DIE DSGVO
DATENSCHUTZ IN DER JUGENDARBEIT

VORWORT

Datenschutz ist für viele zu einer Art Unwort des Jahres 2018 geworden. Gerade in Vereinen und kleineren Betrieben war die Verunsicherung im Kontext der europäischen Datenschutz-Grundverordnung (DSGVO) groß. Mit dem Stichtag am 25. Mai 2018 gingen zahlreiche Internetauftritte offline, Newsletter-Verteiler wurden auf „Null“ gesetzt und Messenger-Dienste wie WhatsApp aus dem Berufsleben verbannt. Das überaus wünschenswerte Ziel, persönliche Daten in einer zunehmend digitalisierten Gesellschaft zu schützen, wurde insbesondere für Träger der Jugendhilfe zu einem Kraftakt, der die Errungenschaften der DSGVO in den Schatten stellte.

Als Dachverband der freien und kommunalen Träger der Jugend(sozial)arbeit sowie als Zusammenschluss der Jugendverbände erarbeiteten der Fachverband Jugendarbeit / Jugendsozialarbeit Brandenburg e. V. und der Landesjugendring Brandenburg e. V. eine gemeinsame Handreichung, um praxistaugliche Empfehlungen für einen verantwortungsbewussten Umgang mit Daten in der Jugend- und Jugendverbandsarbeit zu ermöglichen.

Mit dieser Handreichung soll es gelingen, Datenschutz wieder positiv zu besetzen. Die Vorgaben, die Personen zuallererst vor der unkontrollierten Datenspeicherung bei Großkonzernen schützen sollten, sind nach deutschem Recht auch von gemeinnützigen Institutionen einzuhalten. Daher richtet sich der erste Teil besonders an Trägerverantwortliche wie Vorstände bzw. Geschäftsführungen, da der entscheidende Schritt zur Implementierung von Datenschutzprozessen von ihnen ausgeht. Die weiteren Ausführungen zu den Datenverarbeitungen in der Jugendarbeitspraxis sollen den Fachkräften Handlungssicherheit in ständig wiederkehrenden Situationen verleihen. Und 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“.

Datenschutz erfordert Zeit – vor allem, wenn grundlegende Prinzipien im gesamten Träger verankert werden sollen. Einen solchen Zeitaufwand kann auch die vorliegende Handreichung nicht mindern. Sie bietet jedoch einen Überblick über relevante Prozesse und Alltagssituationen der Jugendarbeit, 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 die Rechtsanwaltskanzlei Cornelius Matutis bietet diese Handreichung jedoch nach aktueller Rechtsauffassung taugliche Vorschläge für den Einsatz in der Jugendarbeit.

Wir hoffen, dass diese Broschüre eine Bereicherung für Ihre Bemühungen darstellt. Wir wünschen Ihnen viel Freude bei der Arbeit mit den Kindern und Jugendlichen im Land Brandenburg.

Silke Hansen
Vorstandssprecherin
Landesjugendring Brandenburg e. V.

Thomas Lettow
Vorstandsvorsitzender
Fachverband Jugendarbeit / Jugendsozialarbeit Brandenburg e. V.

ljr landesjugendring brandenburg

FACHVERBAND Jugendarbeit / Jugendsozialarbeit Brandenburg e. V.

INHALT

03

Datenverarbeitung in der Jugendarbeit

04

Praxissituationen in der Jugendarbeit

05

Besondere Aufgaben

01 DATENSCHUTZ IN DER ORGANISATION

Datenschutz ist nicht nur in den Medien präsent. Auch innerhalb von Einrichtungen und Organisationen kommen Beschäftigte bewusst oder unbewusst immer wieder mit dem Thema Datenschutz in Berührung. Sobald in einer beruflichen Situation beispielsweise ein Name mit Telefonnummer auf einem Zettel notiert wird, 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 alle Organisationen, Vereine oder Unternehmen selbst – und damit deren Leitung, Vorstand oder Geschäftsführung. Gemäß DSGVO gibt es immer eine*n Verantwortliche*n zum Thema Datenschutz:

§ *Art. 4 Abs. 7 DSGVO*
„Verantwortliche*r“ 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 Mitarbeitende. Verantwortliche haben die Pflicht, sich mit den datenschutzrelevanten Vorschriften zu beschäftigen, mit dem Datenschutzrecht auseinanderzusetzen und ein entsprechendes Datenschutzkonzept für die Organisation zu erarbeiten.

Datenschutzkonzept

In jeder Einrichtung und Organisation sollten Regeln und Prozesse zum Umgang mit personenbezogenen Daten in Form eines Datenschutzkonzeptes aufgestellt und kommuniziert werden. Es gilt herauszufinden, welche Arbeitsbereiche betroffen sind und welche Bereiche überhaupt keine personenbezogenen Daten verarbeiten. Praktisch stellt sich für viele Angestellte die Frage: Welche Rolle habe ich, beispielsweise als Sozialarbeiter*in, und welche Regeln muss ich beachten? Die Mitarbeitenden sollten am besten schriftlich über den Datenschutz in der Organisation informiert werden.

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, gilt es immer, diese an die spezifischen Voraussetzungen und individuellen Rahmenbedingungen der eigenen Organisation anzupassen.

1.1 DATENSCHUTZ IST AUFGABE DER LEITUNG

Datenschutz ist Leitungsaufgabe und nicht ohne Aufwand umsetzbar. Das muss der Geschäftsführung oder dem Vorstand bewusst sein oder bewusst gemacht werden. Die erste Information, Schulung und Sensibilisierung der Mitarbeitenden zum Thema Datenschutz sollte von der*dem „Verantwortlichen", also von der Geschäftsführung, ausgehen. Wenn nicht mindestens zehn Mitarbeitende (gemeint sind ausdrücklich sowohl hauptamtliche als auch ehrenamtliche Mitarbeitende) Zugriff auf personenbezogene Daten haben, ist die Benennung einer*s Datenschutzbeauftragten nicht nötig *(siehe hierzu Kapitel 5.1)*. Umso wichtiger ist es, dass die Geschäftsführung oder Vereinsleitung als Verantwortliche*r erste Ansprechperson für die Mitarbeitenden 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)*.

Umgang mit personenbezogenen Daten auf Weisung

Die Geschäftsführung kann den Datenschutz betreffende Aufgaben an Mitarbeitende übertragen, indem sie zum Beispiel als Tätigkeitsbeschreibung im Arbeitsvertrag formuliert werden. Auch externe Dienstleistende dürfen auf Weisung der*des Verantwortlichen mit personenbezogenen Daten umgehen *(siehe Kapitel 5.3)*. Sie werden in der DSGVO als Auftragsverarbeiter*in bezeichnet. Dies kann zum Beispiel das Versandunternehmen sein, das einen Datensatz mit Adressen der Vereinsmitglieder zum Versand von Infopost erhält, oder auch die*der Teamer*in, die personenbezogene Daten der Teilnehmenden zugeschickt bekommt.

Achtung:
In Art. 29 DSGVO und Art. 32 DSGVO ist geregelt, dass der*dem Verantwortlichen und der*dem Auftragsverarbeitenden unterstellte Mitarbeitende personenbezogene Daten nur nach deren Weisung verarbeiten dürfen. Art. 5 DSGVO legt die Grundsätze für die Verarbeitung von personenbezogenen Daten fest. Die*der Verantwortliche muss die Einhaltung dieser Grundsätze nachweisen können *(siehe hierzu die Kapitel 2.3 und 2.4)*.

1.2 DATENSCHUTZ ALS TOP-DOWN-STRATEGIE

Alle festangestellten Mitarbeitenden, die mit personenbezogenen Daten umgehen, müssen bei Aufnahme ihrer Beschäftigung von der Geschäftsführung oder Vereinsleitung umfassend zum Thema Datenschutz innerhalb der Organisation informiert werden. Eine Neubelehrung von Bestandsmitarbeitenden nach dem Inkrafttreten der DSGVO im Mai 2018 zum Thema Datenschutz ist empfehlenswert. So können Arbeitgeber auch dokumentieren, dass sie sich bemühen, die DSGVO intern umzusetzen. Es empfiehlt sich, Mitarbeitende, zum Beispiel durch die Unterzeichnung eines entsprechenden Papiers, zu verpflichten, dass die Verarbeitung personenbezogener Daten gemäß der DSGVO und den intern vereinbarten Richtlinien erfolgt. Verantwortliche haben ihre Mitarbeitenden 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 Mitarbeitende 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 Mitarbeitende 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 Mitarbeitende auch beim Thema DSGVO Vorrang vor dieser Handreichung. Sie kann nur Hilfestellung und Orien-tierung bieten.

1.3 UMGANG MIT DATEN VON MITARBEITENDEN

Arbeitgeber müssen beim Umgang mit den Daten ihrer Mitarbeitenden ebenfalls die Regelungen der DSGVO beachten. So dürfen personenbezogene Daten für Zwecke des Beschäftigungsverhältnisses gemäß § 26 Bundesdatenschutzgesetz (BDSG) und Art. 6 DSGVO aus bestimmten Gründen verarbeitet werden.

§ *§ 26 Bundesdatenschutzgesetz (BDSG)*
Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung […] erforderlich ist.

Wenn keine in einer Rechtsvorschrift oder Betriebsvereinbarung genannten Gründe die Nutzung der Daten erlauben, dürfen personenbezogene Daten von Beschäftigten gemäß § 26 Abs. 2 Bundesdatenschutzgesetz (BDSG) nur mit freiwilliger schriftlicher Einwilligung der*des Betroffenen verarbeitet werden. Da die Informationspflicht ab dem Zeitpunkt der Datenerhebung gilt, sind die Mitarbeitenden bei ihrer Einstellung darüber zu informieren, zu welchen Zwecken Daten von ihnen erhoben werden, wer diese Daten erhält und welche Betroffenenrechte sie haben.

Veröffentlichung im Internet

Die Veröffentlichung von Daten der Mitarbeitenden, zum Beispiel auf der Webseite 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 Telemediengesetz (TMG) zwingend erforderlich.

Handelt es sich nicht um Funktionsträger*innen bzw. ist die Veröffentlichung von zusätzlichen Daten wie Geburtsdatum oder Berufsabschluss beabsichtigt, ist vorab die Einwilligung der*des Beschäftigten einzuholen.

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

Fotos dürfen gemäß § 22 Kunsturhebergesetz (KunstUrhG) nur mit Einwilligung der*des Abgebildeten veröffentlicht werden und müssen nach dem Ausscheiden von Mitarbeitenden unverzüglich gelöscht werden. Fotos, die keinen auf die individuelle Person Bezug nehmenden Inhalt transportieren, dürfen nach einer Einzelfallprüfung ohne Einwilligung veröffentlicht werden.

www.gesetze-im-internet.de/kunsturhg/__22.html

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

www.gesetze-im-internet.de/sgb_8/__72a.html

www.gesetze-im-internet.de/bzrg/__30a.html

Hauptanwendungsfall des § 30a Bundeszentralregistergesetzes (BZRG) ist nach der Intention des Gesetzgebers die Vorlagepflicht nach § 72a Sozialgesetzbuch (SGB) Achtes Buch (VIII) für Beschäftigte bei öffentlichen und freien Trägern der Jugendhilfe.

§ 72a Sozialgesetzbuch (SGB) Achtes Buch (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, 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. Auch die Träger der öffentlichen Jugendhilfe sollen durch Vereinbarungen mit den **Trägern der freien Jugendhilfe** sicherstellen, dass diese keine Person, die wegen einer Straftat nach Abs. 1 Satz 1 rechtskräftig verurteilt worden ist, beschäftigen.

Archivierung nicht erlaubt

Dem Arbeitgeber ist es nicht erlaubt, das Führungszeugnis selbst zu archivieren. Gemäß § 72a Sozialgesetzbuch (SGB) Achtes Buch (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 Straftat nach Abs. 1 Satz 1 rechtskräftig verurteilt worden ist.

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

Praxistipp:
Eine entsprechende Formulierung am Ende der Erklärung könnte lauten:

„Mit der Unterschrift des Honorarvertrages bestätigen Sie, über die Verpflichtung zur Einhaltung der EU-Datenschutz-Grundverordnung informiert worden zu sein. Sie verpflichten sich zur Einhaltung der o. g. Grundsätze, zur Vertraulichkeit und zur Wahrung des Datengeheimnisses hinsichtlich aller Ihnen in Ausführung Ihrer Tätigkeit bei [Arbeitsstätte einfügen] bekannt gewordenen personenbezogenen Daten. Diese Verpflichtung besteht umfassend und hat auch über die Dauer Ihrer Tätigkeit hinaus Bestand.“

1.4 EXTERNE MITARBEITENDE UND HONORARVERTRÄGE

Die Erstellung von Honorarverträgen für externe Mitarbeitende stellt Organisationen und Vereine hinsichtlich des Datenschutzes regelmäßig vor eine Herausforderung.

Neben den hauptberuflichen Mitarbeitenden 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 Mitarbeitende 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 – zum Beispiel für die Organisation einer Ferienfreizeit. Außerdem müssen sie die Daten löschen, wenn der Zweck oder die rechtliche Grundlage nicht mehr besteht und wenn die betroffene Person es fordert – sofern gesetzliche Vorschriften dem nicht entgegenstehen.

Ebenso wie bei hauptamtlichen Mitarbeitenden müssen Arbeitgeber beim Umgang mit den Daten ihrer ehrenamtlich Tätigen und Honorarkräfte die Regelungen der DSGVO beachten und öffentliche und freie Träger der Jugendhilfe sich bei deren Einstellung ein erweitertes Führungszeugnis vorlegen lassen *(siehe hierzu Kapitel 1.3)*.

DSGVO KURZ ERKLÄRT

02

Die DSGVO gilt seit dem 25. Mai 2018 in der gesamten Europäischen Union. 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.

https://dsgvo-gesetz.de/

Die DSGVO geht uns alle an

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

§ *Art. 2 Abs. 2c DSGVO*
Die DSGVO findet keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich **persönlicher oder familiärer Tätigkeiten**.

Übrigens:
„Natürliche Person“ ist ein Rechtsbegriff, der in Gesetzen verwendet wird, und mit dem der Mensch als Träger von Rechten und Pflichten bezeichnet wird. Das Gegenteil ist die juristische Person, mit der man Körperschaften, Vereine und Gesellschaften bezeichnet.

Deutsche und brandenburgische Gesetze, die der DSGVO widersprechen, wurden bzw. werden inzwischen angepasst. Sofern es innerhalb der DSGVO Spielräume gibt, können diese durch nationale Gesetze ausgefüllt werden. Die beiden für Brandenburg wichtigsten sind das Bundesdatenschutzgesetz (BDSG) und das Brandenburgische Datenschutzgesetz (BbgDSG).

http://www.gesetze-im-internet.de/bdsg_2018/

https://bravors.brandenburg.de/gesetze/bbgdsg

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.

https://www.kirchenrecht-ekd.de/document/41335

https://www.datenschutz-kirche.de/sites/default/files/file/NEU/Rechtliches/KDG/KDG_Fassung_des_Beschlusses_der_VV_vom_20_11_2017_korr2.pdf

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. Dabei ist sie übrigens kein neues Recht, sondern sorgt dafür, dass bereits geltendes Recht angewandt wird. 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 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 zu allgemein gehalten sind oder weil andere betroffene Gesetze, zum Beispiel das Kunsturhebergesetz beim Thema Fotografie, noch nicht entsprechend der DSGVO geändert wurden. Diese Unklarheiten werden erst in den kommenden Jahren, zum Beispiel durch Gerichtsurteile, ausgeräumt. Hier sind Änderungen und Konkretisierungen zu erwarten.

Auskünfte erteilen und „Recht auf Vergessenwerden“

Wichtig ist es, jederzeit Auskunft darüber geben zu können, welche Daten von welcher 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 sechsjährige Aufbewahrungspflicht bei Lohnkonten) entgegenstehen.

Dieses „Recht auf Vergessenwerden“ ist insbesondere wichtig in Fällen,

§ *Erwägungsgrund 65 DSGVO*
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:

- **Name**
- **Geburtsdatum**
- **Anschrift**
- **private Telefon- und Handynummer**
- **private E-Mail-Adresse**
- **Ausbildung und Qualifikationen**
- **Beruf**
- **Aufzeichnungen über Arbeitszeiten von Mitarbeitenden**
- **Kontoverbindungen**
- **Datum des Eintritts in Vereine**
- **Mitgliedschaft in Organisationen**
- **Teilnahme an Ferienfreizeiten**
- **Platzierungen bei Wettbewerben**
- **persönliche Interessen**
- **Lebensgeschichte**
- **Beziehungen, Familienstand und Kinder**
- **Bilder, Fotos und Videos**

Sensible Daten

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

- **Nationale oder ethische Herkunft**
- **Politische Meinungen**
- **Religiöse oder weltanschauliche Überzeugungen**
- **Gewerkschaftszugehörigkeit**
- **Genetische Daten**
- **Biometrische Daten**
- **Gesundheitsdaten**
- **Daten zum Sexualleben oder der sexuellen Orientierung**

§ *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

Mit dem Umgang von 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.

Übrigens:
Daten ohne Personenbezug, zum Beispiel anonymisierte Daten, sind datenschutzrechtlich nicht relevant!

2.3 GRUNDSÄTZE DER DATENVERARBEITUNG

Für die Verarbeitung personenbezogener Daten sieht die DSGVO in Art. 5 Abs. 1 sechs Grundsätze vor, die eingehalten werden müssen, und im Folgenden aufgeführt werden. Dabei spielt es keine Rolle, ob die Daten digital oder in 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*r, die*der Daten verarbeitet, muss die sechs Grundsätze aus Art. 5 Abs. 1 DSGVO nicht nur einhalten, sondern sie auch nachweisen können. Diese sogenannte Rechenschaftspflicht wird in *Kapitel 2.4* genau-er beschrieben und kann zum Beispiel durch das Verzeichnis von Ver-arbeitungstätigkeiten 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 sechsjährige Aufbewahrungspflicht von Lohnkonten und die Verarbeitung von Krankenstandsdaten der Mitarbeitenden;
- **Schutz lebenswichtiger Interessen** der betroffenen Person oder einer anderen natürlichen Person;
- **Öffentliches Interesse** oder Ausübung öffentlicher Gewalt;
- **Wahrung berechtigter Interessen:** Hier ist davon auszugehen, dass auch für Einrichtungen der Jugendarbeit ein Mindestmaß an Datenverarbeitung für den reibungslosen Ablauf im Alltag unerlässlich ist. So müssen Daten im Rahmen von Projekten, Dokumentationen, Teambesprechungen oder auch für den Kontakt zu ehrenamtlich Tätigen verarbeitet werden.

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

Achtung:
Wichtig ist beim Kriterium der berechtigten Interessen, dass diese die Interessen oder Grundrechte der betroffenen Person nicht überwiegen dürfen und bei Kindern und Jugendlichen ein besonders strenger Maßstab gilt.

Einwilligung am besten schriftlich einholen

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** gemäß Art. 6 Abs. 1 DSGVO eingeholt werden. Im Idealfall erfolgt diese Einwilligung schriftlich und wird dokumentiert. Dafür gibt es aber keine Vorschriften, denn sie darf auch durch eine eindeutige bestätigende Handlung oder mündlich erfolgen. Das ist in der Praxis nicht empfehlenswert, da hier die Nachweisbarkeit fehlt.

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.

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, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich löschen oder berichtigen zu können.

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 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 hier hilfreichen Verzeichnis von Verarbeitungstätigkeiten.

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

Praxistipp:
Die Behörde wird genau bezeichnen, welche Vorgänge sie vorgelegt bekommen möchte, und dann sollte man ihr auch nur diesen Einzelfall, aber nicht die gesamte DSGVO-Dokumentation vorlegen.

2.5 VERTRAUENSSCHUTZ, DATENSCHUTZ UND SCHWEIGEPFLICHT IN DER JUGENDARBEIT

In der Jugendarbeit 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 und eine zweite Meinung einholen zu können. Insbesondere, wenn es um den Verdacht der Kindeswohlgefährdung gemäß § 8a Sozialgesetzbuch (SGB) Achtes Buch (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

Unter **Schweigepflicht** versteht man die Verletzung von Privatgeheimnissen und diese richtet sich an natürliche Personen. In § 203 Abs. 1 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 arbeitsrechtliche Konsequenzen.

Erlaubte Weitergabe von Geheimnissen

Die Weitergabe von anonymisierten Geheimnissen ohne Bezug zu einer bestimmten Person ist erlaubt. Kann trotz Anonymisierung ein Rückschluss auf die Person gezogen werden, was in kleinen Einrichtungen schnell der Fall ist, darf das Geheimnis nicht ohne Erlaubnis weitergegeben werden.

Übrigens:
Berufstätige, die der Schweigepflicht unterliegen, sind in ihrer Freizeit nicht schweigepflichtig, auch wenn ihnen dann Geheimnisse anvertraut werden. In solch einem Fall sollte die Fachkraft aber darauf hinweisen, dass sie gerade nicht arbeitet.

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

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 Sorgeberechtigten 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.

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 (BSDG) und das Brandenburgische Datenschutzgesetz (BbgDSG). Während sich die **Schweigepflicht** auf anvertraute Geheimnisse bezieht, handelt es sich beim Datenschutz um erhobene Daten.

2.5.4 RECHTFERTIGENDER NOTSTAND UND ZEUGNISVERWEIGERUNGSRECHT

Manchmal ist es notwendig, gegen geltendes Recht, wie die Schweigepflicht, zu verstoßen, um Gefahren von sich oder Dritten abzuwenden:

> *§ 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 Strafgesetzbuch (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 Schweigepflichtsverletzung in der praktischen Jugendarbeit eher selten mit dem rechtfertigenden Notstand begründet werden kann.

Zeugnisverweigerungsrecht

Vor Gericht darf unter bestimmten Umständen die Aussage verweigert werden. Auf dieses sogenannte Zeugnisverweigerungsrecht kann man sich sowohl aus privaten Gründen, weil man beispielsweise ein*e nahe*r Angehörige*r einer*eines Beschuldigten ist, als auch aus beruflichen Gründen berufen.

Gleichzeitig gibt es gesetzliche Regelungen, die zur Offenlegung von Geheimnissen oder persönlichen Daten verpflichten. Diese können auch in der Jugendarbeit relevant werden, da diese Pflichten zum Beispiel der Schweigepflicht vorgehen. An dieser Stelle sind die Anzeigepflicht und das Informationsrecht der Personensorgeberechtigten zu nennen.

2.5.5 ANZEIGEPFLICHT UND AUSKUNFTSPFLICHT

Nach § 138 Strafgesetzbuch (StGB) müssen bestimmte, dort aufgeführte geplante Straftaten wie Mord, Hoch- und Landesverrat und Raub angezeigt werden, wenn man Kenntnis von ihnen erlangt. Nicht von der Anzeigepflicht betroffen sind jedoch Straftaten, die in der Vergangenheit liegen oder auch Körperverletzungsdelikte, Betäubungsmittelstraftaten und Straftaten gegen die sexuelle Selbstbestimmung.

Auskunftspflicht

Bei Kindern und Jugendlichen besteht grundsätzlich ein sogenanntes Informationsrecht der Personensorgeberechtigten. Gleichzeitig gilt die Schweigepflicht nach § 203 Strafgesetzbuch (StGB) grundsätzlich auch für Geheimnisse von Kindern und Jugendlichen im Verhältnis zu ihren Eltern. Dieses Spannungsverhältnis gilt es im Einzelfall auszuloten.

So sind Fälle denkbar, in denen eine Information der Eltern über die einer Fachkraft anvertrauten Probleme bei den Personensorgeberechtigten zu Reaktionen führen würde, die aus pädagogischen Gründen nicht verantwortet werden können. Die Fachkraft würde durch die Information der Eltern 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 der*des betroffenen Jugendlichen, ihre*seine familiären und sonstigen persönlichen Beziehungen, die Art und die Intensität des speziellen Problems. Auch die Art und Weise, mit der die Familie auf die*den Jugendliche*n 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 Informationspflicht gegenüber den Eltern bestehen. Normalerweise gilt aber für Fachkräfte die Pflicht, Eltern über die ihnen bei der Berufstätigkeit bekannt gewordenen Probleme von Kindern und Jugendlichen zu informieren.

03 DATENVERARBEITUNG IN DER JUGENDARBEIT

Zwischen Jugendarbeit und Datenschutz gibt es viele Berührungspunkte und aufgrund der einzuhaltenden Regelungen der DSGVO sind zahlreiche Maßnahmen zu treffen. Da die DSGVO nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person gilt, sind diese (dienstlichen) Daten davon unberührt und nicht Teil der nachfolgenden Ausführungen.

Im folgenden Kapitel werden einige für die Jugendarbeit typische Prozesse dargestellt und dazu praktische Hinweise zum jeweiligen Umgang mit den personenbezogenen Daten geliefert.

3.1 TEILNEHMENDENVERWALTUNG UND STATISTIK

In der Jugendarbeit 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 Teilnehmenden, 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 der*des Verantwortlichen, gegebe-nenfalls auch der*des Datenschutzbeauftragten;
- die Zwecke und die Rechtsgrundlage für die Verarbeitung;
- die berechtigten Interessen (gemäß Art. 6 Abs. 1 Buchstabe f DSGVO, sofern die Verarbeitung darauf beruht);
- gegebenenfalls die Empfänger*innen oder Kategorien von Empfänger*innen der personenbezogenen Daten (zum Beispiel Dachverbände, Kooperationspartner*innen, Fördergeldgebende, 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 Rechten der Betroffenen (das Recht auf Auskunft, Berichtigung, Löschung, des Widerspruchsrechts sowie das Recht auf Datenübertragbarkeit und Einschränkung der Verarbeitung gemäß Artikel 18 DSGVO);

- jederzeitiges Widerrufsrecht der Einwilligung (wenn die Verarbeitung auf Art. 6 Abs. 1 Buchstabe a oder Art. 9 Abs. 2 Buchstabe 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 jeder 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. Besonders die Angabe des Zweckes sollte äußerst sorgfältig überlegt sein, um bei Bedarf eine längere Aufbewahrung der Daten – zum Beispiel, um der von Fördermittelgebenden oft geforderten Dokumentationspflicht nachzukommen – gewährleisten zu können. Bei der Weitergabe von personenbezogenen Daten an Fördermittelgebende handelt es sich übrigens in der Regel um eine zulässige Datenverarbeitung, da sie im Rahmen der Wahrnehmung berechtigter Interessen des Vereins, nämlich der Vereinsförderung, erfolgt *(siehe hier-zu auch Kapitel 3.11)*.

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 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 vor dem Zugriff Unbefugter geschützt 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)*.

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 sie*er 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 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 Mitgliedschafts-Vertrag 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 Antragsformula-re 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 Auftragsverarbeitende 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. E-Mails enthalten meistens personenbezogene Daten und umfassen technisch gesehen eine Nachricht und eventuell beigefügte Dateianhänge. Als Meta-Informationen werden die Adressen der Absender*innen und Empfänger*innen, das Datum und der Betreff der Nachricht gesendet. Laptops und PCs sind wie alle zur dienstlichen Kommunikation und Datenverwaltung genutzten technischen Geräte vor dem Zugriff von Unbefugten zu schützen. Dazu müssen sichere Passwörter gewählt werden und diese dürfen nur der*dem Benutzer*in bekannt sein. Dasselbe gilt für die Zugangsdaten von E-Mail-Konten *(siehe hierzu auch 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 im BCC-Feld eintragen, sodass diese nicht sehen, wer die E-Mail außer ihnen selbst noch erhalten hat. Der Versand muss verschlüsselt erfolgen *(siehe hierzu Kapitel 5.4)*.

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 – falls diese nicht vorliegt – 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:

Zur Erfüllung eines Vertrags

Zur Erfüllung einer gesetzlichen Verpflichtung

Interessenabwägung:

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

Tipp:
In Fällen, bei denen es sich um öffentlich zugängliche E-Mail-adressen handelt, kommt die Interessenabwägung deutlich einfacher zu dem gewünschten Ergebnis der Zulässigkeit, da die*der Betroffene die Daten ja schon selbst veröffentlicht hat als in solchen Fällen, in denen dies gerade nicht der Fall ist. Dort müssen die Grundrechte der Betroffenen intensiver einbezogen und abgewogen werden.

Für eine nichtkommerzielle Kommunikation ist in der Regel keine Einwilligung erforderlich, sofern diese keine Belästigung gemäß § 7 Gesetz gegen den unlauteren Wettbewerb (UWG) darstellt und auch nicht nach Art. 21 Abs. 1 oder 2 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.

https://www.gesetze-im-internet.de/ hgb/__257.html

https://www.gesetze-im-internet.de/ ao_1977/__147.html

3.4 SMS UND TELEFON

Handys und Smartphones sind aus unserem 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 unberechtigtem Zugriff Dritter, zum Beispiel durch eine PIN, die nur der*dem 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 end-to-end-Verschlüsselung gibt. Daher können Daten auf dem Weg zur*zum 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. Im Zuge dessen kann man das Einverständnis der Person für diese Datenverarbeitung einholen und sollte dies dann auch im Anschluss kurz dokumentieren.

Gibt eine Person jedoch unaufgefordert personenbezogene Daten über sich preis und werden (zum Beispiel im weiteren Verlauf des Gesprächs) keine personenbezogenen Daten selbst aktiv beschafft, handelt es sich grundsätzlich nicht um eine Erhebung bzw. verfügt die betroffene Person aufgrund der Umstände möglicherweise bereits über die Information. In diesen Fällen besteht dem Grunde nach keine Informationspflicht nach Art. 13 DSGVO.

3.5 DATENSPEICHER

Werden Daten auf einem mobilen Datenträger wie einem USB-Stick, einer externen Festplatte oder einer DVD/CD gespeichert, sollte der entsprechende Datenträger zum Schutz vor dem Zugriff unberechtigter Personen vor Verlust und Diebstahl gesichert sein, nicht unnötig mitgenommen werden und nur für einen bestimmten Zweck außerhalb eines sicheren Ortes am Arbeitsplatz aufbewahrt werden.

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.

https://www.veracrypt.fr/en/Home.html

https://www.pc-magazin.de/ratgeber/veracrypt-truecrypt-einrichten-anleitung-festplatte-verschluesseln-3153230.html

Datenverschlüsselung

Zur Einhaltung der DSGVO-Vorschriften ist es erforderlich, dass die Daten verschlüsselt gespeichert werden. Mit Hilfe der Verschlüsselung von personenbezogenen Daten kann die Wahrscheinlichkeit einer Datenpanne und somit auch eines Bußgelds 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. Eine Kurz-Anleitung findet sich zum Beispiel auf der Webseite des PC Magazins.

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 problematisch, 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.

Als Cloud-Nutzer*in haftet man normalerweise für die Datenverarbeitung innerhalb der Cloud. Um die eigene Haftung bei DSGVO-Verstößen des gewählten Cloud-Anbieters zu beschränken, sollte man diesen vor der Nutzung, wenn möglich, zur Unterzeichnung eines Auftragsverarbeitungsvertrages *(siehe hierzu Kapitel 5.3)* verpflichten. Einige Dienstleister bieten einen solchen Auftragsverarbeitungsvertrag zum Download auf ihrer Seite an.

https://teamdrive.com/

https://open-telekom-cloud.com/de

Wissenswert:
Microsoft (und damit auch der Dienst OneDrive) hat sich dem EU-U.S. Privacy Shield-Abkommen unterworfen (zu prüfen unter: https://www.privacyshield.gov/list) und garantiert damit, der DSGVO entsprechende Standards zu nutzen. Dies ist zwar „nur“ ein Selbstunterwürfnis, reicht aber aktuell in Hinblick auf die DSGVO-Konformität des Dienstes (im Gegensatz zu einer einfachen Behauptung auf einer Website) aus. Dennoch sind Anbieter mit Sitz innerhalb der EU empfehlenswerter, da diese Selbstunterwerfung stets zeitlich begrenzt ist.

3.6 FOTO, VIDEO, TON

Fotos, Videos und Tonaufnahmen von Personen sind nicht grundsätzlich 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 die*der Abgebildete eingewilligt hat, oder eine Rechtsgrundlage dies erlaubt. Das heißt, eine Einwilligung der abgebildeten Person muss nicht zwingend eingeholt werden. Es empfiehlt sich darüber hinaus nicht, Einwilligungen für Datenverarbeitungsmaßnahmen einzuholen, die bereits aufgrund einer gesetzlichen Grundlage erlaubt sind.

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

Holt man sich dennoch vorsorglich eine Einwilligung ein, muss man berücksichtigen, dass man sich im Falle eines Widerrufs dieser Einwilligung im Nachhinein nicht mehr auf seine berechtigten Interessen berufen kann und die entsprechenden Aufnahmen vernichten muss.

Achtung:
Ob, inwieweit und für welche Zwecke bei der Öffentlichkeitsarbeit Einwilligungen zur Erstellung und Veröffentlichung von Personenaufnahmen gemäß der DSGVO einzuholen sind, ist bisher nicht vollständig geklärt. Zudem ist unklar, ob die Regelungen des Kunsturhebergesetzes (KUG) noch gelten.

https://www.lda.brandenburg.de/media_fast/4055/RechtlicheAnforderungenFotografie.pdf

https://www.lda.brandenburg.de/media_fast/4055/RechtlicheAnforderungenFotografie.pdf

Formulierungsvorschlag:
„Während der Veranstaltung werden Fotos/Videos/Tonaufnahmen gemacht, die zum Teil für die Dokumentation und Nachberichterstattung sowie die Öffentlichkeitsarbeit [des Vereins/des Jugendclubs/etc.] verwendet werden, zum Beispiel auf unserer Webseite, in Printmedien und in den sozialen Netzwerken. Durch Ihre Teilnahme geben Sie Ihr Einverständnis zur medialen Nutzung dieser Aufnahmen.
Die für die Verarbeitung verantwortliche Stelle im Sinne der DSGVO ist: [Adresse der zuständigen Stelle einfügen]“

Statt einer Einwilligung sollten Besucher*innen aber möglichst bereits bei der Anmeldung oder beim Betreten des Veranstaltungsortes angemessene Informationen erhalten. Die Landesbeauftragte für Datenschutz des Landes Brandenburg empfiehlt einen deutlichen Hinweis auf die Datenverarbeitung, etwa in Form eines nicht übersehbaren Aufstellers im Eingangsbereich einer Veranstaltung. 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 Webseite 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 der*dem Fotografierenden 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 gemäß Art. 14, Abs. 5 DSGVO, weil keine Anmeldung erforderlich war und es sich um eine Veranstaltung auf einem offenen Gelände ohne Zugangskontrolle mit vielen Personen handelt, ist es nicht möglich und notwendig den Transparenzpflichten nachzukommen. Bei Aufnahmen von Einzelpersonen müssen die Transparenzpflichten aber unbedingt beachtet werden.

Foto-, Video- und Tonaufnahmen von Kindern und Jugendlichen

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.

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

Sind also Aufnahmen von Kindern und Jugendlichen geplant, sollten diese und gegebenenfalls auch die Erziehungsberechtigten 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 der Kinder und Jugendlichen ab, ob sie diese Einwilligung selbst erteilen dürfen oder ob diese von den Erziehungsberechtigten 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)*.

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 der*des

Verantwortlichen aus und sollte unbedingt auch bei Aufnahmen von Erwachsenen eine Einwilligung einholen, die den Zweck der Veröffentlichung im Internet abdeckt.

https://lfd.niedersachsen.de/startseite/datenschutzreform/dsgvo/anfertigung_und_veroeffentlichung_von_personenfotografien/anfertigung-und-veroeffentlichung-von-personenfotografien-nach-dem-25-mai-2018-166008.html

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 Jugendarbeit 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 Jugendarbeit 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 einzu-halten. Zudem stehen in der Jugendarbeit tätige Personen in der Ver-antwortung, 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, er muss verfolgt und auf Neuerungen reagiert werden. Eigene Arbeitsweisen sollten immer wieder angepasst werden.

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 Erziehungsberechtigten nicht nutzen dürfen, werden diese von der Kommunikation ausgeschlossen.

WhatsApp

Beim Messenger WhatsApp werden Text- und Sprachnachrichten sowie Fotos und Videos beim Versand end-to-end 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 Facebook 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 Jugendarbeit jedoch überhaupt nicht zulässig.

Aus datenschutzrechtlicher Sicht ist es zudem kritisch zu betrachten, dass WhatsApp Daten außerhalb der Europäischen Union in die USA übermittelt. WhatsApp schreibt innerhalb der EU ein Mindestalter von 16 Jahren für die Nutzung des Dienstes vor.

Achtung:
Auszug der Nutzungsbedingungen von WhatsApp:
Im Einklang mit geltenden Gesetzen stellst du uns regelmäßig die Telefonnummern von WhatsApp Nutzer*innen und anderen Kontakten in deinem Mobiltelefon-Adressbuch zur Verfügung, darunter sowohl die Nummern von Nutzer*innen unserer Dienste als auch die von deinen sonstigen Kontakten.

Gut zu wissen:
Die Datenschutzgesetze der Schweiz als Nicht-EU-Land sind mit denen der DSGVO und der Bundesrepublik Deutschland vergleichbar.

Threema

Über den werbefreien Dienst Threema mit Sitz in der Schweiz können ebenso Texte, Sprachnachrichten, Bilder und Videos verschickt werden. Es gibt eine end-to-end-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 Freundinnen und Freunde den Dienst nutzen. So überträgt man als Nutzer*in keine Daten von anderen an das Unternehmen. Das Mindestalter beträgt 16 Jahre. Threema muss einmalig kostenpflichtig heruntergeladen werden. Weitere Kosten entstehen mit der Nutzung nicht.

Signal

Der kostenlose, werbefreie Messenger Signal hat ähnliche Funktionen wie WhatsApp und Threema. Im Gegensatz zu WhatsApp können Nachrichten verschickt werden, die sich nach einer festgelegten Zeit wieder löschen. 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 Jugendarbeit 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 bei der Jugendarbeit in jedem Fall beachtet werden:

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

- Fachkräfte der Jugendarbeit dürfen 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.
- Persönliche Termine mit Jugendlichen immer ohne Angabe eines Grundes kommunizieren.
- Für die Kommunikation mit Jugendlichen ist stets ein Diensthandy zu nutzen.
- Die Begründung für die 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.

3.8 INSTAGRAM UND FACEBOOK

Die Arbeit in sozialen Netzwerken, wie zum Beispiel Instagram und Facebook, ist für viele zum notwendigen Aufgabenbereich innerhalb der Jugendarbeit 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 ausführlich auf das Thema Foto-, Ton- und Videoaufnahmen und deren Veröffentlichung eingegangen.

Instagram

Mit der kostenlosen App Instagram können Angebote und Projekte aus der Jugendarbeit in Form von Fotos veröffentlicht werden und so bekannt gemacht werden. Aus Datenschutzgründen dürfen keine persönlichen Daten von Personen angegeben oder verknüpft werden. Außerdem sollte man keine Bilder veröffentlichen, auf denen einzelne Personen erkennbar sind.

Facebook

Werden soziale Netzwerke wie Facebook für die Öffentlichkeitsarbeit einer Organisation eingesetzt, sollte man sich immer wieder vor Augen halten, hier besonders sensibel und sparsam mit personenbezogenen Daten umzugehen. Dieser Kanal sollte nur zusätzlich zu datenschutzrechtlich unproblematischeren Kommunikationswegen, wie einer eigenen Webseite *(siehe hierzu Kapitel 3.9)*, genutzt werden. Es empfiehlt sich, auf Webseiten 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. Besucherinnen und Besucher einer Organisationsseite in den sozialen Medien sollten zudem auf eine eigenverantwortliche Nutzung hingewiesen werden und Informationen zu alternativen Kontaktmöglichkeiten bekommen.

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

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

Lesetipp:
Siehe hierzu auch https://www.heise.de/newsticker/meldung/Nach-EuGH-Urteil-Facebook-aendert-Datenschutz-Regeln-fuer-Seiten-4161100.html

3.9 WEBSEITE

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 Webseite, bei Facebook, Instagram oder einem anderen Online-Portal, grundsätzlich unzulässig, wenn die*der Betroffene nicht ausdrücklich eingewilligt hat *(siehe hierzu auch Kapitel 1.3)*.

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

Wenn sich eine Webseite 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.

In einem ersten Schritt muss eine gültige Datenschutzerklärung auf der Webseite veröffentlicht sein. Die Landesbeauftragte für Datenschutz Niedersachsen hat ein hilfreiches Papier mit Informationen für Webseitenbetreiber*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.

https://www.lfd.niedersachsen.de/download/130984/Informationen_fuer_Betreiber_von_Webseiten.pdf

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

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

3.10 ÖFFENTLICHE VERANSTALTUNGEN

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

Auch bei der Durchführung von öffentlichen Veranstaltungen ohne Anmeldung 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 Teilnehmenden vor dem Publikum genannt werden. In solchen Fällen ist das aus datenschutzrechtlichen Gründen nur zulässig, wenn die*der Betroffene eingewilligt hat oder eine Rechtsgrundlage dies erlaubt.

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

Erfolgen die Angaben anonymisiert – zum Beispiel indem nach einer Laufveranstaltung eine Liste ausgehängt wird, auf der lediglich die Startnummern der erreichten Laufzeit und einer Platzierung zugeordnet sind, müssen keine Vorschriften der DSGVO eingehalten werden.

3.11 DATENWEITERGABE AN ANDERE STELLEN

In der Jugendarbeit 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 Teilnehmendendaten an Zuwendungsgebende, die Zusammenarbeit mit Medienagenturen, IT-Dienstleistenden oder eine ausgelagerte Buchhaltung, mit denen dann als Verarbeitungsgrundlage ein Auftragsverarbeitungsvertrag geschlossen werden muss *(siehe hierzu Kapitel 5.3)*.

Die Betroffenen müssen 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 keine 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 Empfänger*innen exakt anzugeben – die DSGVO schreibt lediglich die Nennung der Kategorien der Empfänger*innen vor.

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.

Formulierungsvorschlag:
„Ihre personenbezogenen Daten bzw. die Ihres Kindes werden an Dritte, zu Zwecken der Beantragung von Fördermitteln, zum Abschluss von für die Freizeitfahrt notwendigen Versicherungen für die Teilnehmenden sowie an unsere Veranstaltungs- und Reisevertragspartner (Kooperationspartner, Reiseanbieter, Unterkünfte), weitergegeben.“

04 PRAXISSITUATIONEN IN DER JUGENDARBEIT

Nachdem im vorangegangenen Kapitel auf für die Jugendarbeit typische Prozesse und den Umgang mit personenbezogenen Daten im Rahmen dieser Prozesse eingegangen wurde, widmet sich das folgende Kapitel ausgewählten Praxissituationen aus der Jugendarbeit 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 zur*zum Adressatin*Adressaten 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*n Person*en 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*des Beraterin*Beraters 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 was es bei der Nutzung von Messenger-Diensten zu beachten gibt, steht 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 der*des 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 Kolleginnen*Kollegen 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 Jugendarbeit ausgeführt. Auf Wunsch der*des Adressatin*Adressaten 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 beim Veranstalter. 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 Teilnehmenden 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 Arbeits- oder Honorarvertrag oder Einverständniserklärung der*des Betroffenen vorliegen. Dienstliche Kontaktdaten dürfen zu dienstlichen Zwecken veröffentlicht werden.

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.

Ist eine Anmeldung zum Bildungsangebot erforderlich, müssen die Teilnehmenden darüber aufgeklärt werden, wo und wie ihre Daten verarbeitet bzw. gespeichert und gesichert werden. Es empfiehlt sich deshalb, eine Datenschutzerklärung im Rahmen des Anmeldungsprozesses zur Verfügung zu stellen. In *Kapitel 3.1* stehen weitere Hinweise zur Teilnehmendenverwaltung und zur Informationspflicht.

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

Tipp:
Folgender Mustersatz könnte zur Erfüllung der Informationspflicht auf Anmeldeformularen genutzt werden: *„Sie haben das Recht auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit.“*

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

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.

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 14 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 Eltern. Die Sozialarbeitenden 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 Gäste 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 Teilnehmendenliste ausgelegt werden, auf der man sich namentlich eintragen muss, wenn keine benötigt wird und eigentlich nur die Gesamtzahl der Teilnehmenden 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 Mitarbeitende 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 rechtliche Grundlage oder eine Einverständniserklärung der*des 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 umfasst 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 welchen Zwecke (zum Beispiel: Fotoaufnahmen von Gruppenreisen werden zur Öffentlichkeitsarbeit auf der Webseite veröffentlicht, Teilnahmelisten zur Organisation und Abrechnung von Workshops geführt und an externe Teamer*innen und Fördermittelgebende weitergegeben 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 den Kindern und Jugendlichen viele Aktivitäten, Ausflüge, Seminare und Ferienfreizeiten durch. Für jede einzelne Aktivität ist das Einholen der erforderlichen Einverständniserklärungen der Eltern und Teilnehmenden sehr mühsam. Daher wird überlegt, ein Papier mit einer „Generalvollmacht“ zu entwickeln.

4.5 NETZWERKARBEIT UND KOMMUNIKATION

Jugendarbeit wird häufig in Verbundsystemen mit verschiedenen Akteur*innen ermöglicht. Dienstberatungen, E-Mail-Kommunikation, 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 ist dann möglich, wenn das zu dem Zweck geschieht, über den die Betroffenen in Kennt-nis 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 nötig ist. Die Daten dürfen dann aber zum Beispiel nicht genutzt werden, um die*den Jugendliche*n zu weiteren Veranstaltungen oder Workshops einzuladen – es sei denn, sie*er hat diesem Zweck der Datenverarbeitung zugestimmt.

Der Austausch von personenbezogenen Daten muss immer sicher erfolgen – *siehe hierzu das 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 erhobene 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

Fallbeispiel:
Jelena und Clemens sind ehrenamtlich für ihren Jugendverband aktiv und betreuen in den Sommerferien verschiedene Ferienfreizeiten. Im Vorfeld bekommen sie von ihrem Jugendverband die Liste der angemeldeten Teilnehmenden zugeschickt sowie die Ferienpässe, in denen die Eltern besondere Betreuungsbedarfe und Krankheiten der Kinder vermerken.

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 Mitarbeitenden (z. B. im Rahmen des Tätigkeitsausschlusses nach § 72a SGB VIII, *siehe hierzu Kapitel 1.3)* vorzuhalten.

Grundsätzliche Informationen zum Thema Datenschutz und externe Mitarbeitende sind in *Kapitel 1.4* zusammengefasst. Haben sie 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 zum Beispiel in Form einer Vertraulichkeitserklärung als Anhang zum Honorarvertrag bzw. zur Ehrenamtsvereinbarung zur Vertraulichkeit verpflichtet werden. Auch externe Mitarbeitende 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 Mitarbeitende ebenso wie für festangestellte Mitarbeitende Vorrang vor dieser Handreichung.

4.7 ANTRAGS- UND ABRECHNUNGSVERFAHREN

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

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 Vereins, dient. Die Daten dürfen auch so lange gespeichert werden, bis der Zweck – in diesem Fall das Abrechnungsverfahren – 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.

Das Ministerium für Bildung, Jugend und Sport des Landes Brandenburg hat ein vereinfachtes Verfahren entwickelt, das einen verantwortungsbewussten Umgang mit personenbezogenen Daten ermöglicht.

Hierbei sind auf der neuen Teilnahmeliste seit dem 1. Januar 2019 nur statistische Angaben zur Anzahl der Teilnehmenden, den Bundesländern in denen sie ihren Wohnort haben sowie die Verteilung nach Geschlecht und Alter zu tätigen. Auf das Ausfüllen einer Teilnahmeliste in der bisherigen Form (mit Angaben zu Wohnort, Alter, Unterschrift) wird gänzlich verzichtet. Diese Daten müssen jedoch im Falle einer vertiefenden Prüfung durch das Ministerium von den Zuwendungsempfänger*innen vorgehalten werden. Dies kann aber zum Beispiel auch durch die Speicherung der Anmeldedaten der Teilnehmer*innen erfolgen.

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 Verarbeitungstätigen erstellt und gepflegt und bei einer Zusammenarbeit mit externen Dienstleistern Datenverarbeitungsverträge geschlossen werden. Intern müssen technische und organisatorische Maßnahmen ergriffen werden und auch das Verhalten bei Datenschutzpannen erfordert eine korrekte Vorgehensweise.

5.1 DATENSCHUTZBEAUFTRAGTE

Öffentliche Stellen müssen gemäß Art. 37 DSGVO immer eine*n Datenschutzbeauftragte*n benennen. Vereine, Organisationen und kleine Unternehmen sind gemäß § 38 Bundesdatenschutzgesetz (BDGS) dazu nur verpflichtet, wenn sich mindestens zehn 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.

https://www.lda.brandenburg.de/cms/detail.php/bb1.c.233960.de/bbo_contact

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

Die Aufgaben der*des Datenschutzbeauftragten sind klar geregelt

Art. 39 DSGVO

- Unterrichtung und Beratung der*des Verantwortlichen oder der*des Auftragsverarbeitenden 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 der*des Verantwortlichen oder der*des Auftragsverarbeitenden für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeitenden 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

In einem Verzeichnis von Verarbeitungstätigkeiten wird die Erfassung und der Umgang mit personenbezogenen Daten schriftlich dokumentiert und kann bei Bedarf nachvollzogen werden. So kommt man als Organisation der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO nach und kann auf Anfrage von Aufsichtsbehörden oder auch Betroffenen den Nachweis datenschutzrechtlicher Pflichterfüllung erbringen.

https://www.bitkom.org/sites/default/files/file/import/180529-LF-Verarbeitungsverzeichnis-online.pdf

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

Name und Kontakt

Der*Des 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.

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 Mitarbeitenden an ein externes Lohnbüro zur Gehaltsabrechnung)

Fristen für die Datenlöschung der verschiedenen Datenkategorien

Zum Beispiel, wenn sie für die Zwecke nicht mehr erforderlich sind, für die sie verarbeitet

Beschreibung der technischen und organisatorischen Maßnahmen

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

ggf. Datenschutzfolgenabschätzung

Die Brandenburgische Landesdatenschutzbeauftragte hat eine Liste von Verarbeitungsvorgängen veröffentlicht, für die eine Datenschutzfolgenabschätzung nötig ist. Auch wenn die in der Jugendarbeit erhobenen Daten darin nicht explizit erwähnt werden, so muss jede Organisation für sich klären, ob eine Datenschutzfolgenabschätzung nach Art. 35 DSGVO durchzuführen ist.

Es geht immer um die verschiedenen Kategorien und Verarbeitungstätigkeiten, sodass 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).

Inzwischen gibt es Muster von Verzeichnissen von Verarbeitungstätigkei-ten, auf die sich die Landesdatenschutzbehörden geeinigt haben und die verwendet werden können. Aber auch das Anlegen einer eigenen Tabelle ist möglich.

https://www.lda.brandenburg.de/sixcms/detail.php/bb1.c.587757.de

https://www.lfd.niedersachsen.de/themen/wirtschaft/verfahrensverzeicnis_und_verfahrensregister_nach_bdsg/verfahrensregister-und-verfahrensbeschreibung-fuer-den-nicht-oeffentlichen-bereich-56247.html

Praxistipp:
In Fällen, in denen die Weitergabe personenbezogener Daten durch Gesetze und Richtlinien geregelt ist, muss nach aktueller Rechtsauffassung kein gesonderter Auftragsverarbeitungsvertrag geschlossen werden. Das betrifft zum Beispiel die Weitergabe von Daten an Fördermittelgebende.

5.3 AUFTRAGSVERARBEITUNGSVERTRAG

Bei Verträgen der*des Verantwortlichen mit externen Dienstleistenden, die im Auftrag personenbezogene Daten verarbeiten, ist es notwendig, mit diesen einen Auftragsverarbeitungsvertrag zu schließen. Die DSGVO betrachtet solch einen Vorgang als Weitergabe von Daten an Dritte. Als Rechtsgrundlage hierfür dient meist das berechtigte Interesse der*des Verantwortlichen. Das betrifft zum Beispiel die Zusammenarbeit mit Medienagenturen, IT-Dienstleistenden oder eine ausgelagerte Buchhaltung. Hier 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 Auftragsverarbeitern geschlossen werden, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen durchgeführt werden. 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.

Achtung:
Verlassen oder teilen Mitarbeitende 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.

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.

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 Benutzerrechten und keine Doppelverwendung von Useraccounts

Zutrittskontrolle

Zu Büros und strikte Trennung von öffentlichen Räumen

Schreddern von Papieren mit personenbezogenen Daten

Effektiver Passwortschutz

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 abliegen.

Folgende technische Maßnahmen sind wichtig und umzusetzen

- Impressum auf Webseiten und Social Media-Auftritten
- Datenschutzerklärung auf Webseiten und Social Media-Auftritten
- SSL-Verschlüsselung der Webseite, zum Beispiel bei Nutzung von Kontaktformularen, Kommentarfunktionen in Blogs oder Analysetools
- E-Mail-Versand (zum Beispiel Newsletter) über BCC statt CC
- Verschlüsselung von E-Mails (TSL/SSL)

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

Zu weiteren organisatorischen Maßnahmen zählen

- Ausarbeitung eines Datenschutzkonzeptes
- Schulung und Sensibilisierung der Mitarbeitenden im Bereich Datenschutz
- Verpflichtung der Mitarbeitenden zur Wahrung des Datengeheimnisses
- Durchführung von internen Prüf- und Kontrollverfahren

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.

https://datenschutz.sachsen-anhalt.de/informationen/internationales/datenschutz-grundverordnung/checkliste-zur-dokumentation-der-getroffenen-technischen-und-organisatorischen-massnahmen/

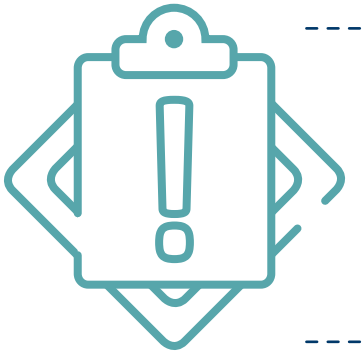
Diese Aufzählung ist ausdrücklich nicht als vollständig zu verstehen und jede Organisation muss im Rahmen des eigenen Datenschutzkonzeptes die für sich geeigneten und notwendigen technischen und organisatorischen Maßnahmen festlegen. Die Checkliste des Landesbeauftragten für Datenschutz Sachsen-Anhalt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

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.

https://www.lda.brandenburg.de/cms/detail.php/bb1.c.610589.de

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 des Schutzes personenbezogener Daten stehenden Fakten, von 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 finanziellen 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

IMPRESSUM

1. Auflage, 2019

Druckauflage: 750 Stück

Herausgebende

Fachverband Jugendarbeit / Jugendsozialarbeit Brandenburg e. V.
Charlottenstraße 123, 14467 Potsdam
Ansprechpartner: Sebastian Müller
Tel. 0331 81329445
info@fjb-online.de
www.fjb-online.de

Landesjugendring Brandenburg e. V.
Breite Straße 7a, 14467 Potsdam
Ansprechpartnerin: Melanie Ebell
Tel. 0331 6207530
info@ljr-brandenburg.de
www.ljr-brandenburg.de

Gefördert durch

Ministerium für Bildung, Jugend und Sport des Landes Brandenburg

Redaktion

Marina Schubert (Agentur Medienlabor)
Melanie Ebell (LJR)
Sebastian Müller (FJB)

Rechtliche Prüfung

Rechtsanwaltskanzlei Cornelius Matutis, Rechtsanwältin Felicitas Warncke
www.anwalt-für-datenschutz.eu

Layout und Druck

Agentur Medienlabor
www.agentur-medienlabor.de

Bildnachweise

Titelseite #996934596 und #996931296 © iStock.com/SIphotography

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

ÜBER DIESES HANDBUCH:

Datenschutz ist für viele zu einer Art Unwort des Jahres 2018 geworden. Gerade in Vereinen und kleineren Betrieben war die Verunsicherung im Kontext der DSGVO groß. „Wenn wir den Datenschutz wirklich ernst nehmen würden, könnten wir unsere Arbeit an den Nagel hängen“, lauteten so manche Reaktionen aus der Praxis.

Die Datenschutz-Grundverordnung hat 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 Arbeitshilfe erläutert daher nicht nur die wichtigsten Herausforderungen, sondern gibt vor allem auch praxistaugliche Hinweise und Formulierungshilfen für eine gelungene Umsetzung des Datenschutzes in der Jugendarbeit.

www.datenschutz-jugendarbeit.de

Herausgebende:

FACHVERBAND Jugendarbeit / Jugendsozialarbeit Brandenburg e. V.

ljr landesjugendring brandenburg

Gefördert durch:

LAND BRANDENBURG
Ministerium für Bildung, Jugend und Sport