DATENSCHUTZ

IN DER SÄCHSISCHEN JUGEND- UND JUGENDVERBANDSARBEIT

Eine Handreichung für Haupt- und Ehrenamtliche mit Fallbeispielen, Vorlagen & praktischen Tipps

VORWORT

Seit den umfassenden Neuerungen und Veränderungen durch die Datenschutz-Grundverordnung im Jahre 2018 haben sich viele Arbeitsabläufe und Verwaltungsvorgänge in der Jugend- und Jugendverbandsarbeit optimiert und neu etabliert. Viele Engagierte haben sich fortgebildet und die alltäglichen Prozesse der Verarbeitung von Daten auf den Prüfstand gestellt. Heute steht fest, dass die Verunsicherung, die gerade in den Vereinen und Verbänden spürbar war, einer Routine gewichen ist. Trotzdem führen die Weiterentwicklungen im Bereich des Datenschutzes, neue Rechtsprechung, die stetig zunehmende Sensibilisierung für das Thema und auch die natürlich stattfindende Personalfluktuation dazu, dass der Informations- und Fortbildungsbedarf zum Thema gleichbleibend hoch ist.

Als Dach- und Fachorganisation für die Jugendarbeit Sachsens sowie als Zusammenschluss der sächsischen Jugendverbände und Stadt- und Kreisjugendringe überarbeiteten die AGJF Sachsen e. V. und der Kinder- und Jugendring Sachsen e. V. eine Broschüre des Fachverband Jugendarbeit / Jugendsozialarbeit Brandenburg e. V. und des Landesjugendring Brandenburg e. V. aus dem Jahr 2019, um praxistaugliche Empfehlungen für einen verantwortungsbewussten Umgang mit Daten in der Jugend- und Jugendverbandsarbeit zu ermöglichen. An dieser Stelle sei den Herausgebern für die Zurverfügungstellung der Vorlage herzlich gedankt!

Mit dieser aktualisierten Handreichung soll es gelingen, die Vereine und Verbände in ihrer tagtäglichen Umsetzung des Datenschutzes zu unterstützen und durch übersichtlich aufbereitete Informationen beim Abbau von Hemmschwellen zu helfen. Ergänzend werden unter www.jugend-datenschutz.de passende Vorlagen, Schulungsangebote und aktuelle Informationen rund um das Thema Datenschutz in der Jugend- und Jugendverbandsarbeit angeboten.

Der erste Teil richtet sich besonders an Trägerverantwortliche wie Vorstände bzw. Geschäftsführungen, da der entscheidende Schritt zur Implementierung von Datenschutzprozessen von ihnen ausgeht. Die weiteren Ausführungen im zweiten Teil zu den Datenverarbeitungen in der Jugend- und Jugendverbandsarbeitspraxis sollen den Fachkräften Handlungssicherheit in ständig wiederkehrenden Situationen verleihen. Nicht zuletzt bietet der sensible Umgang mit personenbezogenen Daten im pädagogischen Alltag gute Ansätze für einen Diskurs mit den jungen Menschen zu Themen wie „Privatsphäre“ und „informationelle Selbstbestimmung“.

Die Handreichung kann den notwendigen Zeitaufwand zur Verankerung grundlegender Datenschutzprinzipien bei den Trägen vor Ort nicht mindern. Sie bietet jedoch einen Überblick über relevante Prozesse und Alltagssituationen der Jugend- und Jugendverbandsarbeit, die im Kontext des Datenschutzes von Bedeutung sind. Dabei stellen die Empfehlungen keinesfalls die allein möglichen Vorgehensweisen dar. Jedes Verfahren muss auf die Praktikabilität und die Umsetzbarkeit im eigenen Träger geprüft werden. Aufgrund der rechtlichen Prüfung durch einen Anwalt für Datenschutzrecht, Herrn Robert Harzewski, bietet diese Handreichung jedoch entsprechend der aktuellen Rechtsauffassung wertvolle Vorschläge für den Einsatz in der Jugend- und Jugendverbandsarbeit.

Wir hoffen, dass diese Handreichung eine Bereicherung für die Praxis der Jugend- und Jugendverbandsarbeit darstellt und bei der Arbeit mit Kindern und Jugendlichen im Freistaat Sachsen unterstützen kann.

Wencke Trumpold
Geschäftsführerin
Kinder- und Jugendring Sachsen e. V.

Anke Miebach-Stiens
Geschäftsführerin
Arbeitsgemeinschaft Jugendfreizeitstätten Sachsen e. V.

INHALT

Vorwort ..... S. 02

01

Datenschutz in der Organisation

1.1 Datenschutz ist Aufgabe der Leitung S. 07

1.2 Datenschutz als Top-Down-Strategie ..... S. 08

1.3 Umgang mit Daten von Mitarbeiter*innen ..... S. 08

1.4 Externe Mitarbeiter*innen und Honorarverträge ..... S. 10

02

DSGVO kurz erklärt

2.1 Grundrecht auf Datenschutz ..... S. 12

2.2 Personenbezogene Daten ..... S. 13

2.3 Grundsätze der Datenverarbeitung S. 14

2.3.1 Rechtmäßigkeit ..... S. 15

2.3.2 Zweckbindung ..... S. 15

2.3.3 Datenminimierung ..... S. 15

2.3.4 Richtigkeit ..... S. 16

2.3.5 Speicherbegrenzung ..... S. 16

2.3.6 Integrität und Vertraulichkeit S. 16

2.4 Rechenschaftspflicht ..... S. 16

2.5 Vertrauensschutz, Datenschutz und Schweigepflicht in der Jugend- und Jugendverbandsarbeit ..... S. 17

2.5.1 Schweigepflicht ..... S. 17

2.5.2 Die Einwilligungserklärung .. S. 18

2.5.3 Datenschutz in Abgrenzung zur Schweigepflicht ..... S. 18

2.5.4 Rechtfertigender Notstand und Anzeigepflicht ..... S. 18

2.5.5 Auskunftspflicht ..... S. 19

03

Datenverarbeitung in der Jugend- und Jugendverbands-arbeit

3.1 Teilnehmer*innenverwaltung und Statistik . . . . . S. 20

3.2 Mitgliederverwaltung . . . . . S. 21

3.3 E-Mails . . . . . S. 22

3.4 SMS und Telefon . . . . . S. 23

3.5 Datenspeicher . . . . . S. 24

3.6 Foto, Video, Ton . . . . . S. 25

3.7 WhatsApp und andere Messengerdienste . . . . . S. 27

3.8 Instagram und Facebook . . . . . S. 29

3.9 Website . . . . . S. 30

3.10 Öffentliche Veranstaltungen . . . . . S. 31

3.11 Datenweitergabe an andere Stellen S. 31

Schlagwort-verzeichnis . . . . . S. 44

Impressum . . . . . S. 47

04

Praxissituationen in der Jugend- und Jugendverbands-arbeit

4.1 Beratung . . . . . S. 32

4.2 Bildungsangebote . . . . . S. 33

4.3 Offene Angebote und Freizeitangebote . . . . . S. 34

4.4 Gruppenarbeit . . . . . S. 35

4.5 Netzwerkarbeit und Kommunikation . . . . . S. 35

4.6 Anleitung von Ehrenamt und Teamer*innen . . . . . S. 36

4.7 Antrags- und Abrechnungsverfahren . . . . . S. 37

05

Besondere Aufgaben

5.1 Datenschutzbeauftragte*r . . . . . S. 38

5.2 Verzeichnis von Verarbeitungstätigkeiten . . . . . S. 39

5.3 Auftragsverarbeitungsvertrag . . . . . S. 40

5.4 Technische und organisatorische Maßnahmen . . . . . S. 41

5.5 Verhalten bei Datenschutzpannen . . S. 42

01 DATENSCHUTZ IN DER ORGANISATION

Datenschutz ist innerhalb jeder Einrichtung und Organisation ein wichtiges Thema. Immer wieder kommen Beschäftigte bewusst oder unbewusst mit dem Datenschutz in Berührung. Werden beispielsweise Namen, E-Mail-Adressen oder Fotos gespeichert, gelten gewisse Regeln zum Schutz dieser personenbezogenen Daten. Datenschutzprozesse sollten jedoch niemals isoliert als Einzelfall, sondern aus der Organisationssicht betrachtet werden.

Verantwortliche innerhalb der Organisation

Verantwortlich für die Umsetzung der Datenschutzregeln gemäß der Datenschutz-Grundverordnung (DSGVO) sind die Vereine, Unternehmen oder sonstigen Einrichtungen selbst – und damit deren Vorstand, Geschäftsführung oder Leitung. Gemäß DSGVO gibt es immer eine*n Verantwortliche*n zum Thema Datenschutz:

§ *Art. 4 Abs. 7 DSGVO*
„Verantwortlicher" ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Gemeint ist damit stets die Leitungsebene innerhalb der Organisation. Verantwortliche*r ist der Rechtsträger der Einrichtung, nicht aber einzelne Organisationseinheiten, Tätigkeitsbereiche oder Mitarbeiter*innen. Verantwortliche haben die Pflicht, sich mit den datenschutzrelevanten Vorschriften zu beschäftigen, diese umzusetzen und deren Einhaltung nachzuweisen. Die Nachweispflicht kann dabei nur durch eine entsprechende Dokumentation und ein Datenschutz-Managementsystem erfüllt werden.

Datenschutzdokumentation

In jeder Einrichtung und Organisation sollten Regeln und Prozesse zum Umgang mit personenbezogenen Daten aufgestellt, verschriftlicht und kommuniziert werden. Zum Zweck des Nachweises aber auch der Orientierung der eigenen Mitarbeiter*innen sollte eine umfassende Dokumentation aller datenschutzrechtlichen Aspekte erfolgen. Diese Dokumentation wird gewöhnlich in einem Datenschutzkonzept oder auch Datenschutzhandbuch zusammengefasst.

Zur Dokumentation gehören zum Beispiel:
- das Verzeichnis der Verarbeitungstätigkeiten;
- Dienst-/Betriebsanweisungen und -vereinbarungen zum Umgang mit personenbezogenen Daten und zur Umsetzung von Betroffenenrechten;
- die Dokumentation der Datenschutzorganisation;
- das Löschkonzept;

- das Sicherheitskonzept und der Notfallplan;
- Nachweis der eingeholten Einwilligungen;
- Vereinbarungen mit Auftragsverarbeiter*innen und gemeinsam Verantwortlichen.

Der Inhalt der Dokumentation variiert stark, in Abhängigkeit der Größe und Ausrichtung der eigenen Einrichtung. Die Vorlage gibt eine Übersicht der inhaltlichen Anforderungen an die Dokumentation.

Vorlage 1: Checkliste zur Dokumentation
jugend-datenschutz.de/link/01

Praktisch stellt sich für Beschäftigte die Frage: Welche Rolle habe ich, beispielsweise als Sozialarbeiter*in, und welche Regeln muss ich beachten? Die vorliegende Handreichung soll dazu Hilfestellung geben, Prozesse beschreiben und diese an praktischen Beispielen verdeutlichen. Bei der Verwendung von Mustern und Vorlagen, auf die in dieser Broschüre verwiesen wird, ist es immer empfehlenswert, diese an die spezifischen Voraussetzungen und individuellen Rahmenbedingungen der eigenen Organisation anzupassen.

1.1 DATENSCHUTZ IST AUFGABE DER LEITUNG

Datenschutz ist Leitungsaufgabe und erfordert eine konsequente und sorgfältige Umsetzung vorgeschriebener Prozesse. Dieser zeitliche und organisatorische Aufwand muss der Geschäftsführung oder dem Vorstand bewusst sein oder bewusst gemacht werden. Die erste Information, Schulung und Sensibilisierung der Mitarbeiter*innen zum Thema Datenschutz sollte von dem*der „Verantwortlichen", also von der Geschäftsführung, ausgehen. Hierfür kann es ratsam sein, dass die Verantwortlichen sich zunächst selbst die erforderlichen Kompetenzen zum Thema erarbeiten oder extern verfügbar machen. Wenn nicht mindestens 20 Mitarbeiter*innen (gemeint sind ausdrücklich sowohl hauptamtliche als auch ehrenamtliche Mitarbeiter*innen) Zugriff auf personenbezogene Daten haben, ist die Benennung eines*r Datenschutzbeauftragten in der Regel nicht nötig *(siehe hierzu Kapitel 5.1)*. Dann ist es umso wichtiger, dass die Geschäftsführung oder Vereinsleitung als Verantwortliche*r erste Ansprechperson für die Mitarbeiter*innen ist. Die Gewährleistung einer technisch sicheren Datenverarbeitung ist ebenfalls Aufgabe der Leitung. Hilfreich hierfür ist das Erstellen von IT-Sicherheitsrichtlinien. Die Bereitstellung einer aktuellen IT-Infrastruktur sollte selbstverständlich sein *(siehe hierzu auch Kapitel 5.4)*.

Vorlage 2: Checkliste für Schulungsinhalte
jugend-datenschutz.de/link/02

Umgang mit personenbezogenen Daten auf Weisung

Die Geschäftsführung kann Aufgaben, die den Datenschutz betreffen, an Mitarbeiter*innen übertragen. Aus Beweisgründen und zur Rechtssicherheit ist es empfehlenswert, eine solche Benennung in geeigneter Form zu dokumentieren. Auch externe Dienstleistende dürfen auf Weisung des*der Verantwortlichen mit personenbezogenen Daten umgehen *(siehe Kapitel 5.3)*. Sie werden in der DSGVO als Auftragsverarbeiter*in bezeichnet. Dies kann zum Beispiel das Speichern von personenbezogenen Daten in einer Cloud, die Datenträgerentsorgung durch einen Dienstleister oder den Hosting-Anbieter der Website betreffen.

Vorlage 3: Benennungsurkunde für eigene Mitarbeiter*innen
jugend-datenschutz.de/link/03

Vorlage 4: Checkliste – wann regelmäßig eine Auftragsverarbeitung vorliegt
jugend-datenschutz.de/link/04

Vorlage 5: Verpflichtung zur Vertraulichkeit
jugend-datenschutz.de/link/05

Achtung:
In Art. 29 DSGVO ist geregelt, dass dem*der Verantwortlichen und dem Auftragsverarbeitenden unterstellte Personen nur nach deren Weisung personenbezogene Daten verarbeiten dürfen.

Vorlage 6: Basisschulung für Mitarbeiter*innen als Video zum Abruf
jugend-datenschutz.de/link/06

Beschäftigte müssen daher auf die Einhaltung betrieblicher Weisungen verpflichtet werden. Es wird empfohlen, dies in Form einer schriftlichen oder elektronischen Verpflichtungserklärung umzusetzen. Neben den regulären Mitarbeiter*innen sind auch Praktikant*innen, Auszubildende, Referendar*innen, Leiharbeiter*innen und ehrenamtlich Tätige mit einzubeziehen.

1.2 DATENSCHUTZ ALS TOP-DOWN-STRATEGIE

Alle Mitarbeiter*innen, die mit personenbezogenen Daten umgehen, müssen bei Aufnahme ihrer Beschäftigung von der Geschäftsführung oder Vereinsleitung umfassend zum Thema Datenschutz innerhalb der Organisation informiert werden. Es ist empfehlenswert, Mitarbeiter*innen regelmäßig, bestenfalls jährlich, im Umgang mit personenbezogenen Daten zu schulen und dies zu dokumentieren. So können Arbeitgeber*innen auch nachweisen, dass sie sich bemühen, die DSGVO intern umzusetzen. Verantwortliche haben ihre Mitarbeiter*innen unter anderem auch darüber zu informieren, dass für dienstliche Zwecke keine private Technik wie Smartphones, Laptops oder Kameras genutzt werden darf. Falls das im Einzelfall nötig sein sollte, sind für den Umgang mit personenbezogenen Daten vorher klare Regeln abzustimmen. Gleichzeitig sollte dienstliche Technik nicht für private Zwecke genutzt werden. Beide Bereiche sind klar voneinander zu trennen.

Verlassen Mitarbeiter*innen die Organisation, müssen Verantwortliche sicherstellen, dass gegebenenfalls alle Schlüssel und IT-Geräte zurückgegeben werden. Bestehende Zugangsberechtigungen und Zugriffsrechte müssen angepasst, entzogen oder gelöscht werden. Für neue Mitarbeiter*innen müssen stets neue Zugänge zum System eingerichtet werden. Bestehende Personen- bzw. Userkonten dürfen aus Sicherheitsgründen nicht erneut vergeben werden *(siehe auch Kapitel 5.4)*. Dienstanweisungen haben für Mitarbeiter*innen auch beim Thema DSGVO Vorrang vor dieser Handreichung. Sie kann nur eine Hilfestellung und Orientierung bieten.

1.3 UMGANG MIT DATEN VON MITARBEITER*INNEN

Arbeitgeber*innen müssen beim Umgang mit den Daten ihrer Mitarbeiter*innen ebenfalls die Regelungen der DSGVO beachten. So dürfen personenbezogene Daten von Beschäftigten zum Beispiel nur verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

Veröffentlichung im Internet

Die Veröffentlichung von Daten der Mitarbeiter*innen, zum Beispiel auf der Website einer Organisation, muss kritisch überprüft werden. Ist eine Veröffentlichung von Basiskommunikationsdaten wie Name, Funktion in der Organisation, dienstliche Adresse, dienstliche Telefonnummer und

dienstliche E-Mail-Adresse im Rahmen der Zweckbestimmung und zur Durchführung des Beschäftigungsverhältnisses notwendig, dann kann das bei Funktionsträger*innen ohne schriftliche Einwilligung erfolgen. So ist zum Beispiel auch die Veröffentlichung von Daten der Geschäftsführung im Impressum gemäß § 5 Digitale-Dienste-Gesetz (DDG) zwingend erforderlich. Handelt es sich nicht um Funktionsträger*innen bzw. ist die Veröffentlichung von zusätzlichen Daten wie dem Foto, dem Geburtsdatum oder dem Berufsabschluss beabsichtigt, ist vorab die schriftliche oder elektronische Einwilligung des*der Beschäftigten einzuholen.

Fotos dürfen grundsätzlich nur mit Einwilligung des*der Abgebildeten veröffentlicht werden. Damit die Einwilligung wirksam ist, muss sie vor der Aufnahme und ihrer Veröffentlichung eingeholt werden. Mit Widerruf einer Einwilligung dürfen Bilder der Beschäftigten grundsätzlich nicht weiterverarbeitet werden. Sie sind daher nach Widerruf zu löschen bzw. zu retuschieren.

Achtung:
Eine Einwilligung zur Veröffentlichung von personenbezogenen Daten muss immer freiwillig erfolgen. Den Beschäftigten dürfen auch bei Verweigerung keine Nachteile entstehen.

Vorlage 7: Einwilligung Fotonutzung für Beschäftigte
jugend-datenschutz.de/link/07

Vorlage eines erweiterten Führungszeugnisses nach § 72a Sozialgesetzbuch Achtes Buch (SGB VIII)

Zum Zweck des Kinder- und Jugendschutzes wurde 2010 das erweiterte Führungszeugnis eingeführt. Dieses kann nach § 30a Bundeszentralregistergesetz (BZRG) über Personen erteilt werden, die beruflich, ehrenamtlich oder in sonstiger Weise kinder- oder jugendnah tätig sind oder tätig werden wollen. Hauptanwendungsfall des § 30a BZRG ist nach der Intention des Gesetzgebers die Vorlagepflicht nach § 72a SGB VIII für Beschäftigte bei öffentlichen und freien Trägern der Jugendhilfe.

§ 72a SGB VIII Abs. 1 und 2

Die **Träger der öffentlichen Jugendhilfe** dürfen für die Wahrnehmung der Aufgaben in der Kinder- und Jugendhilfe keine Person beschäftigen oder vermitteln, die rechtskräftig wegen einer Straftat nach den §§ 171, 174 bis 174c, 176 bis 180a, 181a, 182 bis 184g, 184i, 184j, 184k, 184l, 201a Abs. 3, den §§ 225, 232 bis 233a, 234, 235 oder 236 verurteilt worden ist. Zu diesem Zweck sollen sie sich bei der Einstellung oder Vermittlung und in regelmäßigen Abständen von den betroffenen Personen ein Führungszeugnis nach § 30 Abs. 5 und § 30a Abs. 1 des Bundeszentralregistergesetzes vorlegen lassen. Die Träger der öffentlichen Jugendhilfe sollen durch Vereinbarungen mit den **Trägern der freien Jugendhilfe** sowie mit Vereinen im Sinne des § 54 sicherstellen, dass diese keine Person, die wegen einer Straftat nach Abs. 1 Satz 1 rechtskräftig verurteilt worden ist, hauptamtlich beschäftigen.

§ 72a SGB VIII
jugend-datenschutz.de/link/sgb8-72a

§ 30a BZRG
jugend-datenschutz.de/link/bzrg-30a

Archivierung nicht erlaubt

Dem*der Arbeitgeber*in ist es nicht erlaubt, das Führungszeugnis selbst zu archivieren. Gemäß § 72a SGB VIII Abs. 5 dürfen von den eingesehenen Daten überhaupt nur folgende Daten erhoben werden:

- der Umstand, dass Einsicht in ein Führungszeugnis genommen wurde;
- das Datum des Führungszeugnisses;
- die Information, ob die das Führungszeugnis betreffende Person wegen einer relevanten Straftat rechtskräftig verurteilt worden ist.

Die Träger der öffentlichen und freien Jugendhilfe dürfen die erhobenen Daten nur speichern, verändern und nutzen, soweit dies erforderlich ist, um die betroffene Person von der Tätigkeit, die Anlass zu der Einsichtnahme in das Führungszeugnis gewesen ist, auszuschließen. Die Daten sind unverzüglich zu löschen, wenn im Anschluss an die Einsichtnahme keine Tätigkeit wahrgenommen wird. Andernfalls sind die Daten spätestens sechs Monate nach der Beendigung einer solchen Tätigkeit zu löschen.

1.4 EXTERNE MITARBEITER*INNEN UND HONORARVERTRÄGE

Die Einbindung externer Mitarbeiter*innen mit Honorarverträgen stellt Organisationen und Vereine hinsichtlich des Datenschutzes regelmäßig vor eine Herausforderung. Neben den hauptberuflichen Mitarbeiter*innen müssen auch Honorarkräfte und ehrenamtlich Tätige, die Zugang zu personenbezogenen Daten haben und diese gegebenenfalls verarbeiten, zur Vertraulichkeit verpflichtet werden. Dies kann in Form einer Vertraulichkeitserklärung als Anhang zum Honorarvertrag bzw. zur Ehrenamtsvereinbarung gemacht werden *(siehe auch Kapitel 4.7)*. Auch externe Mitarbeiter*innen müssen die Grundsätze der Datenverarbeitung *(siehe hierzu Kapitel 2.3)* beachten und dürfen personenbezogene Daten nur zu dem Zweck verarbeiten, zu dem sie ursprünglich erhoben wurden, beispielsweise für die Organisation einer Ferienfreizeit. Außerdem müssen sie die Daten löschen, wenn der Zweck oder die rechtliche Grundlage nicht mehr besteht. Ebenso besteht eine Löschpflicht, wenn die betroffene Person es fordert, sofern gesetzliche Vorschriften dem nicht entgegenstehen. Genau wie bei hauptamtlichen Mitarbeiter*innen müssen Arbeitgeber*innen beim Umgang mit den Daten ihrer ehrenamtlich Tätigen und Honorarkräfte die Regelungen der DSGVO beachten.

Vorlage 8: Datenschutzverpflichtung für ehrenamtlich Tätige und Honorarkräfte
jugend-datenschutz.de/link/08

DSGVO KURZ ERKLÄRT

02

Die DSGVO gilt seit dem 25. Mai 2018 in der gesamten Europäischen Union (EU) und dem Europäischen Wirtschaftsraum (EWR). Sie schließt aber auch Unternehmen, die nicht in der EU niedergelassen sind, in den Anwendungsbereich ein, wenn diese zum Beispiel in der EU Waren oder Dienstleistungen anbieten. Das Gesetz regelt in elf Kapiteln die Verarbeitung von personenbezogenen Daten.

Neben den 99 Artikeln sind 173 Erwägungsgründe angeführt, die zur Auslegung der Artikel mit herangezogen werden. Erwägungsgründe sind Ziele, die mit der Formulierung der Artikel der EU-Verordnung verfolgt werden. Sie sind nicht die eigentlichen Rechtsnormen, aber sie sind hilfreich für deren Interpretation.

DSGVO
jugend-datenschutz.de/link/dsgvo

Die DSGVO geht uns alle an

Betroffen von der DSGVO sind alle, die beruflich Daten verarbeiten oder im Internet unterwegs sind: Arbeitnehmer*innen genauso wie Vereine, Organisationen und Einrichtungen, Website-Betreiber*innen, soziale Netzwerke, App-Anbieter*innen und Unternehmen.

Die Größe des Unternehmens oder Vereins ist grundsätzlich unbeachtlich, so dass die Anforderungen aus der DSGVO sowie die begleitenden datenschutzrechtlichen Regelungen (zum Beispiel aus dem Bundesdatenschutzgesetz) sowohl einen kleinen Verein mit nur einer hauptamtlichen Stelle als auch eine Aktiengesellschaft mit zum Beispiel 10.000 Beschäftigten gleichermaßen betreffen.

Für Einrichtungen mit Zugehörigkeit zu Kirchen oder religiösen Vereinigungen und Gemeinschaften gilt eine Ausnahme. Sie können wegen des verfassungsrechtlich garantierten Selbstbestimmungsrechts von Religionsgemeinschaften eigene Datenschutzregeln erlassen, wenn diese im Einklang mit der DSGVO stehen. Für evangelische Einrichtungen gilt das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD). Katholische Einrichtungen müssen das Kirchliche Datenschutzgesetz (KDG) beachten. Religionsgemeinschaften haben übrigens auch eigene kirchliche Datenschutzbeauftragte.

DSG-EKD
jugend-datenschutz.de/link/ekd

KDG
jugend-datenschutz.de/link/kdg

2.1 GRUNDRECHT AUF DATENSCHUTZ

Die DSGVO sichert das Grundrecht aller Personen auf Datenschutz, wie es in der Grundrechtecharta der Europäischen Union (EU) verankert ist. Mit der DSGVO wurden die bis dato in der EU geltenden unterschiedlichen Datenschutzniveaus vereinheitlicht. Die DSGVO setzt sogar globale Standards, die zum Beispiel Plattformen wie Google, Amazon und Facebook dazu bringen, diese Standards bei der Verarbeitung der Daten ihrer Nutzer*innen anzuwenden, denn sie gilt auch für ausländische Unternehmen, die innerhalb der EU tätig sind.

Achtung:
Bei Verletzung der Vorgaben der DSGVO können Strafen von bis zu 20 Millionen Euro oder vier Prozent des Jahresumsatzes verhängt werden.

Achtung: Auslegungsspielraum!

An einigen Stellen gibt es in der DSGVO noch Auslegungsspielraum, weil die Formulierungen allgemein und eher technikoffen gehalten sind. Diese werden aber zunehmend durch Gerichtsurteile ausgeräumt. Die Aufsichtsbehörden veröffentlichen zudem untereinander abgestimmte Auslegungshilfen in Form von Kurzpapieren und Orientierungshilfen.

Vorlage 9: Übersicht relevanter Kurzpapiere und Orientierungshilfen
jugend-datenschutz.de/link/09

Auskünfte erteilen und „Recht auf Vergessenwerden“

Als Verantwortliche*r für die Verarbeitung personenbezogener Daten ist es wichtig, dass man Auskunft darüber geben kann, welche Daten über welche Person gespeichert sind und an wen sie gegebenenfalls weitergegeben wurden. Außerdem haben Betroffene ein „Recht auf Vergessenwerden“ (Art. 17 DSGVO) und können verlangen, dass die von ihnen gespeicherten Daten unverzüglich gelöscht werden – sofern dem keine öffentlichen Interessen oder rechtlichen Verpflichtungen (zum Beispiel die aktuell sechsjährige Aufbewahrungspflicht bei Lohnkonten) entgegenstehen.

Vorlage 10: Auskunft gemäß Art. 15 DSGVO
jugend-datenschutz.de/link/10

Erwägungsgrund 65 DSGVO
Dieses „Recht auf Vergessenwerden“ ist insbesondere wichtig in Fällen, in denen die betroffene Person ihre Einwilligung noch im Kindesalter gegeben hat und insofern die mit der Verarbeitung verbundenen Gefahren nicht in vollem Umfang absehen konnte und die personenbezogenen Daten – insbesondere die im Internet gespeicherten – später löschen möchte.

2.2 PERSONENBEZOGENE DATEN

Personenbezogene Daten sind nach Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Personenbezogene Daten können, je nach Kontext der damit in Zusammenhang stehenden Daten, sein:

Die DSGVO nennt zudem in Art. 9 besondere Kategorien personenbezogener Daten, die früher sogenannten **sensiblen Daten**, die besonders geschützt werden müssen:

§ *Erwägungsgrund 51 DSGVO*

Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können.

Daten von Kindern und Jugendlichen

Für den Umgang mit Daten von Kindern und Jugendlichen gilt ebenso besondere Sensibilität:

§ *Erwägungsgrund 38 DSGVO*

Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind. Ein solcher besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen. Die Einwilligung des Trägers der elterlichen Verantwortung sollte im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein.

2.3 GRUNDSÄTZE DER DATENVERARBEITUNG

Für die Verarbeitung personenbezogener Daten sieht die DSGVO in Art. 5 Abs. 1 sechs Grundsätze vor, die beachtet werden müssen. Sie werden im Folgenden aufgeführt und erklärt. Dabei spielt es keine Rolle, ob die Daten digital oder in einer strukturierten Papierform verarbeitet werden.

§ *Art. 4 DSGVO*

Im Sinne der DSGVO bezeichnet der Ausdruck „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang 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.

Jede Person, die Daten verarbeitet, muss die Grundsätze aus Art. 5 Abs. 1 DSGVO nicht nur einhalten, sondern auch nachweisen können, dass die Grundsätze eingehalten wurden. Diese sogenannte Rechenschaftspflicht wird in *Kapitel 2.4* genauer beschrieben und kann zum Teil durch das Verzeichnis von Verarbeitungstätigkeiten gewährleistet werden. In *Kapitel 5.2* gibt es weitere Informationen und praktische Hinweise dazu.

2.3.1 RECHTMÄSSIGKEIT

Personenbezogene Daten müssen immer auf rechtmäßige Weise, nach bestem Wissen und Gewissen und in einer für die betroffene Person transparenten, klaren und verständlichen Weise verarbeitet werden.

In Art. 6 DSGVO wird näher auf den Begriff der Rechtmäßigkeit eingegangen. So ist eine Datenverarbeitung dann rechtmäßig, wenn eines der folgenden Kriterien erfüllt ist:

- Personenbezogene Daten dürfen für die Begründung und Durchführung eines Vertrags, aber auch zur Verfolgung des Vertragszweckes und -zieles verarbeitet werden. Zur **Verarbeitung für die Erfüllung vertraglicher Zwecke** zählen Arbeitsverträge, Vereinsmitgliedschaften oder auch Vereinbarungen mit Jugendlichen (zum Beispiel die Anerkennung der Hausordnung im Jugendclub).
- **Erfüllung rechtlicher Pflichten:** Das betrifft zum Beispiel die derzeit sechsjährige Aufbewahrungspflicht von Lohnkonten und die Verarbeitung von Krankenstandsdaten der Mitarbeiter*innen.
- **Schutz lebenswichtiger Interessen** der betroffenen Person oder einer anderen natürlichen Person;
- **öffentliches Interesse** oder Ausübung öffentlicher Gewalt;
- **Wahrung berechtigter Interessen:** 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. Ein solches Überwiegen ist insbesondere immer dann anzunehmen, wenn es sich bei der betroffenen Person um ein Kind handelt.

Wenn keines der oben genannten Kriterien zutrifft – insbesondere keine berechtigten Interessen oder die Erfüllung vertraglicher Pflichten – so muss für eine rechtmäßige Verarbeitung eine **Einwilligung der betroffenen Person** eingeholt werden. Im Idealfall erfolgt diese Einwilligung schriftlich und wird dokumentiert.

Achtung:
Datenverarbeitung ist grundsätzlich verboten, es sei denn, sie ist aufgrund einer Rechtsgrundlage erlaubt.

2.3.2 ZWECKBINDUNG

Ein weiterer Grundsatz ist die sogenannte Zweckbindung. Das bedeutet, dass Daten immer nur für vorab festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen. Eine Weiterverarbeitung ist nur möglich, wenn sie mit den Erhebungszwecken zu vereinbaren ist oder die betroffene Person einverstanden ist.

2.3.3 DATENMINIMIERUNG

Der Grundsatz der Datenminimierung besagt, dass nicht mehr Daten erhoben und verarbeitet werden dürfen, als es für den Zweck angemessen ist. Der Verantwortliche hat daher bei jedem Datenverarbeitungsprozess zu prüfen, ob sich der Umfang der jeweils verarbeiteten personenbezogenen Daten minimieren lässt.

2.3.4 RICHTIGKEIT

Alle erhobenen Daten müssen sachlich richtig und auf dem neuesten Stand sein. Außerdem müssen angemessene Maßnahmen getroffen werden, um personenbezogene Daten unverzüglich löschen oder berichtigen zu können, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind.

2.3.5 SPEICHERBEGRENZUNG

Im Sinne der Speicherbegrenzung dürfen Daten nur so lange gespeichert und verarbeitet werden, wie es für den Zweck notwendig ist. Wenn rechtliche Pflichten erfüllt werden müssen *(siehe hierzu Kapitel 2.3.1)*, ist die entsprechende gesetzliche Aufbewahrungsfrist grundlegend.

2.3.6 INTEGRITÄT UND VERTRAULICHKEIT

Personenbezogene Daten müssen vor unberechtigtem Zugang geschützt werden. Sie müssen also immer in einer Weise aufbewahrt und verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Das schließt den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung ein. Hierzu müssen geeignete technische und organisatorische Maßnahmen *(siehe hierzu auch Kapitel 5.4)* getroffen werden.

2.4 RECHENSCHAFTSPFLICHT

Gemäß der DSGVO sind diejenigen, die personenbezogene Daten erheben und verarbeiten, dafür verantwortlich, dass die in *Kapitel 2.3* vorgestellten Grundsätze eingehalten werden. Sie müssen im Zweifel deren Einhaltung nachweisen können. Die sogenannte Rechenschaftspflicht bedeutet in der Praxis vor allem, dass man auf Nachfrage der Aufsichtsbehörde belegen kann, die DSGVO-Vorgaben erfüllt zu haben.

In *Kapitel 5.2* gibt es weitere Informationen zum hierfür hilfreichen Verzeichnis von Verarbeitungstätigkeiten.

Daneben sollte auch an das Aufstellen einer Leitlinie zum Datenschutz und von Datenschutzrichtlinien, die Festlegung von Zugangsbeschränkungen zu personenbezogenen Daten, Dienstanweisungen und die Datenschutzunterweisungen und -verpflichtungen von Mitgliedern bzw. Beschäftigten gedacht werden.

Vorlage 1: Checkliste zur Dokumentation
jugend-datenschutz.de/link/01

Praxistipp:
Die Aufsichtsbehörde wird genau bezeichnen, welche Vorgänge sie vorgelegt bekommen möchte. Ihr sollte dann auch nur dieser Einzelfall, aber nicht die gesamte DSGVO-Dokumentation, vorgelegt werden.

2.5 VERTRAUENSSCHUTZ, DATENSCHUTZ UND SCHWEIGEPFLICHT IN DER JUGEND- UND JUGENDVERBANDSARBEIT

In der Jugend- und Jugendverbandsarbeit spielt das Vertrauensverhältnis von Kindern bzw. Jugendlichen zu Fachkräften eine besondere Rolle. Sozialarbeiter*innen und Betreuer*innen erhalten mitunter Informationen, die aus Sicht der jungen Menschen nicht für weitere Personen bestimmt sind. Manchmal ist es jedoch für eine Fachkraft wichtig, Informationen weitergeben zu können, um sich im Team über einen Fall auszutauschen oder eine zweite Meinung einholen zu können. Insbesondere, wenn es um den Verdacht der Kindeswohlgefährdung gemäß § 8a SGB VIII geht. Hier kommt der Begriff des Vertrauensschutzes ins Spiel, der mehr abdeckt als den Schutz personenbezogener Daten.

Vertrauensschutz setzt sich aus vier Bereichen zusammen, die im Folgenden kurz vorgestellt werden:

Datenschutz:

Weitergabe von personenbezogenen Daten

Schweigepflicht:

Weitergabe von anvertrauten Geheimnissen

Zeugnisverweigerungsrecht:

Aussagen vor Gericht

Anzeigepflicht:

Anzeige von Straftaten

2.5.1 SCHWEIGEPFLICHT

Die Schweigepflicht ist eine rechtliche Verpflichtung, bestimmte Informationen, die im Rahmen beruflicher oder dienstlicher Tätigkeit bekannt werden, vertraulich zu behandeln und nicht unbefugt an Dritte weiterzugeben. In § 203 Strafgesetzbuch (StGB) findet sich eine Aufzählung von Berufsgruppen, deren Angehörige bei Verletzung der Schweigepflicht strafrechtlich verfolgt werden können. Auch in Arbeitsverträgen gibt es häufig einen Passus zur Schweigepflicht. Erzählt man Geheimnisse anderer dennoch unbefugt weiter, drohen dann auch arbeitsrechtliche Konsequenzen.

Erlaubte Weitergabe von Geheimnissen

Die Weitergabe von anonymisierten Geheimnissen, ohne Bezug zu einer bestimmten Person, ist erlaubt. Dies kann zum Beispiel im Rahmen einer Teambesprechung und zum Austausch mit anderen Fachkräften hilfreich sein. Für eine wirksame Anonymisierung wird gefordert, dass niemand in

der Lage sein darf, einen Rückschluss auf eine Person zu ziehen. Gerade in kleinen Einrichtungen kann jedoch ein vermeintlich anonymer Datenbestand zu einer betroffenen Person führen.

Ohne eine explizite Einwilligung (Schweigepflichtentbindung) der betroffenen Person oder ihrer gesetzlichen Vertretung dürfen dann grundsätzlich keine Daten offenbart werden.

2.5.2 DIE EINWILLIGUNGSERKLÄRUNG

Durch eine Einwilligungserklärung kann die Erlaubnis zur Weitergabe von Geheimnissen erteilt werden. Diese Einwilligung kann mündlich, schriftlich oder durch schlüssiges Handeln erfolgen, wobei es empfehlenswert ist, die Schweigepflichtentbindung zu dokumentieren.

Bei Kindern und Jugendlichen ist kein bestimmtes Alter zu beachten. Ausschlaggebend ist, dass sie einwilligungsfähig sind, also die Bedeutung und Tragweite ihrer Erklärung verstehen können. Das muss immer im Einzelfall beurteilt werden. Im Zweifel sollten die Personensorgeberechtigten einwilligen.

Eine Schweigepflichtentbindung sollte möglichst konkret sein und mindestens folgende Inhalte erfassen: Wer erteilt sie wem, zu welchem Zweck und wem darf das Geheimnis anvertraut werden? Eine zu allgemein formulierte Schweigepflichtentbindung (zum Beispiel: unklarer Zweck oder unüberschaubarer Adressatenkreis) kann die Gültigkeit aufheben.

Praxistipp:
Wenn Kinder und Jugendliche einwilligungsfähig sind, tritt die Personensorge zurück. Es empfiehlt sich, zu dokumentieren, wieso man als Fachkraft zu der Einschätzung gekommen ist, dass der betroffene junge Mensch einwilligungsfähig ist.

Vorlage 11: Schweigepflichtentbindung
jugend-datenschutz.de/link/11

2.5.3 DATENSCHUTZ IN ABGRENZUNG ZUR SCHWEIGEPFLICHT

Datenschutz richtet sich zuerst an den Verein, Träger bzw. die Einrichtung und verpflichtet diese*n sicherzustellen, dass Unbefugte keinen Einblick in dort erhobene Daten haben. Datenschutz wird als Sammelbegriff für verschiedene Rechtsquellen, die das Recht auf informationelle Selbstbestimmung sicherstellen, verwendet. Dazu zählen neben der DSGVO unter anderem das Bundesdatenschutzgesetz (BDSG) und das Sächsische Datenschutzdurchführungsgesetz (SächsDSDG). Während sich die Schweigepflicht auf anvertraute Geheimnisse bezieht, handelt es sich beim Datenschutz um personenbezogene Daten.

2.5.4 RECHTFERTIGENDER NOTSTAND UND ANZEIGEPFLICHT

Im Falle der Gefahrenabwehr kann nach sorgfältiger Interessensabwägung eine Datenübermittlung an andere Stellen ohne Einwilligung der betroffenen Person zulässig sein (§ 34 StGB – Rechtfertigender Notstand).

§ 34 Strafgesetzbuch (StGB)

Wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, handelt nicht rechtswidrig, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Dies gilt jedoch nur, soweit die Tat ein angemessenes Mittel ist, die Gefahr abzuwenden.

§ 34 StGB sieht also vor, dass eine Gefahr tatsächlich und unabwendbar bevorsteht, die nicht anders abgewendet werden kann. Die Maßstäbe werden sehr streng angelegt, sodass eine Schweigepflichtverletzung in der praktischen Jugend- und Jugendverbandsarbeit eher selten mit dem rechtfertigenden Notstand begründet werden kann.

Nach § 138 StGB müssen bestimmte, dort aufgeführte Straftaten wie Mord, Hoch- und Landesverrat und Raub angezeigt werden, wenn man Kenntnis von ihnen erlangt. Berufsgeheimnisträger*innen können sich daher strafbar machen, wenn sie Kenntnis von einem solchen Verbrechen erlangen und dies nicht rechtzeitig der Polizei melden.

2.5.5 AUSKUNFTSPFLICHT

Personensorgeberechtigte haben bei Kindern und Jugendlichen grundsätzlich ein sogenanntes Auskunftsrecht. Gleichzeitig gilt die Schweigepflicht nach § 203 Strafgesetzbuch (StGB) auch für Geheimnisse von Kindern und Jugendlichen im Verhältnis zu ihren Personensorgeberechtigten. Dieses Spannungsverhältnis gilt es im Einzelfall auszuloten.

So sind Fälle denkbar, in denen eine Information über die von Kindern und Jugendlichen einer Fachkraft anvertrauten Probleme bei den Personensorgeberechtigten zu Reaktionen führen würden, die aus pädagogischen Gründen nicht verantwortet werden können. Die Fachkraft würde durch die Informationsweitergabe eine Ursache dafür setzen, dass ihre eigenen Bemühungen im Interesse des Kindeswohls keinen oder einen geringeren Erfolg haben. Zudem würde das Vertrauensverhältnis gestört. Zu bedenken sind weitere Umstände wie Alter, Reife und Stabilität des betroffenen jungen Menschen, seine familiären und sonstigen persönlichen Beziehungen, die Art und die Intensität des speziellen Problems. Auch die Art und Weise, mit der die Familie auf ihr Kind allgemein eingeht und vermutlich nach Information über die spezielle Problematik eingehen wird, ist von Bedeutung. In solch einem Fall kann möglicherweise, nach gewissenhafter Abwägung aller Faktoren, keine Auskunftspflicht gegenüber den Personensorgeberechtigen bestehen.

Gemäß § 34 Abs. 1 in Verbindung mit § 29 Abs. 1 Satz 2 BDSG besteht das Recht auf Auskunft nicht, wenn durch die Auskunft Informationen offenbart würden, die aufgrund einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen überwiegender berechtigter Interessen eines Dritten, geheim gehalten werden müssen. Dies kann dazu führen, dass das Auskunftsrecht der Personensorgeberechtigten zum Schutz des Kindes oder Jugendlichen zurücktreten muss.

03 DATENVERARBEITUNG IN DER JUGEND- UND JUGENDVERBANDSARBEIT

Zwischen Jugend- bzw. Jugendverbandsarbeit und Datenschutz gibt es viele Berührungspunkte. Aufgrund der einzuhaltenden Regelungen der DSGVO sind zahlreiche Maßnahmen zu treffen. Im folgenden Kapitel werden einige für die Jugend- und Jugendverbandsarbeit typische Prozesse dargestellt und dazu praktische Hinweise zum jeweiligen Umgang mit den personenbezogenen Daten geliefert.

3.1 TEILNEHMER*INNENVERWALTUNG UND STATISTIK

In der Jugend- und Jugendverbandsarbeit stehen Anmeldeformulare, das Führen von Teilnahmelisten und deren Archivierung zu Verwendungsnachweis- und Statistikzwecken auf der Tagesordnung.

Informationspflicht

Werden personenbezogene Daten erhoben und verarbeitet, so muss das gemäß Art. 13 und Art. 14 DSGVO so transparent wie möglich für die betroffenen Personen geschehen. Die Informationspflicht ist zum Beispiel gegenüber Teilnehmer*innen, Beschäftigten *(siehe hierzu Kapitel 1.3)* und Mitgliedern *(siehe hierzu das folgende Kapitel 3.2)* zu erfüllen.

Über folgende Punkte müssen die Betroffenen unter anderem aufgeklärt werden:

- den Namen und die Kontaktdaten des*der Verantwortlichen, gegebenenfalls auch des*der Datenschutzbeauftragten;
- die Zwecke und die Rechtsgrundlage für die Verarbeitung;
- die berechtigten Interessen (gemäß Art. 6 Abs. 1 f DSGVO, sofern die Verarbeitung darauf beruht);
- gegebenenfalls die Empfänger*innen oder Kategorien von Empfänger*innen der personenbezogenen Daten (zum Beispiel Dachverbände, Kooperationspartner*innen, Fördergeldgeber*innen, Unterkünfte oder Versicherungen, *siehe hierzu Kapitel 3.11*);
- gegebenenfalls die Absicht, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln;
- die Speicherdauer der Daten oder zumindest die Kriterien für die Festlegung dieser Dauer;
- Informationen zu den Rechten der Betroffenen (das Recht auf Auskunft, Berichtigung, Löschung, das Widerspruchsrecht sowie das Recht auf Datenübertragbarkeit und Einschränkung der Verarbeitung gemäß Art. 18 DSGVO);
- jederzeitiges Widerrufsrecht der Einwilligung (wenn die Verarbeitung auf Art. 6 Abs. 1 a oder Art. 9 Abs. 2 a DSGVO beruht);

- Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde;
- Hinweis, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen und welche möglichen Folgen die Nichtbereitstellung hätte.

Diese Informationspflicht muss bei der Erhebung und Verarbeitung von personenbezogenen Daten, die ja immer nur zweckgebunden erfolgen darf, erfüllt werden. Deshalb empfiehlt es sich, diese Informationen stets vollständig auf entsprechende Formulare, wie Anmeldeformulare oder Teilnahmelisten, abzudrucken.

Angaben zu sensiblen Daten wie Religionszugehörigkeit, Allergien, Krankheiten oder Behinderungen sind manchmal wichtig, um zum Beispiel eine Jugendferienfreizeit entsprechend aller Bedürfnisse gut vorbereiten zu können. Solche Angaben sollten jedoch niemals Pflichtangaben sein, sondern freiwillig (auf Basis einer Einwilligung) erfolgen. Weiterhin dürfen stets nur so wenige Daten wie möglich abgefragt werden und diese müssen gewissenhaft, nach der Erfüllung des Zweckes, wieder gelöscht werden.

Sämtliche personenbezogenen Daten müssen geschützt vor dem Zugriff Unbefugter aufbewahrt sein. In der Praxis bedeutet das, dass zum Beispiel Anmeldelisten nicht frei zugänglich herumliegen dürfen, sondern von der verantwortlichen Person sicher aufbewahrt werden müssen. Dabei ist es egal, ob es sich um lose Blätter oder um Dateien auf dem Computer handelt *(siehe hierzu auch Kapitel 5.4)*.

Vorlage 12: Datenschutzhinweise
jugend-datenschutz.de/link/12

Übrigens:
Beabsichtigt ein*e Verantwortliche*r die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so muss er*sie den betroffenen Personen vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Art. 13 Abs. 2 DSGVO zur Verfügung stellen.

Tipp:
Das Erfassen von statistischen Daten kann unter Umständen anonym erfolgen. Dann finden die Vorschriften der DSGVO keine Anwendung.

3.2 MITGLIEDERVERWALTUNG

Zur Struktur eines Vereins gehören Mitglieder. Eine Vereinsmitgliedschaft ist, ähnlich wie ein Arbeitsverhältnis, vertraglich begründet. Gemäß Art. 6 Abs. 1 b DSGVO dürfen diejenigen Daten erhoben, verarbeitet und gespeichert werden, die für die Begründung und Durchführung des Vertrags erforderlich sind. Entsprechende Vereinsziele müssen dokumentiert sein. So erlaubt ein gültiger Mitgliedschaftsvertrag in Verbindung mit der gültigen Vereinssatzung die Verarbeitung der personenbezogenen Daten der Mitglieder zu den so dokumentierten Vereinszwecken. Vereine haben dennoch auch gegenüber ihren Mitgliedern Informationspflichten und müssen diese über Datenverarbeitungsvorgänge informieren *(siehe hierzu Kapitel 3.1)*. So sollte man im Rahmen der Mitgliedsverträge und Antragsformulare dieser Informationspflicht nachkommen. Bei Vereinsmitgliedschaften ist beim Umgang mit den personenbezogenen Daten zu beachten, dass solch eine Mitgliedschaft meistens auf unbestimmte oder gar unbegrenzte Zeit geschlossen wird. Zugriff auf die Daten der Mitglieder, zum Beispiel auf das Mitgliederverzeichnis, dürfen nur autorisierte Personen haben und auch bei diesen Daten müssen geeignete technische und organisatorische Maßnahmen zu ihrem Schutz getroffen werden *(siehe hierzu Kapitel 5.4)*.

Das „Recht auf Vergessenwerden“ *(siehe Kapitel 2.1)* trifft auch auf Vereinsmitglieder zu, weshalb nach dem Ende einer Mitgliedschaft alle personenbezogenen Daten gelöscht werden müssen, wenn keine anderen rechtlichen Gründe dagegensprechen. Eventuelle Auftragsverarbeiter*innen und gegebenenfalls auch der Dachverband müssen informiert werden, damit auch sie die Daten löschen.

3.3 E-MAILS

Zur Kommunikation werden häufig E-Mails eingesetzt. Ohne Verschlüsselung wird eine E-Mail in Klartext versendet. Ähnlich wie eine Postkarte kann diese von jedem gelesen werden, der Zugriff auf die Datenübertragung hat. Um eine Weitergabekontrolle zu ermöglichen, ist beim E-Mail-Versand zwingend eine Verschlüsselung vorzunehmen. Bei der Verschlüsselung von E-Mails kann grundsätzlich zwischen der Transportverschlüsselung und der Ende-zu-Ende-Verschlüsselung unterschieden werden.

Die Transportverschlüsselung kann mit dem Briefversand verglichen werden. Hierbei wird der Klartext der E-Mail nur auf dem Weg von Absender*in zu Empfänger*in geschützt. Wird die E-Mail also irgendwo auf der Verbindungsstrecke abgefangen, so kann sie nicht gelesen werden. Die Ende-zu-Ende-Verschlüsselung ermöglicht dagegen einen vollständigen Schutz vor dem unberechtigten Zugriff Dritter. Hier können selbst Provider, welche die E-Nachricht an den*die Empfänger*in übermitteln, nicht mitlesen.

Für die Zugangsdaten von E-Mail-Konten müssen sichere Passwörter gewählt werden. Diese dürfen nur dem*der Benutzer*in bekannt sein *(siehe hierzu Kapitel 5.4)*.

Beim Versand einer E-Mail an mehrere Personen dürfen aus datenschutzrechtlichen Gründen die E-Mail-Adressen nicht für alle sichtbar sein. Das gilt zum Beispiel auch für die Nutzung eines Presseverteilers. Daher sollte man beim Versand an einen Verteiler im Empfängerfeld lediglich die eigene E-Mail-Adresse und alle anderen Empfänger*innen im BCC-Feld eintragen, sodass diese nicht sehen, wer die E-Mail außer ihnen selbst noch erhalten hat.

Das Anlegen von E-Mail-Verteilern und das Speichern und Nutzen von E-Mail-Adressen muss nach den Regeln der DSGVO erfolgen. So können für dienstliche Zwecke auf dienstlichen Geräten gemeinsame Outlook-Adressbücher genutzt werden, sofern der technische Schutz der Daten auf allen Geräten gewährleistet ist. Für die Nutzung von E-Mail-Verteilern ist gemäß Art. 6 DSGVO wie für jede Datenverarbeitung eine Rechtsgrundlage oder oft eine Einwilligung der betroffenen Person zur Datenverarbeitung nötig.

Gut zu wissen:
E-Mail-Adressen ohne Personenbezug wie kontakt@ oder info@ sind von der DSGVO ausgenommen.

Praxistipp:
Für die Kommunikation per E-Mail in einem geschlossenen Empfänger*innenkreis ist die Nutzung von Mailinglisten empfehlenswert. Es handelt sich hierbei um eine Liste von E-Mail-Adressen, die selbst eine eigene E-Mail-Adresse hat. Dadurch kann jedes teilnehmende Mitglied an alle anderen Mitglieder eine Nachricht schicken, ohne deren E-Mail-Adressen kennen zu müssen.

Mögliche **Rechtsgrundlagen** sind:

Erfüllung eines Vertrags

Erfüllung einer gesetzlichen Verpflichtung

Interessenabwägung

Der*die Datenverarbeitende hat ein eigenes, legitimes Interesse an dieser Verarbeitung und der*die Betroffene kein überwiegendes Gegeninteresse.

Für eine nichtkommerzielle Kommunikation ist in der Regel keine Einwilligung erforderlich, sofern diese keine unzumutbare Belästigung gemäß § 7 Gesetz gegen den unlauteren Wettbewerb (UWG) darstellt und auch nicht nach Art. 21 DSGVO widersprochen wurde. Eine E-Mail-Archivierung ist aus rechtlichen Gründen oft nötig. Für Unternehmen, die nach Steuer- und Handelsrecht zur Buchführung und Aufzeichnung verpflichtet sind, gilt je nach Art des Dokuments eine Aufbewahrungspflicht von beispielsweise sechs oder zehn Jahren nach § 257 Handelsgesetzbuch und § 147 Abgabenordnung.

§ 257 Handelsgesetzbuch
jugend-datenschutz.de/link/hgb-257

§ 147 Abgabenordnung
jugend-datenschutz.de/link/ao-147

3.4 SMS UND TELEFON

Handys und Smartphones sind aus dem Alltag nicht mehr wegzudenken. Ein wesentlicher Teil der Kommunikation wird darüber erledigt. Nutzt man diese Geräte im beruflichen Kontext und tauscht personenbezogene Daten aus, müssen die Vorschriften der DSGVO beachtet werden. Auch auf Handys und Smartphones sind gespeicherte personenbezogene Daten vor dem unberechtigten Zugriff Dritter, zum Beispiel durch eine PIN, die nur dem*der Besitzer*in bekannt ist, zu schützen. So ist zum Beispiel das Adressbuch eines Handys eine Ansammlung personenbezogener Daten, die nicht frei zugänglich sein darf.

SMS

Nutzt man SMS zur Kommunikation, gilt auch hier das Gebot der Datensparsamkeit. Man sollte sich bewusst machen, dass es hier keine Ende-zu-Ende-Verschlüsselung gibt. Daher können Daten auf dem Weg zum*zur Empfänger*in im Zuge einer sogenannten Man-in-the-Middle-Attacke gelesen oder auch verändert werden, ohne dass Empfänger*in oder Sender*in das bemerken. Können SMS nicht direkt zugestellt werden, werden sie bis zu sieben Tage beim Netzbetreiber in der Kurzmitteilungszentrale auf dem Server gespeichert.

Telefon

Telefonate sind aus DSGVO-Gesichtspunkten unkritischer, da vom Telefonat selbst keine Daten gespeichert werden und Anrufer*in und Angerufene*r direkt miteinander kommunizieren. Anders verhält es sich, wenn ein Kontakt zum ersten Mal hergestellt wird und dabei (bisher unbekannte) persönliche Daten ausgetauscht oder abgefragt werden, zum Beispiel im Rahmen einer Anmeldung zu einer Jugendferienfreizeit. Dann müsste rechtlich gesehen zunächst der Informationspflicht gemäß Art. 13 DSGVO Rechnung getragen werden. Da eine umfassende Information am Telefon zwar rechtlich erforderlich, aber wenig praktikabel ist, sollte man zumindest am Ende des Gesprächs wiederholen, welche Daten aufgenommen wurden und zu welchem Zweck diese nun gespeichert werden. Für die Mitteilung der weiteren Pflichtinformationen genügt in der Regel ein Verweis auf die eigene Website, wo die vollständigen Informationen platziert werden können.

Um eine Informationsermüdung bei den betroffenen Personen zu verhindern, können die Informationspflichten in abgestufter Form erfüllt werden. Dies wird auch als Medienbruch bezeichnet. In der ersten Stufe werden dabei nur die Basisinformationen übermittelt. In der zweiten Stufe werden dann alle Informationen nach Art. 13 bzw. Art. 14 DSGVO bereitgehalten.

Basisinformationen sind:
- die genaue Bezeichnung des Verantwortlichen;
- die Einzelheiten der Verarbeitungszwecke und
- die Betroffenenrechte.

Übrigens:
Der Verlust eines mobilen Datenträgers, auf dem die Daten nach aktuellem Stand der Technik verschlüsselt wurden, muss in der Regel nicht bei der zuständigen Datenschutzbehörde gemeldet werden.

VeraCrypt
jugend-datenschutz.de/link/veracrypt

Anleitung VeraCrypt
jugend-datenschutz.de/link/veracrypt-anleitung

3.5 DATENSPEICHER

Zur Einhaltung der DSGVO-Vorschriften kann es erforderlich sein, dass die Daten verschlüsselt gespeichert werden. Mit Hilfe der Verschlüsselung von personenbezogenen Daten kann die Wahrscheinlichkeit einer Datenpanne und somit auch eines Bußgeldes verringert werden. Inzwischen gibt es auch Hersteller, die verschlüsselte USB-Sticks anbieten.

Ein kostenloses Programm, mit dem man DSGVO-konform einzelne Daten oder auch eine ganze Festplatte verschlüsseln kann, ist VeraCrypt. Die Portable-Version des Programms kann man ohne Installation starten und so auch auf einem USB-Stick nutzen, auf dem sich personenbezogene Daten befinden.

Cloud-Speicher

Die Aufbewahrung von Daten in Cloud-Speichern ist inzwischen weit verbreitet und macht die gemeinsame Bearbeitung von Dokumenten einfacher. In Bezug auf die Regelungen der DSGVO ist es oft mit einem größeren Aufwand verbunden, wenn Anbieter von Cloud-Diensten genutzt werden, die ihren Sitz außerhalb der EU haben und dort die Daten speichern. DSGVO-konforme Alternativen zu den bekannten Anbietern

Dropbox, OneDrive und iCloud sind nach derzeitigem Stand der Technik und Sicherheit zum Beispiel TeamDrive und die Open Telekom Cloud.

In jedem Fall sollte mit dem Cloud-Anbieter vor der Nutzung ein Auftragsverarbeitungsvertrag *(siehe hierzu Kapitel 5.3)* abgeschlossen werden. Einige Dienstleister bieten einen solchen Auftragsverarbeitungsvertrag zum Download auf ihrer Seite an.

TeamDrive
jugend-datenschutz.de/link/teamdrive

Open Telekom Cloud
jugend-datenschutz.de/link/open-telekom-cloud

3.6 FOTO, VIDEO, TON

Fotos, Videos und Tonaufnahmen von Personen sind immer auch datenschutzrelevant. Geht es darum, eine Veranstaltung zu dokumentieren, ist das unter Beachtung einiger Regeln grundsätzlich möglich, selbst wenn einzelne Personen auf den Aufnahmen zu identifizieren sind.

Foto-, Video- und Tonaufnahmen von Erwachsenen

Die Anfertigung von Foto-, Video- und Tonaufnahmen von Erwachsenen (als Verarbeitung personenbezogener Daten) ist gemäß Art. 6 Abs. 1 DSGVO zulässig, wenn der*die Abgebildete eingewilligt hat oder eine andere Rechtsgrundlage dies erlaubt. Das heißt, eine Einwilligung der abgebildeten Person muss nicht immer zwingend eingeholt werden. Es empfiehlt sich darüber hinaus nicht, Einwilligungen für Datenverarbeitungsmaßnahmen einzuholen, die bereits aufgrund einer gesetzlichen Grundlage erlaubt sind. In jedem Fall muss darüber informiert werden, dass und auf Basis welcher Rechtsgrundlage Aufnahmen gemacht werden.

Die Verarbeitung personenbezogener Daten in Form von Foto-, Video- und Tonaufnahmen kann auch auf eine Abwägung der schutzwürdigen Interessen der Beteiligten nach Art. 6 Abs. 1 f DSGVO gestützt werden. Hiernach ist eine Datenverarbeitung zulässig, wenn dies zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten des*der Abgebildeten, die den Schutz personenbezogener Daten erfordern, überwiegen. Die Dokumentation einer Veranstaltung wäre ein solch berechtigtes Interesse des Verantwortlichen.

Vorlage 13: Anleitung zur Findung der richtigen Rechtsgrundlage bei Foto- und Videoaufnahmen als Video zum Abruf
jugend-datenschutz.de/link/13

Wichtig:
Es muss eine Interessenabwägung erfolgen, die dokumentiert werden sollte.

Unabhängig von der Rechtsgrundlage müssen Besucher*innen aber möglichst bereits bei der Anmeldung oder beim Betreten des Veranstaltungsortes angemessene Informationen erhalten. Die Aufsichtsbehörden empfehlen auf die Datenverarbeitung etwa in Form eines nicht übersehbaren Aufstellers im Eingangsbereich einer Veranstaltung hinzuweisen. Der Hinweis sollte mindestens folgende Inhalte haben:

- die Information, dass eine Datenverarbeitung stattfindet und in welcher Form;
- Art und Zweck der weiteren Verarbeitung (z. B. Verwendung auf der Website oder in sozialen Medien);
- an wen sich Betroffene für Datenschutzfragen wenden können.

Sollten einzelne Personen eine Ablichtung nicht wünschen, stünde es ihnen so frei, den Kontakt mit dem*der Fotograf*in zu suchen, um eine interessengerechte Umsetzung zu erreichen.

Aufnahmen dürfen niemals heimlich gemacht werden und nicht die Privat- oder Intimsphäre der Betroffenen erfassen.

Erfordert die Erteilung der Information einen unverhältnismäßigen Aufwand, kann unter Umständen die direkte Informationspflicht entfallen. In diesen Fällen ist nach Art. 14 Abs. 5 b Satz 2 DSGVO die Information für die Öffentlichkeit bereitzustellen.

Foto-, Video- und Tonaufnahmen von Kindern und Jugendlichen

Gemäß Art. 6 DSGVO ist insbesondere dann von einer überwiegenden Schutzbedürftigkeit der Betroffeneninteressen gegenüber den berechtigten Interessen des Verantwortlichen auszugehen, wenn Aufnahmen von Kindern und Jugendlichen gemacht werden.

Sind also Aufnahmen von Kindern und Jugendlichen geplant, sollten die jungen Menschen und gegebenenfalls auch die Personensorgeberechtigten schon frühzeitig so transparent wie möglich informiert und gegebenenfalls eine Einwilligung eingeholt werden. Diese muss leicht verständlich sein, freiwillig erfolgen können und darf nicht zu allgemein formuliert sein, da sie sonst die Anforderungen der DSGVO nicht erfüllt. Es hängt von der Einwilligungsfähigkeit des jungen Menschen ab, ob dieser die Einwilligung selbst erteilen darf oder ob die Einwilligung von den Personensorgeberechtigten erteilt werden muss. Die Einwilligungsfähigkeit wird nicht an einem bestimmten Alter ausgemacht. Es erfolgt stets eine Beurteilung im Einzelfall *(siehe hierzu Kapitel 2.5.2)*.

Gut zu wissen:
Eine solche Einwilligung muss nicht zwingend schriftlich erfolgen. Das bisherige Schriftformerfordernis ist mit Geltung der DSGVO grundsätzlich entfallen. Auch mündliche Erklärungen sind wirksam, müssen jedoch im Zweifel nachgewiesen werden. Es empfiehlt sich deshalb, die Einwilligungserklärungen schriftlich einzuholen und sie zu Dokumentationszwecken aufzubewahren.

Veröffentlichung im Internet

Sollen Aufnahmen im Internet veröffentlicht werden, gilt besondere Vorsicht, da sich das erfahrungsgemäß nicht vollständig rückgängig machen lässt. Daher geht man hier aktuell von einem Überwiegen der Betroffeneninteressen gegenüber den berechtigten Interessen des*der Verantwortlichen aus und es sollte unbedingt auch bei Aufnahmen von Erwachsenen eine Einwilligung eingeholt werden, die den Zweck der Veröffentlichung im Internet abdeckt. Zu beachten ist auch, dass die Veröffentlichung auf der eigenen in der EU gehosteten Website unkritischer ist als die Veröffentlichung in sozialen Netzwerken.

Datensparsamkeit

Auch für Foto-, Video- und Tonaufnahmen gilt das Gebot der Datensparsamkeit. So sollten Beschriftungen, Dateinamen und Metadaten, mit denen sich ein Personenbezug herstellen lassen könnte, aus den Dateien entfernt werden. Bildunterschriften sollten immer allgemein gehalten werden und keine Namen von abgebildeten Personen enthalten.

3.7 WHATSAPP UND ANDERE MESSENGERDIENSTE

Die Nutzung von Online-Diensten spielt im Kontext der Jugend- und Jugendverbandsarbeit eine große Rolle. Messenger sind fester Bestandteil der Lebenswelt junger Menschen. So erscheint es nur zeitgemäß, diese Art der Kommunikation mit ihnen zu nutzen. In der Jugend- und Jugendverbandsarbeit sind jedoch, im Gegensatz zur privaten Nutzung, bei der Verwendung von Diensten wie WhatsApp oder Instagram *(siehe hierzu Kapitel 3.8)* die Regelungen der DSGVO einzuhalten. Zudem stehen in der Jugend- und Jugendverbandsarbeit tätige Personen in der Verantwortung, Themen wie Privatsphäre und Medienkonsum im Kontext des erzieherischen Kinder- und Jugendschutzes zu bearbeiten. Sie haben dadurch eine besondere Vorbildfunktion zu erfüllen. Im Folgenden werden einige Dienste kurz vorgestellt und ihre Vor- und Nachteile beschrieben. Jegliche Nutzung sollte intensiv abgewogen und ihr Einsatz im Verhältnis zur beabsichtigten Wirkung geprüft werden. Die Entwicklung der Online-Dienste befindet sich im stetigen Wandel. Dieser muss verfolgt werden, um auf Neuerungen reagieren zu können. Eigene Arbeitsweisen sollten immer wieder geprüft und angepasst werden.

WhatsApp

Beim Messenger WhatsApp werden Text- und Sprachnachrichten sowie Fotos und Videos beim Versand Ende-zu-Ende-verschlüsselt (das heißt, Nachrichten können nur von Sender*in und Empfänger*in gelesen werden), aber der Dienst liest sämtliche Kontaktdaten aus den Adressbüchern der Nutzer*innen aus und gibt diese Daten dann zum Beispiel an Meta weiter.

Normalerweise haben Nutzer*innen nicht sämtliche ihrer Kontakte über ihre Nutzung von WhatsApp informiert und deren Erlaubnis eingeholt, dass sie die Übertragung der Daten durch Zustimmung zu den Nutzungsbedingungen zulassen. Das ist bereits im privaten Bereich heikel – im beruflichen Umfeld der Jugend- und Jugendverbandsarbeit jedoch überhaupt nicht zulässig.

Threema

Über den werbefreien Dienst Threema mit Sitz in der Schweiz können ebenso Texte, Sprachnachrichten, Bilder und Videos verschickt werden. Es gibt eine Ende-zu-Ende-Verschlüsselung und anfallende Metadaten sind geschützt. Nachrichten werden unmittelbar nach ihrer Zustellung von den Servern gelöscht und der Quellcode steht als Open Source zur Verfügung. Die Identifikation der Nutzer*innen erfolgt über eine achtstellige ID, sodass Threema anonym genutzt werden kann und keine Verknüpfung mit der eigenen Telefonnummer oder E-Mail-Adresse nötig ist. Threema bietet zwar die Möglichkeit eines Adressbuchabgleiches, lädt die dort gespeicherten Nummern aber nicht auf seine Server, sondern erstellt aus ihnen einen sogenannten „Hash“. Das ist eine zufällige Nummernfolge, mit der sich abgleichen lässt, ob Freund*innen den Dienst nutzen. So überträgt man als Nutzer*in keine Daten von anderen an das Unternehmen. Threema muss einmalig kostenpflichtig heruntergeladen werden. Weitere Kosten entstehen mit der Nutzung nicht.

Achtung:
Wenn der Kontakt bezüglich Terminabsprachen oder Koordination von Projekten zu einer Gruppe Jugendlicher vorrangig mittels eines Messengers erfolgt, einzelne Jugendliche den von den meisten gewählten Dienst aber nicht nutzen möchten oder von Seiten ihrer Personensorgeberechtigten nicht nutzen dürfen, werden diese von der Kommunikation ausgeschlossen.

Signal

Der kostenlose, werbefreie Messenger Signal hat ähnliche Funktionen wie WhatsApp und Threema. Signal gleicht auch das Adressbuch ab, allerdings werden beim Abgleich des Adressbuches alle Kontakte anonymisiert und nach dem Abgleich wieder von den Signal-Servern gelöscht. Die Server des Dienstes stehen jedoch in den USA und zur Identifikation muss die eigene Telefonnummer angegeben werden.

Praxistipps

Besonders WhatsApp ist beim Thema Datenschutz in der Jugend- und Jugendverbandsarbeit kritisch zu betrachten und kein DSGVO-konformer Dienst. Das sollte auch den jungen Menschen gegenüber immer wieder klar kommuniziert werden.

Folgende Punkte können beim Einsatz von Online-Diensten, insbesondere in der Jugend- und Jugendverbandsarbeit, in jedem Fall beachtet werden:

- Fachkräfte der Jugend- und Jugendverbandsarbeit dürfen Kinder und Jugendliche nicht zur Registrierung eines Online-Dienstes auffordern und sollten immer alternative Kontaktmöglichkeiten und auch verschiedene Messenger-Dienste anbieten.
- Veranstaltungsinformationen und allgemeine Termine können vermittelt werden, sensible Informationen und Gespräche jedoch nicht.
- Beratungstermine mit Kindern und Jugendlichen sollten immer ohne Angabe eines Grundes kommuniziert werden.
- Für die Kommunikation mit Kindern und Jugendlichen ist stets ein Diensthandy zu nutzen.
- Die Begründung der Entscheidungen für Online-Dienste mit den Abwägungen (Zweck, Verhältnismäßigkeit, Eignung, Erforderlichkeit und Angemessenheit) und den bekannten Problemfeldern sollte gut und genau dokumentiert werden.
- Dienstanweisungen haben Vorrang vor diesen Hinweisen.

Achtung:
Diese Hinweise machen die Dienste nicht DSGVO-konformer, ermöglichen jedoch einen sensibleren Umgang mit personenbezogenen Daten.

3.8 INSTAGRAM UND FACEBOOK

Die Arbeit in sozialen Netzwerken, wie zum Beispiel Instagram und Facebook, ist für viele zum notwendigen Aufgabenbereich innerhalb der Jugend- und Jugendverbandsarbeit geworden. Sie dient gleichermaßen der Kommunikation und Interaktion mit den Adressat*innen wie auch der eigenen Darstellung und Bewerbung von Aktivitäten. Für eine erfolgreiche Öffentlichkeitsarbeit stellt sich immer die Frage, wie Foto- und Video-Material aus datenschutzrechtlicher Sicht richtig verwendet werden kann, ohne die Persönlichkeitsrechte der Betroffenen zu verletzen. In *Kapitel 3.6* wird auf das Thema Foto-, Ton- und Videoaufnahmen und deren Veröffentlichung eingegangen. Unabhängig davon kann der Betrieb von Facebook-Fanpages und Instagram aktuell nicht rechtskonform durchgeführt werden. Die Aufsichtsbehörden weisen seit Jahren auf die datenschutzrechtlichen Probleme hin und fordern die Abschaltung der Seiten.

FAQ zu Facebook-Fanpages
jugend-datenschutz.de/link/facebook

Werden soziale Netzwerke wie Instagram und Facebook für die Öffentlichkeitsarbeit einer Organisation eingesetzt, sollte man sich immer wieder vor Augen halten, hier besonders sensibel und sparsam mit personenbezogenen Daten umzugehen. Diese Kanäle sollten nur zusätzlich zu datenschutzrechtlich unproblematischeren Kommunikationswegen, wie einer eigenen Website *(siehe hierzu Kapitel 3.9)*, genutzt werden. Es empfiehlt sich, auf Websites und insbesondere in den sozialen Netzwerken lediglich unverfängliche Inhalte mit informativem Charakter zu veröffentlichen, bei denen es kein Problem ist, wenn sie auch noch nach Jahren im Internet auffindbar sind. Besucher*innen einer Organisationsseite in den sozialen Medien sollten zudem auf eine eigenverantwortliche Nutzung hingewiesen werden und Informationen zu alternativen Kontaktmöglichkeiten bekommen.

Achtung:
Bei den Nutzer*innen darf niemals der Eindruck entstehen, ein soziales Netzwerk wie Facebook müsse genutzt werden, um bestimmte Informationen zu erhalten oder um mit der Organisation kommunizieren zu können.

Auf der Facebook-Seite sollte im Fall von Organisationsseiten im Info-Bereich neben dem Impressum auch ein eigener Datenschutzhinweis, zum Beispiel als Link zur auf der Organisations-Website veröffentlichten Datenschutzerklärung, sowie ein Hinweis zur Verwendung von personenbezogenen Daten durch Facebook eingetragen werden.

Vorlage 14: Der richtige Umgang mit eigenen Social-Media-Präsenzen als Video zum Abruf
jugend-datenschutz.de/link/14

3.9 WEBSITE

Der Internet-Auftritt von Organisationen, Jugendringen und Jugendverbänden ist aus der Praxis nicht mehr wegzudenken. Allerdings stellt die Veröffentlichung von personenbezogenen Daten im Internet (ohne Passwortschutz) eine Datenübermittlung an Dritte dar und ist mit hohen Risiken besetzt. Daher ist die Veröffentlichung von personenbezogenen Daten im Internet, egal ob auf der Website, bei Facebook, Instagram oder einem anderen Online-Portal, grundsätzlich unzulässig, wenn der*die Betroffene nicht ausdrücklich eingewilligt hat *(siehe hierzu auch Kapitel 1.3)*.

Übrigens:
Auch IP-Adressen sind als personenbezogene Daten anzusehen.

Wenn sich eine Website an einen unbestimmten Personenkreis richtet und grundsätzlich für alle Internetnutzer*innen abrufbar ist, müssen die Anforderungen der DSGVO beachtet werden, egal ob es sich um einen gemeinnützigen Seitenbetreiber oder um ein gewinnorientiertes Unternehmen handelt.

Wenn die Website über einen Webhosting-Anbieter ins Internet gestellt wird, hat dieser Anbieter Zugang zu personenbezogenen Daten, wie den IP-Adressen der Besucher*innen. Aus diesem Grund muss mit dem Webhoster ein Vertrag zur Auftragsverarbeitung abgeschlossen werden. Schon allein deswegen muss ein vollständiger Datenschutzhinweis auf der Website veröffentlicht sein. Die Landesbeauftragte für Datenschutz Niedersachsen hat ein hilfreiches Papier mit Informationen für Websitebetreiber*innen veröffentlicht. Darin steht auch, welche Informationen die Datenschutzerklärung in welcher Form enthalten muss. Gemäß Art. 12 Abs. 1 DSGVO müssen beispielsweise alle Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form, in einer klaren und einfachen Sprache geschrieben sein.

Informationen für Betreiber*innen von Websites zur Anpassung an die DSGVO:
jugend-datenschutz.de/link/webseiten

Nutzer*innen müssen unter anderem darüber informiert werden, ob Cookies gesetzt werden, ob Inhalte von anderen Websites (zum Beispiel Videos) oder Social Plug-Ins (zum Beispiel Facebook) unmittelbar eingebunden sind und ob die Website Möglichkeiten vorsieht, durch die Nutzer*innen selbst personenbezogene Daten auf der Website eingeben und diese Daten auch übermitteln zu können (zum Beispiel über Formulare).

Außerdem müssen auch für Websites geeignete technische und organisatorische Maßnahmen getroffen werden *(siehe hierzu auch Kapitel 5.4)*. Können Nutzer*innen personenbezogene Daten auf der Website eingeben (zum Beispiel über Kontaktformulare oder eine Kommentarfunktion), dürfen diese Daten nur verschlüsselt (durch den Einsatz eines aktuellen https-Protokolls) an den*die Verantwortliche*n übermittelt werden.

3.10 ÖFFENTLICHE VERANSTALTUNGEN

Auch bei der Durchführung von öffentlichen Veranstaltungen sind die Regelungen der DSGVO zu beachten. Hinweise zu Foto-, Video- oder Tonaufnahmen im Rahmen solcher Veranstaltungen sind in *Kapitel 3.6* zusammengefasst. Häufig sollen bei sportlichen Veranstaltungen wie Skatecontests bei der Ehrung der Sieger*innen personenbezogene Daten wie Namen, Alter, Wohnort und die sportliche Leistung von den Teilnehmer*innen vor dem Publikum genannt werden. In solchen Fällen ist das aus datenschutzrechtlichen Gründen nur zulässig, wenn der*die Betroffene eingewilligt hat oder eine Rechtsgrundlage dies erlaubt.

Bei einwilligungsfähigen Kindern und Jugendlichen *(siehe hierzu Kapitel 2.5.2)* muss keine gesonderte Einwilligung der Personensorgeberechtigten eingeholt werden.

Praxistipp:
Die Teilnahme an sportlichen Wettbewerben setzt in den meisten Fällen eine Anmeldung voraus. In diesem Fall besteht die Möglichkeit, die Teilnehmer*innen über die Datenerfassung und Weitergabe im Rahmen der Siegerehrung zu informieren.

3.11 DATENWEITERGABE AN ANDERE STELLEN

In der Jugend- und Jugendverbandsarbeit müssen personenbezogene Daten aus unterschiedlichsten Gründen an andere Stellen weitergegeben werden. Hierbei handelt es sich um eine Weitergabe an Dritte. Typische Beispiele für diese Art der Weiterverarbeitung von Daten sind die Übermittlung von Teilnehmer*innendaten an Zuwendungsgeber*innen oder Mitveranstalter*innen, die Zusammenarbeit mit Medienagenturen, IT-Dienstleistenden oder eine ausgelagerte Buchhaltung. Erfolgt dies im Rahmen einer Auftragsverarbeitung, so muss ein Auftragsverarbeitungsvertrag geschlossen werden *(siehe hierzu Kapitel 5.3)*.

Ansonsten müssen die Betroffenen der Datenweitergabe entweder nach umfassender Information zugestimmt haben oder eine andere rechtliche Grundlage erlaubt dies. So kann die Weitergabe zur Erfüllung von Vertragszwecken (zum Beispiel eines Arbeitsvertrages) erforderlich und damit rechtlich abgesichert sein.

Liegt eine rechtliche Grundlage vor, kann in den Datenschutzhinweisen, die zum Beispiel zusammen mit dem Anmeldeformular für eine Ferienfreizeit an die Betroffenen übermittelt werden, unter dem Punkt „Kategorien von Empfänger*innen der personenbezogenen Daten“ angegeben werden, an wen und zu welchen Zwecken eine Datenübermittlung stattfindet. Wenn möglich, empfiehlt es sich aus Gründen der Transparenz, die konkreten Empfänger*innen exakt anzugeben. Neben dem Namen des*der Empfänger*in sollte auch seine*ihre Adresse angegeben werden. Es gilt zu beachten, dass jede Weiterverarbeitung, und damit auch die Datenweitergabe an Dritte, einen Zweck verfolgen muss, der mit dem Zweck der Erhebung vereinbar ist.

Vorlage 15: Datenschutzhinweis für eine Ferienfreizeit
jugend-datenschutz.de/link/15

04 PRAXISSITUATIONEN IN DER JUGEND- UND JUGENDVERBANDSARBEIT

Nachdem im vorangegangenen Kapitel auf für die Jugend- und Jugendverbandsarbeit typische Prozesse und den Umgang mit personenbezogenen Daten im Rahmen dieser Prozesse eingegangen wurde, widmet sich das folgende Kapitel ausgewählten Praxissituationen aus der Jugend- und Jugendverbandsarbeit und ordnet diesen die jeweils relevanten Prozesse zu.

4.1 BERATUNG

Fallbeispiel:
Die 13-jährige Lisa bittet die Schulsozialarbeiterin Petra per WhatsApp um ein vertrauliches Gespräch. Sie berichtet in ihrer Sprachnachricht von Schwierigkeiten zwischen ihren Eltern und dem Klassenlehrer. Petra bietet Lisa ein gemeinsames Gespräch in ihrem Büro an. Petra ist sich unsicher, ob sie die Informationen aus der WhatsApp-Nachricht dokumentieren darf.

Ein Beratungsprozess ist durch ein für Berater*in und Adressat*in gleichermaßen bewusstes Setting gekennzeichnet. Dieses beinhaltet zum Beispiel die Vertraulichkeit der Gesprächsinhalte und eine Rollenklärung. Bestandteile einer Beratung sind die Informationsvermittlung, die Bewertung von Entscheidungsalternativen sowie eine auf einen definierten Zeitraum beschränkte Einzelhilfe. Spontane Gespräche, die keine weiteren Tätigkeiten der Beratungsgebenden erfordern, sind im Kontext dieser Handreichung nicht relevant, da in aller Regel keine personenbezogenen Daten verarbeitet werden.

Bevor eine Beratung zustande kommt, findet eine Kontaktaufnahme zwischen Berater*in und Adressat*in statt. Es ist davon auszugehen, dass sich beide bereits kennen und ein Vertrauensverhältnis vorliegt. Ist das nicht der Fall und sollen personenbezogene Daten aufgenommen und verarbeitet werden, um beispielsweise zu einem späteren Zeitpunkt erneut Kontakt aufnehmen zu können, muss dies wegen der Informationspflicht *(siehe Kapitel 3.1)* gemäß Art. 13 und Art. 14 DSGVO so transparent wie möglich für die betroffene Person geschehen.

Egal ob personenbezogene Daten im Rahmen einer Beratung in Papierform oder elektronisch erfasst wurden – sie müssen ausreichend gesichert sein *(siehe hierzu Kapitel 5.4)*.

Je nachdem, auf welchem Kommunikationsweg welche Informationen ausgetauscht werden, müssen gegebenenfalls die Richtlinien der DSGVO oder eine geltende Schweigepflicht beachtet werden. Werden von Seiten der beratenden Person Informationen wie Geburtsdatum, Telefonnummer oder Adresse erfragt, ist das DSGVO-relevant. Ein Austausch von Informationen über die persönlichen, familiären, wirtschaftlichen und beruflichen Verhältnisse und auch schon die Tatsache, dass ein Besuch in einer Beratungsstelle stattgefunden hat, erfordern von bestimmten Berufsgruppen das Einhalten der Schweigepflicht *(siehe hierzu Kapitel 2.5)*.

Grundsätzliche Informationen zur Kommunikation per E-Mail gibt es in *Kapitel 3.3*, Ausführungen zum Einsatz von SMS und Telefon in *Kapitel 3.4* und zur Nutzung von Messenger-Diensten in *Kapitel 3.7*.

Werden personenbezogene Daten erhoben und verarbeitet, sind die Adressat*innen zu Beginn der Beratung zu informieren. Der Zweck muss entsprechend weit gefasst werden, so dass er zum Beispiel auch den Fall abdeckt, dass Inhalte der Beratung aus Gründen des Selbstschutzes dokumentiert und längerfristig gespeichert werden.

Eine Weitergabe von Gesprächsinhalten an Dritte ist auch im geschützten Rahmen von Teambesprechungen ohne Einverständnis des*der Betroffenen ausgeschlossen. Um eine Fallbesprechung im kollegialen Rahmen durchführen zu können, muss der Beratungsprozess so weit anonymisiert werden, dass kein Rückschluss auf die betroffene Person möglich ist. In vielen Fällen genügen den Kolleg*innen jedoch wenige Informationen, um eine Person zu identifizieren. Hierfür empfiehlt es sich, die betroffene Person über die Fallbesprechung mit anderen Fachkräften zu informieren. In *Kapitel 2.5* sind weitere Ausführungen zu Aspekten aus den Bereichen Vertrauensschutz, Datenschutz und Schweigepflicht in der Jugend- und Jugendverbandsarbeit ausgeführt. Auf Wunsch der betroffenen Person müssen alle gespeicherten Daten rückstandslos gelöscht werden. Das schließt die gesamte Kommunikation und sämtliche Kontaktdaten, Informationen und Notizen, die gespeichert wurden, ein.

Gut zu wissen:
Wenn der Zweck der Erhebung und der Zweck der Weiterverarbeitung (Speicherung/Aufbewahrung) miteinander vereinbar sind, verstößt die Weiterverarbeitung der Daten nicht gegen die nötige Zweckbindung. Sie kann also auf die Erlaubnis gestützt werden, die für die Erhebung galt. Einer neuen oder gar zusätzlichen Rechtsgrundlage bedarf es für die Weiterverarbeitung nicht. Betroffene müssen gemäß Art. 13 Abs. 3 DSGVO lediglich darüber informiert werden. So ist der Zweck der Beratung bzw. Hilfestellung mit dem Zweck der Aufbewahrung bzw. Dokumentation vereinbar.

4.2 BILDUNGSANGEBOTE

Maßnahmen der außerschulischen Jugendbildung sind sehr vielfältig: Workshops, Seminare, Kurse, Schulungen oder Fachtage. In aller Regel erfolgt die Anmeldung im Vorfeld bei dem*der Veranstalter*in. Daraus ergibt sich die Chance, erforderliche Einverständniserklärungen, zum Beispiel für die Datenverarbeitung, Fotoerlaubnis und die Datenweitergabe bei Verwendungsnachweisen bereits mit dem Anmeldeformular einzuholen.

Die Bewerbung und Bekanntmachung von Bildungsangeboten zur Gewinnung von Teilnehmer*innen können auf verschiedenen Wegen erfolgen. So werden zum Beispiel Aushänge in der Jugendfreizeiteinrichtung gemacht, Mailings versendet oder eine Veranstaltung per Facebook geteilt. Sind DSGVO-relevante Daten (zum Beispiel als Kontaktangabe die Handynummer oder E-Mail-Adresse der Kursleitung) Teil der Information und Einladung, muss eine rechtliche Grundlage (zum Beispiel Honorarvertrag oder Einverständniserklärung des*der Betroffenen) vorliegen.

Wird die Einladung direkt an Einzelpersonen adressiert (zum Beispiel per E-Mail verschickt, *siehe hierzu Kapitel 3.3*) sind die Vorschriften der DSGVO einzuhalten, wenn es sich um private E-Mail-Adressen handelt. Von den Betroffenen muss die Zustimmung vorliegen, dass ihre Daten zum Zweck des Versandes einer Einladung an sie genutzt werden dürfen.

Wie bei jedem Datenverarbeitungsprozess müssen auch bei Bildungsangeboten die Grundsätze der Datenverarbeitung *(siehe Kapitel 2.3)* eingehalten werden. Daher sollten bei der Anmeldung nur die Daten abgefragt werden, die zur Durchführung der Maßnahme nötig sind. Durch die Anmeldung kommt ein Vertrag zwischen Veranstalter*in und Teilnehmer*in zustande, auf dessen Grundlage für den Zweck der Veranstaltung bzw. des Bildungsangebotes personenbezogene Daten gespeichert und verarbeitet werden dürfen.

Fallbeispiel:
Svenja organisiert die Juleica-Schulung ihres Jugendverbandes. Für die Anmeldung zur mehrtägigen Juleica-Schulung ist von den Teilnehmer*innen ein Anmeldeformular auszufüllen. Bisher wurden die Anmeldedaten (Adresse und E-Mail) auch dazu genutzt, um den Teilnehmer*innen weitere Informationen und Angebote des Jugendverbandes zuzusenden.

Gut zu wissen:
Die verbindliche Anmeldung zu einer Veranstaltung ist Grundlage für die weitere Datenverarbeitung gemäß Art. 6 Abs. 1 b DSGVO.

Zusammen mit der Anmeldung kann bei Bedarf eine Einverständniserklärung zu Foto-, Ton- und/oder Filmaufnahmen erbeten werden *(siehe hierzu Kapitel 3.6)*.

Wenn keine anderen rechtlichen Gründe dagegensprechen oder andere Fristen vereinbart wurden, müssen sämtliche personenbezogene Daten nach Vertragserfüllung gelöscht werden. Für Statistiken empfiehlt es sich, Daten anonymisiert zu speichern.

4.3 OFFENE ANGEBOTE UND FREIZEITANGEBOTE

Fallbeispiel:
Der städtische Jugendclub organisiert einmal jährlich ein Mitternachtsturnier für junge Menschen ab 16 Jahren. Eine Anmeldung ist grundsätzlich nicht nötig. Die Teams werden erst vor Ort gebildet. Personen, die noch nicht volljährig sind, benötigen jedoch zur Teilnahme eine Einverständniserklärung der Personensorgeberechtigten. Die Sozialarbeiter*innen rätseln, ob diese Einverständniserklärung beim Träger aufbewahrt werden darf.

In Abgrenzung zu den Bildungsangeboten nehmen junge Menschen häufig unangemeldet an offenen Angeboten teil. Bei der Gestaltung offener Treffpunkte, wie es sie in Jugendclubs gibt, und bei der Durchführung von öffentlichen Veranstaltungen, wie Fußballturnieren, Skatecontests und Spielplatzfesten, muss daher zunächst geklärt werden, welche personenbezogenen Daten überhaupt erhoben werden müssen, um die Maßnahme durchzuführen und gegebenenfalls abzurechnen.

Ist eine Teilnahme ohne Anmeldung und Registrierung vor Ort möglich, findet keine Erfassung personenbezogener Daten der Nutzer*innen statt und das Angebot ist aus datenschutzrechtlicher Sicht unproblematisch. Werden jedoch Foto-, Ton- oder Filmaufnahmen gemacht, sollten die Empfehlungen aus *Kapitel 3.6* berücksichtigt werden. Handelt es sich um Wettbewerbe, bei denen Sieger*innen ermittelt und bekannt gemacht werden sollen, müssen personenbezogene Daten erfasst werden. Hinweise dazu finden sich in *Kapitel 3.10*. In jedem Fall gilt es auch hier, das Gebot der Datensparsamkeit zu beherzigen und so wenige Daten wie möglich zu erfassen. So sollte keine Teilnahmeliste ausgelegt werden, auf der ein namentlicher Eintrag erforderlich ist, wenn keine benötigt wird und lediglich die Gesamtzahl der Teilnehmer*innen erfasst werden soll. Das ist auch durch anonymisierte Verfahren möglich. Sind eine Anmeldung bzw. eine Einverständniserklärung der Personensorgeberechtigten zur Veranstaltung möglich oder gar erforderlich, gibt es weitere Informationen zum Verfahren in *Kapitel 4.2*.

Da festangestellte Mitarbeiter*innen bei offenen Angeboten und Freizeitangeboten oft von Honorarkräften und ehrenamtlich Tätigen unterstützt werden, empfiehlt sich ein Blick in *Kapitel 1.4* und den Abschnitt zum Thema Absicherung privater Technik in *Kapitel 5.4*.

4.4 GRUPPENARBEIT

Bei der Arbeit mit festen Gruppen, die in der Regel durch einen geschlossenen Teilnehmendenkreis gekennzeichnet sind, steht oftmals die Kommunikation (z. B. via WhatsApp, in Gesprächskreisen) und die gemeinsame Planung von Aktivitäten (z. B. Gruppenfahrten) im Vordergrund.

Da für die Verarbeitung personenbezogener Daten entweder eine Einverständniserklärung oder eine andere rechtliche Grundlage des*der Betroffenen vorliegen muss, kommt manchmal die Idee auf, eine einmalige und allumfassende Einverständniserklärung einzuholen, die dann im Idealfall jahrelang für verschiedenste Zwecke genutzt werden könnte. Da eine Datenverarbeitung aber jeweils nur für einen bestimmten Zweck erfolgen darf, der klar kommuniziert werden muss, ist von einer zu allgemeinen Formulierung in einer Einverständniserklärung abzuraten, da diese im Zweifelsfall als ungültig erachtet wird. Das heißt, der Zweck sollte stets sorgfältig überlegt und kommuniziert werden, genau benannt und möglichst nachvollziehbar sein. So können die mit einer langfristigen Teilnahme in einer Jugendgruppe einhergehenden Datenverarbeitungsprozesse auch über einen längeren Zeitraum hinweg ein regelkonformer Grund sein, vergleichbar mit einem Arbeitsverhältnis oder einer Vereinsmitgliedschaft. Idealerweise sollte aufgeführt werden, welche Datenverarbeitungsprozesse abgedeckt werden sollen und für welche Zwecke (zum Beispiel: Fotoaufnahmen von Gruppenreisen werden zur Öffentlichkeitsarbeit auf der Website veröffentlicht, Teilnahmelisten zur Organisation und Abrechnung von Workshops geführt oder Handynummern innerhalb der Gruppe ausgetauscht, um die Kommunikation untereinander zu ermöglichen).

Für die Kommunikation innerhalb der Gruppe wird im Alltag auf SMS *(siehe hierzu Kapitel 3.4)* oder auf Messenger wie WhatsApp zurückgegriffen. Was hierbei zu beachten ist, ist in *Kapitel 3.7* zusammengefasst.

Fallbeispiel:
Der Gemeindepädagoge Jakob der jungen Gemeinde im Kirchenkreis führt gemeinsam mit Kindern und Jugendlichen viele Aktivitäten, Ausflüge, Seminare und Ferienfreizeiten durch. Für jede einzelne Aktivität ist das Einholen der erforderlichen Einverständniserklärungen der Personensorgeberechtigten und Teilnehmenden sehr mühsam. Daher wird überlegt, ein Papier mit einer „Generalvollmacht“ zu entwickeln.

4.5 NETZWERKARBEIT UND KOMMUNIKATION

Jugend- und Jugendverbandsarbeit wird häufig in Verbundsystemen mit verschiedenen Akteur*innen ermöglicht. Dienstberatungen, E-Mail-Kommunikation und Adressverwaltung sind von besonderer Bedeutung, damit Fachkräfteteams, zum Teil auch trägerübergreifend, Veranstaltungen durchführen können. Im Vordergrund stehen daher Verhaltensregeln im Umgang mit dienstlichen Kontakten.

Hinweise für einen datenschutzkonformen Einsatz von E-Mails sind in *Kapitel 3.3* zusammengefasst. Regeln für die Teilnehmendenverwaltung bei Veranstaltungen sind in *Kapitel 3.1* zu finden und was es bei öffentlichen Veranstaltungen zu beachten gibt, steht in *Kapitel 3.9*. Die Weitergabe von Daten an andere Stellen ist in *Kapitel 3.11* ausgeführt und das Thema Auftragsverarbeitungsvertrag wird in *Kapitel 5.3* näher beleuchtet.

Der Austausch und die Weitergabe von Kontakten sind dann möglich, wenn das zu dem Zweck geschieht, über den die Betroffenen in Kenntnis gesetzt wurden. Hat sich beispielsweise ein*e Jugendliche*r für einen Workshop angemeldet und wurde bei der Anmeldung darüber

Fallbeispiel:
Die mobilen Jugendarbeiter*innen in einem Landkreis erarbeiten ein Streetsoccerturnier, das trägerübegreifend an verschiedenen Orten umgesetzt wird. Für die Vorbereitung ist es notwendig, gemeinsamen Zugriff auf die Kontakte der Vorbereitungsgruppe sowie die Teilnehmendenverwaltung zu haben. Es herrscht Uneinigkeit, ob die Anmeldedaten der Teilnehmenden unter den beteiligten Trägern ausgetauscht werden dürfen.

informiert, dass personenbezogene Daten zum Zweck der Organisation und Durchführung der Veranstaltung durch Dritte verarbeitet werden, können die Daten an alle beteiligten Fachkräfte weitergegeben werden – sofern das erforderlich ist. Die Daten dürfen dann aber zum Beispiel nicht genutzt werden, um den*die Jugendliche*n zu weiteren Veranstaltungen oder Workshops einzuladen – es sei denn, er*sie hat diesem Zweck der Datenverarbeitung zugestimmt.

Der Austausch von personenbezogenen Daten muss immer sicher erfolgen – *siehe hierzu Kapitel 3.5*, in dem es auch um die Datenverschlüsselung geht, und *Kapitel 5.4*, das die technischen und organisatorischen Maßnahmen beschreibt, die zu ergreifen sind.

Ein weiteres Thema ist bei einem fachlichen Austausch der Unterschied zwischen Datenschutz und Schweigepflicht. Während sich die Schweigepflicht auf anvertraute Geheimnisse bezieht, handelt es sich beim Datenschutz um personenbezogene Daten *(siehe hierzu Kapitel 2.5, insbesondere Kapitel 2.5.3)*. Grundsätzlich ist ein fachlicher Austausch (auch trägerübergreifend) über Beratungssituationen möglich, wenn er anonymisiert erfolgt und nicht nachvollziehbar ist, welche Person die Beratung in Anspruch genommen hat.

4.6 ANLEITUNG VON EHRENAMT UND TEAMER*INNEN

Die hauptamtliche Tätigkeit wird in vielen Fällen durch Ehrenamt oder externe Honorarkräfte unterstützt. Diese müssen die Anforderungen des Datenschutzes gleichermaßen wie die hauptamtlich Beschäftigten beachten. Zusätzlich gilt es, entsprechende Nachweise über die Tauglichkeit der externen Mitarbeiter*innen (z. B. im Rahmen des Tätigkeitsausschlusses nach § 72a SGB VIII, *siehe hierzu Kapitel 1.3*) vorzuhalten.

Grundsätzliche Informationen zum Thema Datenschutz und externe Mitarbeiter*innen sind in *Kapitel 1.4* zusammengefasst. Haben externe Mitarbeiter*innen im Rahmen ihres Vertrags mit der Organisation oder dem Verein auch Aufgaben zu erledigen, die datenschutzrelevant sind, müssen sie bei Aufnahme ihrer Beschäftigung von der Geschäftsführung oder Vereinsleitung umfassend zum Thema Datenschutz innerhalb der Organisation informiert werden. Außerdem sollten sie zur Vertraulichkeit verpflichtet werden, zum Beispiel in Form einer Vertraulichkeitserklärung als Anhang zum Honorarvertrag bzw. zur Ehrenamtsvereinbarung. Auch externe Mitarbeiter*innen und Teamer*innen sollten für dienstliche Zwecke möglichst keine private Technik wie Smartphones, Laptops oder Kameras nutzen *(siehe hierzu Kapitel 1.2 und 5.4)*. Dienstanweisungen haben für externe ebenso wie für festangestellte Mitarbeiter*innen Vorrang vor dieser Handreichung.

Vorlage 8: Datenschutzverpflichtung für ehrenamtlich Tätige und Honorarkräfte
jugend-datenschutz.de/link/08

4.7 ANTRAGS- UND ABRECHNUNGSVERFAHREN

Maßnahmen, die über das Alltagsgeschäft der Jugend- und Jugendverbandsarbeit hinausgehen, werden häufig durch zusätzliche öffentliche Mittel oder Drittmittel finanziert. Hierfür sind dem Zuwendungsgebenden in der Regel entsprechende Nachweise über die tatsächliche Verwendung der Mittel vorzulegen, zum Beispiel in Form von Teilnahmelisten und Fotodokumentation.

Die Weitergabe von personenbezogenen Daten an Fördermittelgebende ist in der Regel eine zulässige Datenverarbeitung, da diese zur Wahrnehmung berechtigter Interessen des Fördermittelnehmenden, also der Organisation oder des Vereins, dient. Bei jeder Übermittlung ist der Grundsatz der Datenminimierung zu beachten. Kann ein Nachweis auch in anonymisierter Form gegenüber dem Fördergebenden erfolgen, so dürfen keine personenbezogenen Daten weitergegeben werden. Die Daten dürfen auch so lange gespeichert werden, bis der Zweck – in diesem Fall das Abrechnungsverfahren und die Prüfung des Verwendungsnachweises – abgeschlossen ist. Gibt es von Seiten des Fördermittelgebenden Fristen, die eine längere Aufbewahrung aufgrund von Dokumentations- und Beweiszwecken erfordern, so sind diese ausschlaggebend. Ein Auftragsverarbeitungsvertrag muss nach aktueller Rechtsauffassung für die Weitergabe von Daten an Fördermittelgebende nicht vorliegen. Dennoch müssen Betroffene vorab über die Datenverarbeitung informiert werden. Informationen zum Prozess der Teilnehmer*innenverwaltung sind in *Kapitel 3.1* zusammengefasst und in *Kapitel 3.11* stehen Hinweise für den Fall der Datenweitergabe an Dritte.

Fallbeispiel:
Für die Durchführung einer Ferienfreizeit stellt der Jugend e. V. einen Antrag auf Mikroprojektförderung beim örtlichen Jugendamt. Entsprechend des Zuwendungsbescheids werden für die Abrechnung die Daten der Teilnehmenden (Name, Anschrift und Geburtsdatum) in einer Liste gesammelt und an das Jugendamt übermittelt. Die Eltern des 12-jährigen Tim möchten wissen, ob das mit der DSGVO vereinbar ist.

05 BESONDERE AUFGABEN

Durch die Umsetzung der Vorgaben und Richtlinien der DSGVO innerhalb von Organisationen ist die Durchführung einiger möglicherweise neuer, besonderer Aufgaben nötig. So müssen unter Umständen ein*e Datenschutzbeauftragte*r benannt, ein Verzeichnis von Verarbeitungstätigkeiten erstellt und gepflegt und bei einer Zusammenarbeit mit externen Dienstleister*innen Datenverarbeitungsverträge geschlossen werden. Intern müssen technische und organisatorische Maßnahmen ergriffen werden und auch das Verhalten bei Datenschutzpannen erfordert eine korrekte Vorgehensweise.

5.1 DATENSCHUTZBEAUFTRAGTE*R

Öffentliche Stellen müssen gemäß Art. 37 DSGVO immer eine*n Datenschutzbeauftragte*n benennen. Vereine, Organisationen und kleine Unternehmen sind gemäß § 38 Bundesdatenschutzgesetz (BDSG) dazu nur verpflichtet, wenn sich mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Dazu zählen beispielsweise der Umgang mit E-Mail-Verteilern, Adresslisten, Mitgliederdateien und Anmeldelisten. Dabei wird nicht zwischen haupt- und ehrenamtlich Tätigen unterschieden. Nehmen der*die Verantwortliche oder der*die Auftragsverarbeiter*in Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung unterliegen oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine*n Datenschutzbeauftragte*n zu benennen.

Die Benennung einer*s externen Datenschutzbeauftragten ist ebenso möglich wie die einer internen, unabhängigen ehren- oder hauptamtlich tätigen Person. Sie muss jedoch immer schriftlich erfolgen und ist dem*der Datenschutzbeauftragten des Bundeslandes, in dem sich der Vereinssitz befindet, namentlich anzugeben.

Vorlage 16:
Benennungsurkunde für interne Datenschutzbeauftragte
jugend-datenschutz.de/link/16

Mit der Benennung sollten immer auch der zeitliche Umfang für die Tätigkeit sowie bereitzustellende Ressourcen geklärt werden. Die Aufgaben des*der Datenschutzbeauftragten brauchen Zeit und können nicht nebenbei erledigt werden.

Die Aufgaben des*der Datenschutzbeauftragten sind klar geregelt:

§ *Art. 39 DSGVO*

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;
- Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
- Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß § 35 DSGVO;
- Zusammenarbeit mit der Aufsichtsbehörde;
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß § 36 DSGVO, und gegebenenfalls Beratung zu allen sonstigen Fragen.

5.2 VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Neben der Sicherstellung einer rechtskonformen Datenverarbeitung muss der*die Verantwortliche diese auch nachweisen können. Dies gelingt mit der Führung eines sogenannten Verzeichnisses der Verarbeitungstätigkeiten. In diesem wird die Erfassung und der Umgang mit personenbezogenen Daten schriftlich dokumentiert und kann bei Bedarf nachvollzogen werden.

Das Verzeichnis soll vor allem zur Erfüllung der Rechenschaftspflichten dienen. Die Auflistung aller Verarbeitungstätigkeiten ermöglicht einen guten Überblick über alle Vorgänge im Verband oder Verein, die im Zusammenhang mit personenbezogen Daten stehen. Dennoch ist es nur ein Baustein, um der in Art. 5 Abs. 2 DSGVO normierten Rechenschaftspflicht zu genügen.

Das Verzeichnis stellt den Ausgangspunkt für die Festlegung und Kenntnis bestehender Datenverarbeitungsvorgänge im Verband oder Verein dar. Es bildet damit die Basis und Grundvoraussetzung, um Vorgaben aus dem Datenschutzrecht überhaupt einhalten zu können.

Art. 30 DSGVO enthält die genauen Vorschriften zum **Verzeichnis von Verarbeitungstätigkeiten**. Folgende Informationen müssen zwingend im Verzeichnis enthalten sein:

Name und Kontakt

des*der Verantwortlichen sowie ggf. der Vertretung

Verarbeitungszweck

zum Beispiel Mitgliederverwaltung, Teilnahme an Seminar, Information per Newsletter

Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten

Welche Daten werden von welchen Personen erhoben? Zum Beispiel: Name und Adresse von Teilnehmenden, Kontodaten von Ehrenamtlichen usw.

Fristen für die Datenlöschung der verschiedenen Datenkategorien

zum Beispiel, wenn sie für die Zwecke nicht mehr erforderlich sind

Beschreibung der technischen und organisatorischen Maßnahmen

gemäß Art. 32 Abs. 1 DSGVO *(siehe hierzu Kapitel 5.4)*

Kategorien von Empfänger*innen der Daten, falls die Daten an Dritte übermittelt werden

zum Beispiel Teilnahmelisten an Fördermittelgebende zur Erfüllung der Fördermittelrichtlinien oder Daten von Mitarbeiter*innen an ein externes Lohnbüro zur Gehaltsabrechnung

Es geht immer um die verschiedenen Kategorien und Verarbeitungstätigkeiten, so dass nicht für jede einzelne Maßnahme oder Ferienfreizeit ein gesondertes Verzeichnis von Verarbeitungstätigkeiten angelegt wird. Pro Zweck der Datenerhebung muss einmalig das gesamte Verfahren dokumentiert werden (zum Beispiel: Mitgliederverwaltung, Anmeldedaten von Teilnehmenden oder Informationsweitergabe via E-Mail-Verteiler).

Vorlage 17: Beispiel für Verzeichnis der Verarbeitungstätigkeiten
jugend-datenschutz.de/link/17

Inzwischen gibt es Muster von Verzeichnissen von Verarbeitungstätigkeiten, auf die sich die Landesdatenschutzbehörden geeinigt haben und die verwendet werden können. Auch das Anlegen einer eigenen Tabelle ist möglich.

5.3 AUFTRAGSVERARBEITUNGSVERTRAG

Praxistipp:
In Fällen, in denen die Weitergabe personenbezogener Daten bei Vorliegen einer entsprechenden Rechtsgrundlage an andere Verantwortliche erfolgt, muss kein Auftragsverarbeitungsvertrag geschlossen werden.

Bei Verträgen des*der Verantwortlichen mit externen Dienstleistenden, die im Auftrag personenbezogene Daten verarbeiten, ist es notwendig, mit diesen einen Auftragsverarbeitungsvertrag zu schließen. Hierzu kann ein Mustervertrag zur Auftragsdatenverarbeitung angepasst und verwendet oder ein eigener Vertrag entwickelt werden. In Art. 28 DSGVO finden sich weitere Details der Regelung zum Thema Auftragsverarbeitung. So dürfen nur Verträge mit Auftragsverarbeitenden geschlossen werden, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen durchgeführt werden.

Vorlage 18: Auftragsverarbeitungsvertrag
jugend-datenschutz.de/link/18

Zudem muss die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgen und den Schutz der Rechte der betroffenen Personen gewährleisten.

5.4 TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

In Art. 24 und Art. 25 DSGVO sind die technischen und organisatorischen Maßnahmen (TOM) aufgeführt. Durch ihren Einsatz sollen Unbefugte daran gehindert werden, Zugriff auf schutzwürdige Daten zu erlangen. Die Dokumentation der technischen und organisatorischen Maßnahmen ist vorgeschrieben und wird im Rahmen des Verzeichnisses von Verarbeitungstätigkeiten durchgeführt *(siehe Kapitel 5.2)*. Im Fall einer Datenschutzpanne können Verantwortliche so gegenüber der Datenschutzbehörde belegen, dass innerhalb der Organisation angemessene Maßnahmen zum Schutz personenbezogener Daten getroffen wurden.

§ *Art. 24 DSGVO*

Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Grundsätzlich gilt: je sensibler die Daten, desto besser muss ihr Schutz durch technische und organisatorische Maßnahmen sein. Nachfolgend werden einige der möglichen Maßnahmen exemplarisch aufgeführt.

Achtung:
Verlassen oder teilen Mitarbeiter*innen einen Arbeitsplatz, sind datenschutzrelevante Unterlagen stets verschlossen abzulegen und die Bildschirmsperre bei technischen Geräten wie PC, Laptop oder Smartphone zu aktivieren. Die Aufhebung der Sperre darf nur durch PIN bzw. Passworteingabe möglich sein.

Praxistipp:
Sichere Passwörter bestehen aus mindestens acht Zeichen und einer Mischung aus Klein- und Großbuchstaben, Zahlen sowie Sonderzeichen. Sie dürfen insbesondere nicht als Notiz in der Nähe des Arbeitsplatzes abgelegt werden.

Zu den etablierten Sicherheits-Standardmaßnahmen am Arbeitsplatz zählen:

Nutzung aktueller Betriebssysteme

regelmäßige Backups

zum Schutz der Daten vor Zerstörung oder Verlust und regelmäßige Überprüfung, ob diese zur Wiederherstellung der Daten geeignet sind und funktionieren

Einsatz von Virenscannern

Aktenablage in abschließbaren Schränken

Arbeit mit Benutzer*innenrechten und keine Doppelverwendung von Useraccounts

Zutrittskontrolle

zu Büros und strikte Trennung von öffentlichen Räumen

Schreddern von Papieren mit personenbezogenen Daten

effektiver Passwortschutz

Praxistipp:
Bei Nutzung von E-Mail-Programmen wie Outlook oder Thunderbird muss eine entsprechende Verschlüsselung (TLS/SSL) zwischen Endgerät und Ausgangsserver eingerichtet werden, falls das nicht vom Programm voreingestellt ist.

Absicherung privater Technik

Wenn private Technik wie zum Beispiel Computer, Laptops, Tablets oder Smartphones verwendet wird, muss nachweislich sichergestellt sein, dass nur berechtigte Personen auf personenbezogene Daten zugreifen können. Dazu zählt auch die Weitergabekontrolle. Dokumente mit personenbezogenen Daten müssen auf sicheren Wegen übermittelt werden. Hier empfiehlt sich die Nutzung von virtuellen privaten Netzwerken (VPN), E-Mail-Verschlüsselung oder Passwortschutz einzelner Dokumente (PDF-Verschlüsselung, ZIP-Verschlüsselung). Auch das Anlegen eines separaten Useraccounts für dienstliche Zwecke kann den Zugriff durch Unbefugte beschränken. Die Weitergabe von mobilen Geräten an Dritte darf niemals unbeaufsichtigt erfolgen.

Diese Aufzählung ist ausdrücklich nicht als vollständig zu verstehen und jede Organisation muss im Rahmen des eigenen Datenschutzkonzeptes die für sich geeigneten und notwendigen technischen und organisatorischen Maßnahmen festlegen. Die Checkliste des Bayerischen Landesamts für Datenschutzaufsicht kann hier als ein Instrument der Selbstüberprüfung genutzt werden und auch als Anlage bei Datenverarbeitungsverträgen und dem Verzeichnis von Verarbeitungstätigkeiten Verwendung finden.

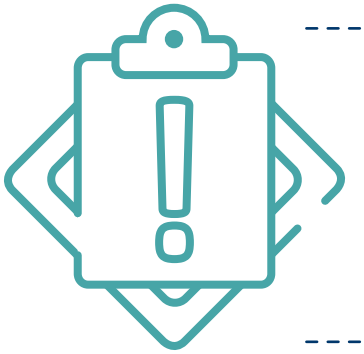
Checkliste technische und organisatorische Maßnahmen (TOM)
jugend-datenschutz.de/link/checkliste-tom

5.5 VERHALTEN BEI DATENSCHUTZPANNEN

Nach Art. 33 DSGVO müssen Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten binnen 72 Stunden, nachdem ihnen diese Verletzung bekannt wurde, den Fall der zuständigen Datenschutzbehörde melden. Die Vorschrift führt auch im Einzelnen auf, welche Angaben hierfür nötig sind. Die betroffenen Personen sind im Falle eines hohen Risikos nach Art. 34 DSGVO ebenfalls zu informieren. Eine Meldung an die Datenschutzbehörde und die Betroffenen ist nicht notwendig, wenn der Vorfall voraussichtlich nicht zu einem Risiko für die betroffenen Personen führt.

Meldeformular von Sachsen
jugend-datenschutz.de/link/meldung

Beispiele für **Datenschutzpannen** sind:



Diebstahl
eines Diensthandys oder -laptops

Verlust
einer Teilnahmeliste mit Namen und Adressen

Hackerattacke
auf eine Datenbank

Praxistipp:
Wenn die Daten auf dem verlorenen oder gestohlenen Gerät gesichert oder verschlüsselt sind, ist der Vorfall nicht meldepflichtig, sofern es Unbefugten dadurch nicht möglich ist, an die Daten zu gelangen.

Innerhalb einer Organisation sollte im Rahmen des Datenschutzkonzeptes ein Prozess festgelegt werden, wie und durch wen solch eine Meldung zu erfolgen hat.

Dokumentation von Datenschutzpannen

In jedem Fall ist auch bei Datenschutzpannen eine Dokumentation notwendig. Gemäß Art. 33 DSGVO dokumentiert der*die Verantwortliche die Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung stehenden Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen der DSGVO.

Achtung:
Beim Verstoß gegen die Datenschutzvorschriften drohen nicht nur die Schädigung des eigenen guten Rufes und finanzielle Konsequenzen durch Betroffene, die möglicherweise Haftungsansprüche geltend machen, sondern auch von Aufsichtsbehörden verhängte Bußgelder. Art. 84 DSGVO besagt, dass Sanktionen wirksam, verhältnismäßig und abschreckend sein müssen. Die maximale Geldbuße beträgt bis zu 20 Millionen Euro oder bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr; je nachdem, welcher Wert der höhere ist.

SCHLAGWORTVERZEICHNIS

A

Anmeldeformular . . . . . S. 20f, 31, **33**

Aufbewahrungspflicht . . S. 12, 15, 23

Auftragsverarbeitungsvertrag . . . . . S. 25, 31, 35, 37, **40**

B

Beratung / Einzelfallhilfe . . . . . S. 14, **32f**, 36, 39

C

Cloud-Speicher . . . . . S. **24f**

D

Datenschutzbeauftragte . . . . . S. 07, 11, 20, **38f**

Datenschutzerklärung . . . . . S. 29, **30**

Datenschutzkonzept . . . . . S. **06**, 42

Datenschutzpanne . . . . S. 38, 41, **42f**

Datenweitergabe . . . . . S. **31**, 33, 37

Dienstberatung . . . . . S. 35

E

E-Mail . . . . . S. 08, 13, **22**, 33, 35

Ehrenamt . . . . . S. 07, 09, **10**, **36**

Einwilligungserklärung . . . . . S. **18**, 26

F

Facebook . . . . . S. 12, **29f**, 33

Ferienfreizeit . . . . . S. 21, **31**, 35

Fördermittelgebende. . . . . S. **37**, 40

Fotoerlaubnis . . . . . S. 33

Fotos . . . . . S. 09, **25ff**, 31, 33f

Führungszeugnis . . . . . S. **09f**

G

Gruppenarbeit . . . . . S. **35**

Gruppenfahrt . . . . . S. 35

H

Handy . . . . . S. **23**, 42

Honorarverträge . . . . . S. **10**, 33, 36

I

Informationspflicht . . S. **20f**, 24, 26, 32

Instagram . . . . . S. 27, **29f**

J

Jugendbildung . . . . . S. **33**

K

Kirche . . . . . S. **11**, 35

M

Messenger . . . . . S. **27f**, 32, 35

Mitarbeiter*innen . . . . . S. **06ff**, 10, 36

Mitglieder . . . . . S. **21f**

N

Netzwerkarbeit . . . . . S. **35**

O

Offene Angebote . . . . . S. 34

P

Personenbezogene Daten . . . . . S. 07ff, **13**, 15f, 20

Presseverteiler . . . . . S. 22

S

Schweigepflicht . . . . . S. **16ff**, 32f, 36

Seminar . . . . . S. 33, 35, 40

Sensible Daten . . . . . S. **13**, 21

Signal . . . . . S. **28**

Smartphone . . . . . S. 08, **23**, 42

SMS . . . . . S. **23**, 32, 35

T

Teamer*in . . . . . S. **36**

Technische und organisatorische Maßnahmen (TOM) . . . . . S. 16, 21, 30, 38, **40f**

Teilnahmelisten. . . . . S. **20f**, 35, 37

Telefon . . . . . S. 08, 13, **23f**, 27f, 32

Threema . . . . . S. **27**

V

Veranstaltungen . . . . . S. **31f**, 34ff

Verantwortliche . . . . . S. **06ff,** 12, 20f, 25f, 38ff

Verwendungsnachweis . . . . . S. 20, 33

Verzeichnis von Verarbeitungstätigkeiten . . . . . S. 14, 16, **39f**, 42

Video . . . . . S. 13, **25ff**

W

Website . . . . . S. 26, 29, **30**, 35

WhatsApp . . . . . S. **27f**, 32, 35

Workshops . . . . . S. 33, 35f

NOTIZEN

IMPRESSUM

1. Auflage, 2024

Herausgebende

Kinder- und Jugendring Sachsen e. V.
Saydaer Straße 3, 01257 Dresden
Ansprechpartner: Jürgen Bahr
Tel. 0351 316790
info@kjrs.de
www.kjrs.de

Arbeitsgemeinschaft Jugendfreizeitstätten Sachsen e. V.
Neefestraße 82, 09119 Chemnitz
Ansprechpartnerin: Karen Pethke
Tel. 0371 533640
info@agjf-sachsen.de
www.agjf-sachsen.de

Gefördert durch

Sächsisches Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt

Redaktion

Jürgen Bahr (KJRS e. V.)
Karen Pethke (AGJF Sachsen e. V.)
Robert Harzewski (Rechtsanwaltskanzlei Harzewski)

Rechtliche Prüfung

Diese Arbeitshilfe basiert in weiten Teilen auf der Broschüre „Datenschutz in der Jugendarbeit“, herausgegeben 2019 vom Fachverband Jugendarbeit / Jugendsozialarbeit Brandenburg e. V. und dem Landesjugendring Brandenburg e. V.
Diese wurde rechtlich geprüft von:
Rechtsanwaltskanzlei Cornelius Matutis, Rechtsanwältin Felicitas Warncke
www.anwalt-für-datenschutz.eu

Die Änderungen in der vorliegenden Fassung wurden geprüft von:
Rechtsanwaltskanzlei Harzewski, Rechtsanwalt Robert Harzewski
www.rechtsanwalt-harzewski.de

Layout

Layout in Anlehnung an o. g. Broschüre aus 2019, Originallayout:
Agentur Medienlabor
www.agentur-medienlabor.de

Druck

dieUmweltdruckerei
www.dieUmweltDruckerei.de

Bildnachweise

Titelseite ©Roman Amanov und Icons8 via Canva.com

Mehr Informationen **www.jugend-datenschutz.de**

ÜBER DIESE HANDREICHUNG:

Datenschutz ist durch die seit 2018 gültige Datenschutz-Grundverordnung (DSGVO) inzwischen im Alltag der Jugend- und Jugendverbandsarbeit angekommen. Auch wenn es nicht unbedingt das Lieblingsthema von Fach- und Führungskräften ist, hat der Datenschutz jedoch ein gutes Anliegen, dem sich die Soziale Arbeit schon aus ihrer Berufsethik heraus verpflichtet fühlt: den Schutz der eigenen Daten im Lebensalltag gewährleisten. Diese Handreichung erläutert daher nicht nur die wichtigsten Herausforderungen, sondern gibt vor allem auch praxistaugliche Hinweise und Formulierungshilfen für eine gelungene Umsetzung des Datenschutzes in der Jugend- und Jugendverbandsarbeit.

www.jugend-datenschutz.de

Herausgebende:

KINDER & JUGEND RING SACHSEN
Arbeitsgemeinschaft der Jugendverbände in Sachsen

agjf Arbeitsgemeinschaft Jugendfreizeitstätten Sachsen e.V.

Gefördert durch:

SACHSEN
Diese Maßnahme wird mitfinanziert durch Steuermittel auf der Grundlage des vom Sächsischen Landtag beschlossenen Haushaltes.