsmitglieder ausgegeben werden. Der einzuhaltende Datenschutz unterscheidet sich dabei nur geringfügig.
Die Besonderheit bei einer digitalen Verbreitung ist, dass Publikationen im Internet weltweit abrufbar sind. Sie können durch Suchmaschinen aufgefunden und ggfs. mit anderen Informationen verknüpft werden. Dies beinhaltet auch, dass die ins Internet gestellten Informationen, einschließlich Fotos, kopiert und weiterverbreitet werden können. Alle Fragen zur Veröffentlichung von Fotos klärt das nachfolgende Kapitel auf Seite 21; in diesem Abschnitt werden stehen schriftliche personenbezogene Informationen im Mittelpunkt.



1. Verbandszeitschrift

Wenn Jugendverbände eine Zeitschrift herausgeben, sind bei personenbezogenen Informationen datenschutzrechtliche Vorgaben zu beachten. Obwohl eine Verbandszeitung in erster Linie für Mitglieder bestimmt ist, handelt es sich dabei um eine Übermittlung an einen nicht überschaubaren Kreis von Adressaten. Es kann nicht ausgeschlossen werden, dass auch Fremde die Zeitung lesen.
Die Publikation personenbezogener Daten über eine Zeitschrift ist daher nur mit einem Rechtsgrund zulässig. Für Jugendverbände gibt es dafür im Wesentlichen drei berechtigte Gründe: die Erfüllung der Ziele des Jugendverbandes, sein berechtigtes Interesse oder die Einwilligung des Mitglieds.
Persönliche Nachrichten mit einem Bezug zum Jugendverband wie Eintritte, Austritte, Spenden, Geburtstage und Jubiläen können veröffentlicht werden, wenn dem Verband keine schutzwürdigen Belange des Betroffenen bekannt sind, die dem entgegenstehen. Es empfiehlt sich, beim Eintritt in einen Jugendverband darauf aufmerksam zu machen, welche Ereignisse im Vereinsblatt veröffentlicht werden und um eine Mitteilung zu bitten, wenn dies nicht gewünscht wird.
Informationen aus dem persönlichen Lebensbereich eines minderjährigen Vereinsmitglieds (z.B. Abschluss von Schul- und Berufsausbildungen) dürfen nur veröffentlicht werden, wenn die Erziehungsberechtigten und das 16- bis 17-jährige Mitglied ausdrücklich das Einverständnis dazu gegeben haben.
Die »dienstliche« Erreichbarkeit von Funktionsträgern des Vereins, insbesondere der Vorstände, können in der Regel bekannt gegeben werden. Dagegen dürfen Mitgliederlisten für gewöhnlich nur dann veröffentlicht werden, wenn die Betroffenen explizit eingewilligt haben. Ist es das Ziel des Vereins, persönliche Kontakte zu fördern (Satzung), ist eine Einwilligung nicht notwendig.

2. Newsletter

Digitale Newsletter werden üblicherweise per Mail versendet. Technisch ist auch der Versand per Messenger-Dienst oder über Soziale Medien denkbar. Bei jeglichem digitalen Versand ist die Abgrenzung zwischen Werbung und vereinsinterner Information besonders wichtig. Ein Newsletter ist dann als Werbung einzuordnen, wenn beispielsweise offene Angebote oder Veranstaltungen des Jugendverbandes beworben werden, die über den Kreis der Mitglieder hinausgehen. Für den Versand ist somit eine Einwilligung des Empfängers zwingend notwendig. Ein Versand unangeforderter

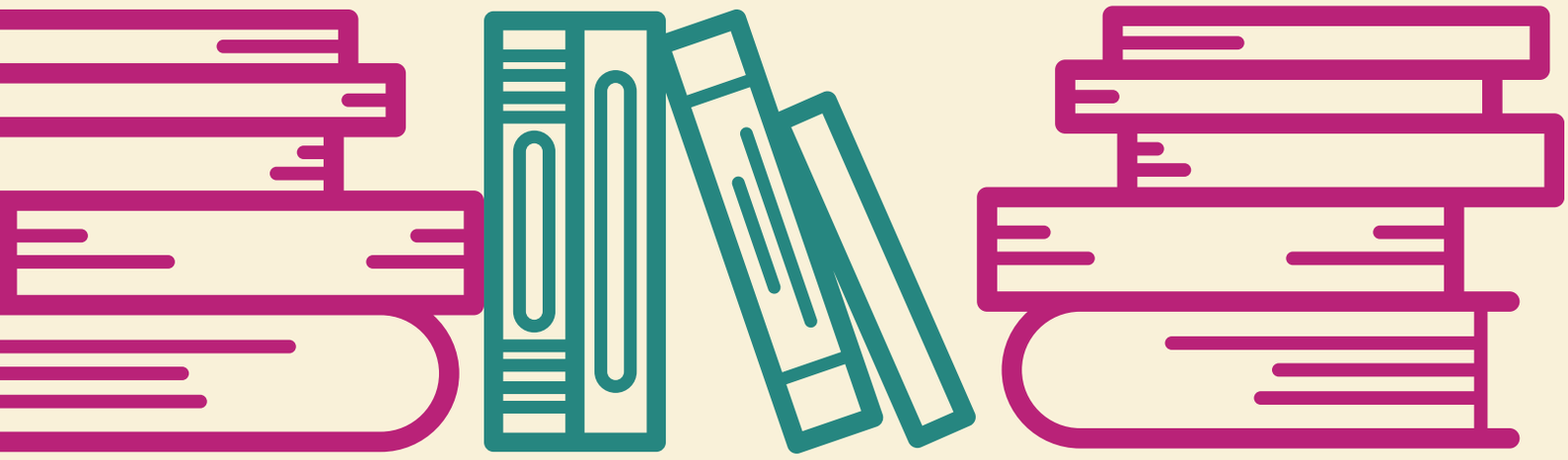
kommerzieller Mails ist nicht erlaubt. Daher muss zuvor eine Einwilligung im sogenannten Double-Opt-In-Verfahren eingeholt werden. Das Double-Opt-in-Verfahren soll Schutz vor Spam gewähren. Ein Nutzer, der sich mit seiner Mail-Adresse in einen Verteiler eingetragen hat (Single Opt-in), erhält durch eine anschließende Bestätigungs-Mail die Möglichkeit, seine Anmeldung zu bestätigen. Bestätigt er die Anmeldung, ist der Double-Opt-in abgeschlossen. Im Newsletter ist auf die Weitergabe der Daten an Dritte, den Verwendungszweck, die Kündigungs- und Widerrufsmöglichkeit hinzuweisen. Ein entsprechender Link für eine Kündigung ist in jedem Newsletter einzubauen.
Wenn kein besonderes Mail-Marketing-Programm verwendet wird, kann die Einwilligung durch eine Eintragung in eine Liste (Single Opt-in) erteilt und dokumentiert werden. Immer ist darauf zu achten, dass alle Newsletter per Mail in Blindcopy (bcc) zu versenden sind. Auch bei diesem Verfahren muss auf die Weitergabe der Daten an Dritte, den Verwendungszweck, die Kündigungs- und Widerrufsmöglichkeit hingewiesen werden.
Bei Minderjährigen ist wiederum besonders darauf zu achten, dass die Erziehungsberechtigten und die 16- bis 17-jährigen Jugendlichen ausdrücklich eingewilligt haben.

3. Reklame für eigene Zwecke und Lobbyarbeit

Um Veranstaltungen oder Ferienfreizeiten zu bewerben, versenden Jugendverbände Einladungen oder Infoblätter an Interessierte der Jugendarbeit oder potentielle Teilnehmende. Dafür kann ein berechtigtes Interesse nach dem Vereinszweck vorliegen. Werbung für eigene Zwecke und Lobbyarbeit wird gemäß der Rechtsgrundlagen in den B2B-Bereich (Geschäftskunde zu Geschäftskunde) eingeordnet. Es ist erlaubt, mit papiernen Informationen Lobbyarbeit oder Reklame zu betreiben.
Bei einem digitalen Versand ist eine Einwilligung nicht notwendig, wenn …

- die Mail-Adresse durch eine Dienstleistung erhalten wurde (z. B. durch die Teilnahme der Person an einer vorangegangenen Veranstaltung),
- der neue Kontakt für die Bewerbung einer ähnlichen Dienstleistung stattfindet,
- der Empfänger der Verwendung seiner Mailadresse nicht widersprochen hat,
- und in der neuen Werbesendung deutlich darauf hingewiesen wird, dass der Verwendung der Mailadresse jederzeit widersprochen werden kann.

Bei Empfängern, die im Rahmen ihrer Tätigkeit auf Informationen von anderen angewiesen sind (z. B. jugendpolitische Sprecher einer Partei), kann davon ausgegangen werden, dass sie auch digitale Post empfangen möchten. Dies gilt zumindest dann, wenn die Mail-Adresse im Rahmen der Tätigkeit bekannt gegeben wurde.
Werden Informationen an Interessierte (z. B. potentielle Teilnehmende, potentielle Vereinsmitglieder) versendet, so liegt die Rechtfertigung dieses Vorgangs in der einen Vertrag vorbereitenden Handlung.



Fotos

Früher blieben persönliche Fotos weitgehend in den eigenen vier Wänden. Im digitalen Zeitalter können Fotos via Internet in einer Cloud gespeichert und auch geteilt werden. Für Jugendverbände stellt sich die Frage, in welcher Form Fotos erstellt und veröffentlicht werden dürfen. Die nachfolgenden Ausführungen gelten sowohl für digitale als auch für papierne Fotos. Einen Unterschied macht das Format nur hinsichtlich des Verbreitungsgrades. An die Frage, mit welcher Berechtigung fotografiert werden darf, schließt sich die Frage an, auf welchen Wegen – Newsletter, Website oder Verbandszeitschrift – die Fotos publiziert werden dürfen.

1. Rechtsgrundlagen und Problemlagen

Auf Fotos sind Personen leicht identifizierbar. Im digitalen Zeitalter gilt dies noch weitreichender. Denn digitale Fotos speichern weitere Informationen (Metadaten) wie Datum und Aufnahmeort (GPS). Diese Daten lassen Rückschlüsse zu, wann die aufgenommene Person sich wo aufgehalten hat. Damit stehen Fotografen sowohl beim Fotografieren als auch bei der Publikation der Aufnahmen vor der Herausforderung, wie die Regelungen der DSGVO in Bezug auf Fotos im Jugendverbandsalltag praktikabel einzuhalten sind.

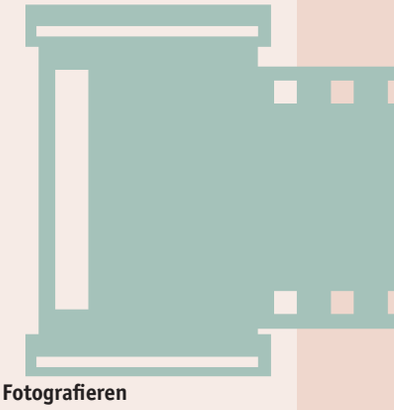
»Ich darf erst auf Veranstaltungen fotografieren, wenn ich von jedem Gast eine Einwilligungserklärung erhalten habe!«, so lautet die Befürchtung seit Einführung der DSGVO im Mai 2018. Diese Aussage ist so allgemein nicht zutreffend. Ein Fotograf braucht eine Berechtigung fürs Fotografieren und fürs Veröffentlichen. Diese kann sich entweder aus dem berechtigten Interesse des Veranstalters ergeben oder durch eine Einwilligung des Fotografierten zustandekommen.

Berechtigte Interessen des Veranstalters sind: die Dokumentation der Veranstaltung (z. B. im Hinblick auf Verwendungsnachweise der eingesetzten finanziellen Mittel) oder die Berichterstattung über eine Veranstaltung.

Prinzipiell kann sich damit der Veranstalter auf ein berechtigtes Interesse beim Fotografieren stützen. Abzuwägen sind dabei jedoch die berechtigten Interessen der fotografierten Person selber. Folgendes ist zu beachten:

- keine unvorteilhaften Posen,
- die Art der Fotografie muss im nachvollziehbaren Zusammenhang mit der Veranstaltung und dem Zweck der Veranstaltung stehen,
- Werbemaßnahmen zu Gunsten Dritter müssen für die fotografierte Person ausgeschlossen sein.

Berechtigtes Interesse des Jugendverbandes, Fotos zu schießen



Eine **Einwilligung** zum Fotografieren kann auch für Veranstaltungen im Voraus oder direkt vor Ort eingeholt werden. Bei Minderjährigen ist jedoch die Einwilligung der Erziehungsberechtigten und bei über 16-Jährigen auch der Jugendlichen nachzuweisen. Eine datenschutzrechtliche Einwilligung kann jederzeit ohne Angabe von Gründen frei widerrufen werden. Durch erfolgten Widerruf dürfen die zuvor erstellten Bilder nicht weiter verarbeitet werden.

Einwilligung zum Fotografieren

In den Zeiten vor DSGVO fand beim Fotografieren hauptsächlich das Kunsturheberrecht Anwendung. Nach diesem dürfen Bildnisse der Zeitgeschichte ohne Einwilligung veröffentlicht werden. Zeitgeschichte wird dabei weit gefasst. Darunter fallen

Bildnisse der Zeitgeschichte

auch allgemeine gesellschaftliche Ereignisse, wie z. B. das Sommerfest eines Vereins. Das Alltagsleben darf dokumentiert werden. Das Kunsturheberrecht bezieht sich nicht allein auf Ereignisse von historisch-politischer Bedeutung. Ein Grenzbereich stellt dabei die Öffentlichkeitsarbeit (z. B. Flyer etc.) dar. Diese hat grundsätzlich werbenden Charakter und schließt damit die Verwendung von Fotos ohne explizite Einwilligung aus. Erst wenn ein Beitrag über eine Veranstaltung eine journalistische (meinungsbildende) Qualität erreicht, dürfen dabei Fotos von der Veranstaltung verwendet werden. Es ist eine einzelfallbezogene Betrachtung vorzunehmen.
Abzuwägen sind dabei das Interesse des Vereins an der öffentlichen Dokumentation (Informationsfreiheit), die Art und Weise der Veröffentlichung (Vereinszeitung, Presse oder Social Media), die Dauer der Veröffentlichung und das berechtigte Interesse der Fotografierten an ihrem Persönlichkeitsschutz.

Fazit zum DSGVO-konformen Fotografieren

Fazit: Da eine Einwilligung zum Fotografieren von der abgebildeten Person jederzeit widerrufen werden kann, stellt diese Form für den Fotografen oder den Jugendverband eine unsichere Rechtsgrundlage dar und kann bei geplanten Publikationen (Zeitschrift, Website, Newsletter, Flyer) zu unabsehbaren Risiken führen. Daher sollte die Rechtfertigung zum Fotografieren und Publizieren der Fotos besser auf dem berechtigten Interesse des Jugendverbandes beruhen. Nachfolgend werden diese Rechtsabwägungen anhand von praxisnahen Situationen dargestellt.

2. Praxisbeispiele

Personen nur als »Beiwerk«

- **Personenabbild nur als Beiwerk zur Veranstaltung, bei einem Gebäude oder in der Landschaft**

Rechtsgrundlage: Berechtigtes Interesse | keine Einwilligung notwendig
Zu beachten: Keine unvorteilhaften Posen | Die Art der Veröffentlichung muss im nachvollziehbaren Zusammenhang mit der Veranstaltung stehen.
Hinweispflichten: Ein Verweis auf der Einladung (Flyer, Poster) zur Datenschutzerklärung kann reichen.

Geschlossene Veranstaltungen

- **Fotografieren bei einer geschlossenen, jugendverbandsinternen Veranstaltung oder Freizeit**

Bei einem Gruppentreffen, einer Vollversammlung, einem Seminar oder einer Freizeit ist es – auf Grund des überschaubaren Teilnehmerkreises – möglich, eine Einwilligung zum Fotografieren und zur Weiterverarbeitung der Fotos bei den Teilnehmenden direkt einzuholen. Dabei ist zugleich eine Datenschutzinformation (siehe Kasten auf S. 24) auszuhändigen. Besondere Vorschriften gelten bei Minderjährigen (s.o.). Die Art der Veröffentlichung muss im nachvollziehbaren Zusammenhang mit der Gruppe stehen. Wenn eine gruppeninterne Veröffentlichung geplant ist, liegt ein berechtigtes Interesse an der Dokumentation der Gruppenaktivitäten vor. Werden Fotos hingegen im Rahmen der Pressearbeit veröffentlicht, ist eine Einwilligung notwendig.
Rechtsgrundlage: Berechtigtes Interesse oder eine Einwilligung
Hinweispflichten: Mit Eintritt in den Jugendverband sollten für diese Fälle entsprechende Hinweise gegeben werden.

Große, öffentliche Veranstaltungen

- **Öffentliche Veranstaltungen oder Events**

Auch hier ist der Veranstalter oder Fotograf grundsätzlich dazu verpflichtet, alle Personen über die Datenschutzerkärung und Widerspruchsrechte beim Fotografieren zu informieren. Dies stellt jedoch bei einer großen Anzahl von Besuchern eine nicht praktikable Hürde dar.
Folglich sollte sich der Veranstalter hier auf sein berechtigtes Interesse zur fotografischen Dokumentation der Veranstaltung berufen. Die Besucher haben sich freiwillig

auf die Veranstaltung begeben und müssen damit rechnen, dass sie fotografiert und diese Bilder publiziert werden. Der Veranstalter hat dafür Sorge zu tragen, dass keine Fotos mit besonders unvorteilhaften Posen von Personen veröffentlicht werden. Die Art der Veröffentlichung muss im nachvollziehbaren Zusammenhang mit der Veranstaltung stehen.
Rechtsgrundlage: Berechtigtes Interesse
Hinweispflichten: Ein Verweis auf der Einladung (Flyer, Poster) zur Datenschutzerklärung kann reichen.

3. Publikationsweisen

• Internet

Einzelne Personen im Fokus

Vor einer Veröffentlichung von Fotos **einzelner Personen** im Internet sind grundsätzlich Einwilligungserklärungen der fotografierten Personen einzuholen. Ausnahmen bestehen aber dann, wenn es sich um Bilder handelt, bei denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen, oder wenn die Bilder Versammlungen, Aufzüge und ähnliche Vorgänge (Beispiel: Vereinsfest) zeigen, an denen die dargestellten Personen teilgenommen haben.

Große Anzahl von Personen

Fotos von einer öffentlichen Sportveranstaltung, Versammlungen, Aufzügen und ähnlichen Ereignissen, die eine **große Anzahl von Personen** zeigen, dürfen publiziert werden. Voraussetzung ist, dass der Vorgang in der Öffentlichkeit stattgefunden hat und die Darstellung des Ereignisses im Vordergrund steht.

Der Fokus entscheidet

Liegt der **Fokus eines Bildes** nicht auf der Veranstaltung als solcher sondern auf einzelnen Personen der Veranstaltung, greift die rechtliche Privilegierung des Veranstalters zur Publikation auf Basis seines berechtigten Interesses dagegen regelmäßig nicht. Personen, die dann einzeln oder in kleinen Gruppen abgelichtet werden, müssen vorher um ihr Einverständnis in das Fotografieren und in die Veröffentlichung der Fotos im Internet gebeten werden.

• Newsletter und Zeitungen

Für die Verbreitung von Fotos in Newslettern oder Vereinszeitungen gilt:
Soll das Verbandsleben dokumentiert werden (Informationsfreiheit), so ist eine Einwilligung zur Veröffentlichung der Fotos nicht notwendig. Sobald es sich überwiegend um Werbung handelt, wird eine Einwilligung notwendig.
Überwiegt das Interesse des Fotografierten an seiner Personenidentität, ist eine Einwilligung erforderlich. Bei Kindern und Jugendlichen überwiegt meist das Persönlichkeitsrecht, so dass der Minderjährigenschutz zu beachten und die Einwilligung der Erziehungsberechtigten und des Jugendlichen einzuholen ist.

• Soziale Medien

Für die Veröffentlichung von Fotos in Sozialen Netzwerken ist eine Einwilligung notwendig. Dies gilt auch, wenn der Zugriff des Accounts begrenzt ist.

4. Guideline zum Fotografieren im Jugendverband

Jeder Jugendverband sollte eine interne Handreichung erstellen, die den Umgang mit Fotos und der Publikation für alle Mitglieder erläutert.

- Werden Vereinsmitglieder, Teilnehmer oder sonstige Dritte fotografiert, dann sollten Formularblätter »Hinweise zum Fotografieren auf Veranstaltungen« und »Erklärung und Einwilligung zum Zwecke der Veröffentlichung« zur Verfügung gestellt und verwendet werden.
- Stets ist zu dokumentieren, ob auf das Fotografieren bei einer Veranstaltung hingewiesen wurde und die datenschutzrechtlichen Hinweise aushingen. Ebenso sind die gegebenen Einwilligungen von Personen zur Verwendung von Fotos oder

Bei Veranstaltungen aushängen!

Filmaufnahmen zu dokumentieren. Hierzu sind Name und Vorname, bei nicht zum Verein gehörenden Personen auch deren Anschrift zu erfassen und in das entsprechende Formular einzutragen.

- Wird eine Einwilligung für Filmaufnahmen eingeholt, muss die Einwilligungserklärung ein Foto der einwilligenden Person enthalten. Diese Einwilligungserklärung ist bei den Filmaufnahmen von einer verantwortlichen Person stets mitzuführen. Zudem ist zu kontrollieren, dass nur einwilligende Personen auf den Filmaufnahmen zu sehen sind.
- Eine Einwilligung kann auch eingeschränkt werden: Beispielsweise kann einer Verwendung im Intranet zugestimmt, einer Verwendung im Internet (öffentlicher Bereich) jedoch widersprochen werden. Entsprechende Einwilligungsinhalte sind in solchen Fällen aus dem verwendeten Formular zu streichen.
- Die ausgefüllten und unterschriebenen Einwilligungserklärung sind zu archivieren.
- Alle Verbandsmitglieder, Gruppenleitende, Trainer, Ehrenamtliche oder sonstige Verantwortliche sind aufgefordert sicherzustellen, dass sie den Datenschutzvorgaben beim Fotografieren ordnungsgemäß nachkommen.

5. Aushang: Datenschutzinformation

Der nachfolgende Text kann als Vorlage für Veranstaltungen genutzt werden, um auf die Datenschutzrichtlinien beim Fotografieren hinzuweisen.

Datenschutzinformationen

Auf dieser Veranstaltung wird fotografiert oder gefilmt. Wenn Sie nicht abgebildet werden möchten, lassen Sie es dem jeweiligen Fotografen bitte wissen. Wir können leider nicht verhindern, dass Sie auf Aufnahmen größerer Menschenansammlungen abgebildet werden.

Veranstwortliche Stelle: [Name und Kontaktdaten des Verantwortlichen / Veranstalters]

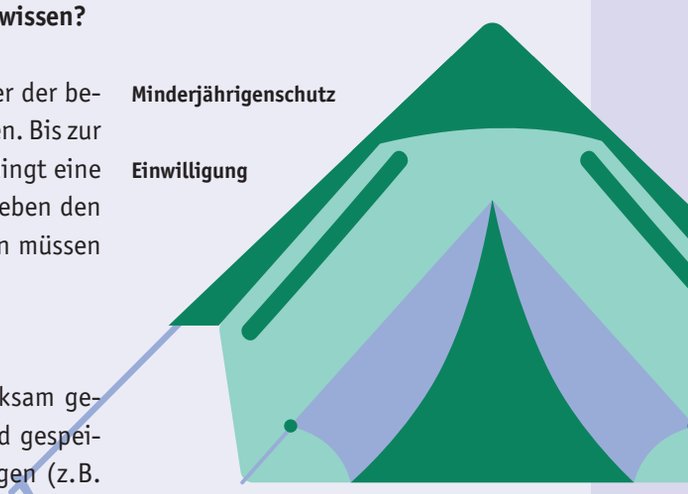
Zweck der Verarbeitung, Rechtsgrundlage und Speicherdauer: Die Aufnahmen werden im Rahmen unserer Presse- und Öffentlichkeitsarbeit zur Darstellung und Dokumentation unserer Aktivitäten auf unserer Website, unserer Zeitschrift oder unseren Social-Media-Kanälen veröffentlicht. Hierin liegt auch unser berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit f DSGVO. Nicht veröffentlichte Fotos werden zwei Jahre lang digital gespeichert und danach gelöscht.

Empfänger: Die Aufnahmen geben wir im Rahmen unserer Pressearbeit ggfs. auch an Medienvertreter weiter. Auf Wunsch stellen wir das Bildmaterial auch Personen und Organisationen zur Verfügung, die an unserer Veranstaltung beteiligt sind.

Widerspruchsrecht: Sie haben das Recht, gegen die genannte Verarbeitung Widerspruch zu erheben. Nutzen Sie hierfür bitte die oben genannten Kontaktdaten. Soweit die rechtlichen Voraussetzungen vorliegen, werden wir zukünftig durch geeignete Maßnahmen die weitere Verbreitung der entsprechenden Aufnahmen unterlassen. Löschungen auf Websites oder in Social-Media-Kanälen erfolgen im Rahmen der technischen Möglichkeiten.
Weitere Informationen zum Thema Datenschutz, insbesondere über Ihre Rechte als betroffene Person, erhalten Sie in unserer Datenschutzerklärung, die am Eingang eingesehen oder auf unserer Website [link zur Datenschutzerklärung] abgerufen werden kann.

Veranstaltungen und Freienfreizeiten

Werden Veranstaltungen oder Ferienreisen organisiert, stellen sich Fragen zum Datenschutz hauptsächlich bei der Erhebung der Daten und ihrer Weiterleitung. Ist eine Anmeldung gewünscht? Welche Daten dürfen dabei erhoben werden? An wen dürfen die Anmeldedaten weitergeleitet werden? Was darf der Gruppenleiter alles wissen?



Minderjährigenschutz

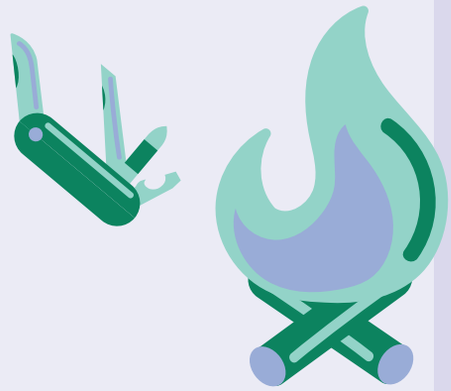
Einwilligung

Wie bei allen anderen Bereichen in der Jugendverbandsarbeit ist auch hier der besondere Schutz der Kinder und Jugendlichen durch in der DSGVO zu beachten. Bis zur Vollendung des 16. Lebensjahres können Kinder und Jugendliche nur bedingt eine Einwilligung in die Verarbeitung der personenbezogenen Daten geben. Neben den Eltern müssen auch Jugendliche ab 16 Jahren einwilligen. Einwilligungen müssen nicht schriftlich erteilt – aber nachgewiesen werden.

1. Veranstaltungen

Für Veranstaltungen gilt allgemein, dass die Betroffenen darauf aufmerksam gemacht werden müssen, welche Daten von ihnen verarbeitet, erhoben und gespeichert werden. Interne (z.B. Vereinsfeiern) und öffentliche Veranstaltungen (z.B. Turniere und Seminare) unterscheiden sich nur hinsichtlich des Umfanges, in dem datenschutzrechtliche Hinweise gegeben werden müssen.

Regelmäßige Gruppenveranstaltungen



Für regelmäßige Gruppentreffen sollten die notwendigen Hinweise (Information, Auskunft, Berichtigung, Löschung, Datenübertragung, Widerspruchsrecht, etc.) bereits beim Vereinsbeitritt oder bei der ersten Anfrage zum Kennenlernen ausgegeben werden. Es sollten Hinweise zum Fotografieren und zum Umgang mit Fotos sowie zu Messenger-Diensten verteilt werden. Eine Herausgabe der Teilnemendenliste an alle Teilnehmenden ist gerechtfertigt, wenn der Vereinszweck darin besteht, persönliche Kontakte zu pflegen. Die Daten sollten sich auf die zur Kontaktaufnahme notwendigen Angaben beschränken. Einzelheiten dazu werden unter dem Stichwort Teilnehmendenliste erläutert (s.u.). Ist die Herausgabe der Kontaktdaten nicht durch den Vereinszweck gerechtfertigt, kann in den Gruppentreffen eine entsprechende Liste erstellt werden. Dabei ist zu beachten, dass bei Minderjährigen die Erziehungsberechtigten darüber zu informieren sind, da ihre Einwilligung erforderlich ist (Minderjährigenschutz). Gruppenleitende und Trainer sollten immer wieder auf ihre Verschwiegenheitspflicht und den sachgemäßen Umgang mit den personenbezogenen Daten hingewiesen werden.

Einmalige Gruppen- und Verbandsveranstaltungen

Bei einmaligen internen Veranstaltungen sind die notwendigen datenschutzrechtlichen Hinweise (Information, Auskunft, Berichtigung, Löschung, Datenübertragung, Widerspruchsrecht, etc.) ebenfalls bereits beim Vereinsbeitritt mitzuteilten. Beim Versand von Einladungen per Mail ist zunächst darauf zu achten, dass sie keine Werbung enthalten. Des Weiteren sind die Mails im Blindmodus (bcc) zu versenden, damit die Empfänger nicht alle Adressaten erkennen können. Im Mail-Programm muss eine Weg-Verschlüsselung (z.B. SSL oder TLS) zum Mail-Server eingerichtet sein, damit die verwendeten Adressen nicht ausgelesen werden können. Bereits die Einladung sollte Hinweise zur eventuellen, weiteren Datenverarbeitungen (zum Umgang mit Fotos, Teilnehmerlisten, etc.) enthalten.

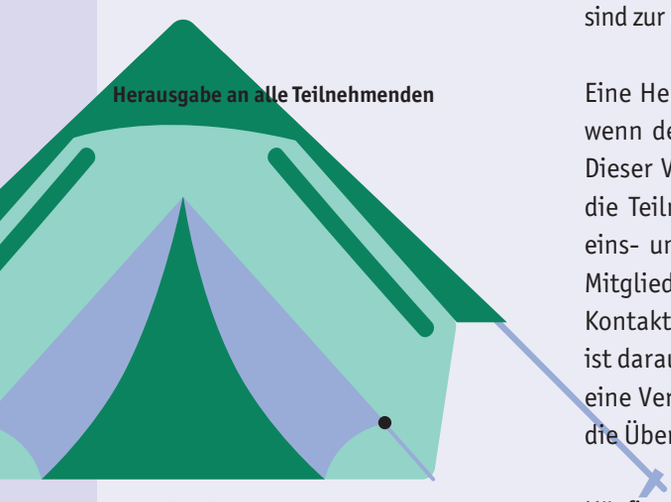
2. Teilnehmerlisten

Wenn Teilnehmerlisten erstellt werden, ist zunächst der Zweck (z.B. für eine interne Statistik, für Verwendungsnachweise oder zur Abrechnung) zu klären. Vom Zweck der Datenerhebung hängt der Umfang der berechtigterweise zu erhebenden Daten ab. Es dürfen grundsätzlich nur jene Daten erhoben werden, die erforderlich sind. Müssen z.B. Listen, die für statistische Zwecke erhoben werden, den vollständigen Namen enthalten? Reicht vielleicht eine Strichliste?

Listen für Jugendleiter

Jugendleitende oder Trainer benötigen für ihre Tätigkeit Angaben zu den Kindern und Jugendlichen ihrer Gruppe. Diese Listen, soweit sie nur die notwendigen Angaben enthalten, sind zur Durchführung der Verbandsarbeit notwendig und dürfen erhoben werden.

Herausgabe an alle Teilnehmenden



Eine Herausgabe der Teilnehmendenliste an alle Teilnehmenden ist gerechtfertigt, wenn der Vereinszweck u.a. darin besteht, die persönlichen Kontakte zu pflegen. Dieser Vereinszweck muss sich aus der Satzung ergeben. Welche Angaben dabei in die Teilnehmendenliste aufgenommen werden dürfen, hängt vom jeweiligen Vereins- und Gruppenzweck ab. Die Interessen und die schutzwürdigen Belange der Mitglieder sind angemessen zu berücksichtigen. Die Daten sollten sich auf die zur Kontaktaufnahme notwendigen Angaben beschränken. Bei der Herausgabe der Liste ist darauf hinzuweisen, dass diese nur für Vereinszwecke verwendet werden darf und eine Verwendung für andere Zwecke (insbesondere für kommerzielle Zwecke) sowie die Überlassung der Liste an außenstehende Dritte nicht zulässig ist.

Liste für Eltern

Häufig werden Elternlisten oder sog. Verteilerlisten gewünscht, die Namen, Adresse sowie Kontaktdaten der anderen Eltern, Kinder und Jugendlichen enthalten. Sieht die Vereinssatzung die Kontaktpflege nicht als Ziel vor, kann entweder ein berechtigtes Interesse vorliegen, oder es wird eine Einwilligung aller Beteiligten benötigt. Die Einwilligung könnte paraktischerweise bereits vorab dadurch erfolgen, dass beim Aufnahmeantrag in den Jugendverband die Möglichkeit gegeben wird, einer derartigen Liste zuzustimmen. Die Aufnahme in den Verein darf jedoch nicht versagt werden, wenn Eltern, Jugendliche oder Kinder dieser Regelung nicht pauschal zustimmen wollen.
Ein weiterer praktischer Weg ist die Auslage von Blankolisten, auf die sich bei einem Elternabend alle Bereitwilligen zum Kontaktaustausch eintragen (Eintragung = Einwilligung zur Bekanntgabe innerhalb des Elternkreises). Ein entsprechender Hinweis, wozu die Angaben verwendet werden, muss auf dem Blankoformular vorhanden sein. Die Listen sind zu löschen, sobald sie nicht mehr benötigt werden. Zu beachten sind ggfs. statistische und nachweisteschnische Verpflichtungen.

Kostenpflichtige Veranstaltungen

Ist eine Veranstaltung kostenpflichtig, oder ist ein Beitrag zu den Materialien zu zahlen? Dann dürfen Listen geführt werden, um nachzuvollziehen, wer bezahlt hat. Auch können Bankdaten erhoben werden, wenn eine Lastschrift geplant ist.

Öffentliche Veranstaltungen

Bei öffentlichen Veranstaltungen sind Hinweise über die persönlichen Rechte (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Widerruf, etc.) und die Datenerhebung sowie -verarbeitung (Weiterleitung der Daten an Dritte? Speicherdauer, etc.) zu geben. Dabei geht es im Wesentlichen um Fotos und Teilnehmerlisten. Die erforderlichen Hinweise sind für jede Form der personenbezogenen Daten zu erteilen. Die Hinweise können als Aushang (z.B. bei Fotos) veröffentlicht oder mit der Veranstaltungseinladung versendet werden.

2. Ferienfreizeiten

Wenn Kinder und Jugendlichen an einer Ferienfreizeit teilnehmen, dürfen ihre Daten

erhoben werden. Die Rechtmäßigkeit der Datenerhebung ergibt sich aus der Teilnahmevereinbarung (Vertrag). Es wird keine daüber hinausgehende Einwilligung zur Datenerhebung benötigt. Gleichwohl sind auf den Anmeldebögen Hinweise über die persönlichen Rechte nach der DSGVO und zur Datenerhebung sowie -verarbeitung zu geben. Des Weiteren ist bei der Datenerhebung wichtig, die Grundsätze der Datenminimierung, der Speicherbegrenzung (Recht auf Löschen) und der Datensicherheit zu beachten.

Berechtigte Abfragen

Diese Angaben der Teilnehmenden dürfen abgefragt werden:

- Name, Geburtstag und Anschrift,
- Datum der (noch) bedeutsamen Tetanusimpfungen,
- Anschrift und Telefonnummer des Hausarztes,
- Name und Anschrift von Eltern mit Notfall-Telefonnummern,
- Name und Geburtstag von Geschwistern, wenn Gebührenfragen davon abhängen,
- chronische Krankheiten, um auf diese angemessen reagieren zu können.

Zu begründende Abfragen

Zusätzliche Angaben der Teilnehmenden dürfen nur mit begründeter Notwendigkeit erhoben werden:

- Krankenkasse der Eltern,
- Staatsangehörigkeit,
- Berufstätigkeit,
- Religion, um auf diese angemessen reagieren zu können.

Daten pseudonymisieren?

Die Daten dürfen an die Jugendleiter und sonstigen Veranstalter weitergegeben werden. Dabei ist zu prüfen, ob die Daten pseudonymisiert werden können. Dem Küchenpersonal reicht z.B. die Information, wie viele allergiefreie Essen zu erstellen sind. Konkrete Namen müssen in diesem Fall nicht weiter gegeben werden.
Alle Daten müssen gelöscht werden, sobald sie nicht mehr benötigt werden. Zu beachten sind Verpflichtungen, die sich aus der Rechenschaftspflicht gegenüber der BASFI ergeben. Es ist zudem zulässig, Kontaktdaten aufzubewahren, um im nächsten Jahr erneut zur Ferienfreizeit einzuladen.

4. Verwendungsnachweise

Abrechnung gegenüber der BASFI

Die BASFI verlangt im Rahmen der Mittelvergabe die Übersendung der Teilnahmebögen. Die Rechtfertigung ergibt sich aus der Haushaltshoheit der Freien und Hansestadt Hamburg. In einer Dienstanweisung ist geregelt, wie die Verwendung der Haushaltsmittel nachzuweisen ist. Die Frage, ob diese Handhabung datenschutzrechlich notwendig ist, sollte dem behördlichen Datenschutzbeauftragten überlassen werden.

5. Hinweis für Zuwendungsempfänger durch die BASFI, Mai 2018

Die BASFI erläutert in einem Hinweis, wie ihrer Meinung nach die Datenschutzregeln zu handhaben sind. Die Darstellung ist sehr verkürzt. Sie lässt die wichtigste Rechtsgrundlage, nämlich den Vertrag durch die Vereinsmitgliederschaft auf Grundlage der Satzung, außer Betracht und bezieht sich nur auf gesetzliche Verpflichtungen oder Einwilligungen. Auf der dritten Seite des Hinweises wird ein Muster für die Verpflichtung von Mitarbeitenden auf die Verschwiegenheit zur Verfügung gestellt. Dieses kann aber muss nicht genutzt werden. Alle Mitarbeitenden, das gilt auch für Ehrenamtliche, sind auf ihre Verschwiegenheit hinzuweisen. Der Hinweis kann mündlich oder schriftlich erfolgen. Wichtig ist die Verpflichtung zu dokumentieren, damit der Verein sie bei Bedarf nachweisen kann. Ansonsten sind die Informationen zum Umgang mit der DSGVO in diesem punktum-Heft wesentlich ausführlicher und hilfreicher als der BASFI-Hinweis.

Hilfen

Rechtsgrundlagen
DSGVO, BDSG: https://dsgvo-gesetz.de/art-1-dsgvo
Gesetzesstexte: www.gesetze-im-internet.de/aktuell.html

(Aufsichts-) Behörden
Bundesamt für den Datenschutz und die Informationsfreiheit: www.bfdi.bund.de
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: https://datenschutz-hamburg.de
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD): www.datenschutzzentrum.de
Bayerisches Landesamt für Datenschutzaufsicht: www.lda.bayern.de

IT-Informationen
Bundesamt für Sicherheit in der Informationstechnik (BSI): www.bsi.bund.de
BSI für Bürger: www.bsi-fuer-buerger.de
Frauenhofer Institut für sichere Informationstechnologie: www.sit.fraunhofer.de
Chaos Computer Club: www.ccc.de
Heise Verlag: www.heise.de

Infos für Erwachsene
www.klicksafe.de
https://mobilsicher.de
Kompetenzzentrum für den Jugendschutz im Internet: www.jugendschutz.net

Infos für Kinder und Jugendliche
www.youngdata.de
www.klicksafe.de

Infoblätter: Verein
https://datenschutz-hamburg.de/dsgvo-information/datenschutz-vereine
https://www.datenschutzzentrum.de/informationsmaterial
https://www.lda.bayern.de/de/faq.html

Infoblätter: Orientierungshilfen
https://www.lda.bayern.de/de/orientierungshilfen.html
https://www.lda.bayern.de/de/kleine-unternehmen.html

Infoblätter: Sozialer Bereich
ULD, Stichwort Bildung: https://www.datenschutzzentrum.de/bildung

Musterverzeichnis für Verarbeitungstätigkeiten
https://www.datenschutzzentrum.de/informationsmaterial
https://www.datenschutzzentrum.de/dsgvo/#vorlagen

Muster: TOM
DSK-Hinweis zur Verarbeitungstätigkeit https://www.datenschutzkonferenz-online.de/anwendungshinweise.html