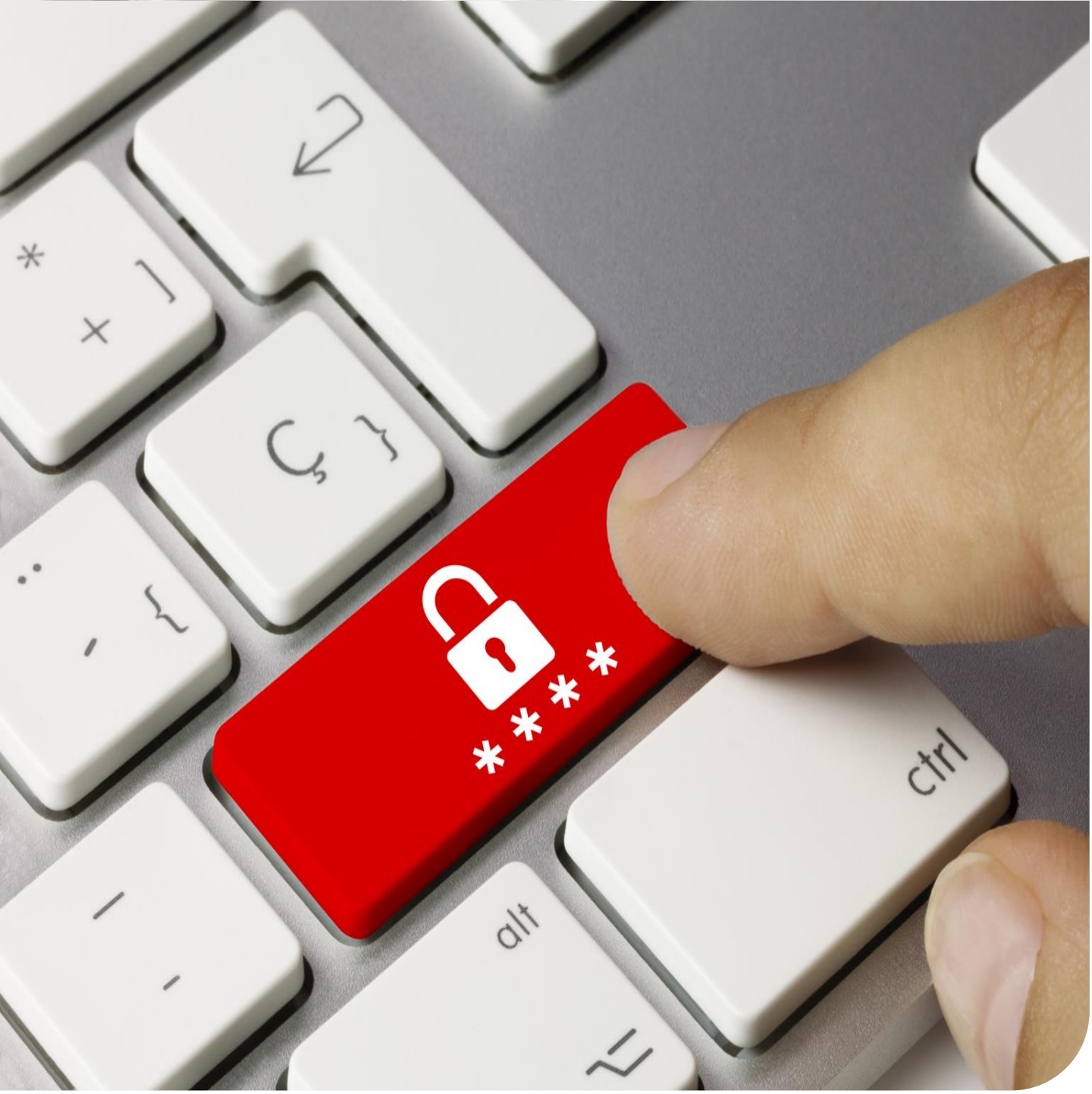
Arbeitshilfe



DATENSCHUTZ IM JUGENDRING

Bayerischer Jugendring

Vorwort

1 Grundinformation Datenschutz___ 4

1.1 Warum Datenschutz? ____ 4

1.2 Grundbegriffe des Datenschutzes ____ 5

2 Rechtliche Informationen zum Datenschutz___ 8

2.1 Regelwerke zum Datenschutz____ 8

2.2 Grundsätze ____ 9

2.3 Rechtsgrundlagen der Verarbeitung ____ 10

2.4 Datenverarbeitung von und durch Dritte ____ 12

3 Der_Die Verantwortliche: Aufgaben und Pflichten ___ 14

4 Der_Die Datenschutzbeauftragte___ 19

4.1 Aufgaben und Funktionen____ 19

4.2 Die Benennung____ 20

4.3 Rechte und Position____ 21

4.4 Dokumentation und Berichterstattung____ 22

5 Datenschutz im Jugendring___ 23

5.1 Personal und Mitarbeiter_innen____ 23

5.2 Ehrenamtliche____24

5.3 Datenschutz bei Maßnahmen____24

5.4 Datenschutz bei Projekten____ 26

5.5 Datenschutz für Teilnehmer_innen____ 26

5.6 Bußgelder und Spenden____27

5.7 EDV und Auftragsdatenverarbeitung____ 27

6 Quellen und Anlagen ___ 28

Vorwort

Der Bayerische Jugendring (BJR) unterliegt mit seinen Gliederungen als eine Körperschaft des öffentlichen Rechts dem Bayerischen Datenschutzgesetz (BayDSG). Hieraus leitet sich u.a. die gesetzliche Pflicht zur Bestellung von Datenschutzbeauftragten beim BJR und in den Gliederungen ab.

Das BayDSG trägt Sorge dafür, dass öffentliche Stellen die Persönlichkeitsrechte der Bürger und Bürginnen wahren.

Um dieser gesetzlichen Verpflichtung nachzukommen und die Umsetzung in den Gliederungen zu unterstützen, stellt der BJR die folgende Arbeitshilfe allen Gliederungen und deren Datenschutzbeauftragten zur Verfügung. Die in ihr enthaltenen Vorlagen und Empfehlungen sollen die Arbeit erleichtern.

Ziel ist es, den Datenschutz als selbstverständlichen Bestandteil in den Verwaltungs- und Arbeitsalltag der Jugendarbeit zu integrieren.

1 Grundinformationen zum Datenschutz

1.1 Warum Datenschutz?

Das Aufkommen des Datenschutzes ist verbunden mit der Entwicklung von Großrechnern in den 60er-Jahren. Diese Computer ermöglichten es, große Mengen von Daten – auch über Personen – zu verarbeiten und auszuwerten. Aus den Erfahrungen in den USA zeigte sich, dass es dafür einen rechtlichen Rahmen brauchte.
So entstand das relativ junge Rechtsgebiet Datenschutz in den 70er-Jahren mit ersten Gesetzen aus den Bundesländern, etwa Hessen 1970, Rheinland-Pfalz 1974 und auch das erste Bundesdatenschutzgesetz (BDSG) im Jahr 1977. Ziel der Gesetze war es, „der Beeinträchtigung der schutzwürdigen Belange der Betroffenen bei der Verarbeitung ihrer Daten“, entgegenzuwirken. Angesichts der heute allgegenwärtigen Verarbeitung von Personendaten in der IT und mit dem im Vergleich zu den 70er-Jahren mehrfach potenzierten Umfang ist es bemerkenswert, dass die möglichen Probleme damit schon so früh aufgegriffen wurden.

Aus dem Schutz vor Beeinträchtigungen entwickelte sich in der Auseinandersetzung um die Volkszählung Anfang der 80er-Jahre schließlich das Recht auf informationelle Selbstbestimmung. Im Urteil des Bundesverfassungsgerichts zur Beschwerde gegen das Volkszählungsgesetz stellte dieses fest, dass darin Eingriffe in Grundrechte ohne Rechtfertigung vorgenommen würden. Zum Schutz des Einzelnen und der freiheitlichen und demokratischen Grundordnung formulierten die Verfassungsrichter_innen das Grundrecht auf informationelle Selbstbestimmung.
Sie leiteten es aus der Menschenwürde nach Art. 1 des Grundgesetzes und dem Recht auf freie Entfaltung der Persönlichkeit (Art. 2 GG) ab. Demnach müssten die Bürger_innen immer wissen können, wer zu welchem Zeitpunkt und bei welcher Gelegenheit etwas über sie wisse. Eine Unsicherheit über das Verwenden von Informationen über Personen und deren Verhalten würde zu einer Anpassung dieser selbst führen. Darin sahen die Richter_innen einen Widerspruch zu den Grundrechten, Demokratie und Freiheit.

In der Folge hat sich die Gesetzgebung zum Datenschutz stets weiterentwickelt, um auch mit der Technik Schritt zu halten. Es gibt in allen Bundesländer Landesdatenschutzgesetze, die vor allem die öffentliche Verwaltung im Fokus haben.

Die am 25. Mai 2018 eingeführte **Datenschutzgrundverordnung (DSGVO)** beansprucht in der gesamten Europäischen Union, und damit auch in Bayern, die unmittelbare Geltung. Hierdurch wurde es notwendig die nationalen Datenschutzgesetze zu ändern und anzupassen. Die neuen angepassten nationalen Gesetzgebungen wurden bereits verabschiedet und verkündet und sind am 25. Mai 2018 in Kraft getreten.
Für den Bayerischen Jugendring als Körperschaft des öffentlichen Rechts (KdöR) und seine Gliederungen gilt, wie für alle öffentlichen bayerischen Stellen jedoch weiterhin als allgemeines Datenschutzgesetz das Bayerische Datenschutzgesetz (BayDSG) in seiner Neufassung. Wenn das BayDSG keine Regelung trifft, gilt das Bundesdatenschutzgesetz (BDSG) als Bundesgesetz.
Die genannten Rechtsgrundlagen stehen in einem hierarchischen Verhältnis zueinander. Die DSGVO steht dabei an der Spitze.
Neben den speziellen Datenschutzgesetzen hat der Schutz von Daten in vielen bereichsspezifischen Gesetzen Einzug gehalten. Dort wird der Umgang mit personenbezogenen Daten, z.B. in der Telekommunikation (TKG) oder in den Sozialsystemen (SGB) festgelegt.

Datenschutz ist zu einem Querschnittsthema geworden, das an vielen Stellen geregelt wird.

Die Entwicklung der Gesetzgebung zum Umgang mit Daten ist nur ein Teil des Gesamtbildes zum Thema Datenschutz in Gesellschaft, Wirtschaft und Technik. Internetzugang, die Verbreitung von Smartphones und die fortschreitenden Vernetzung schaffen neue Möglichkeiten und Herausforderungen. Nicht nur in der digitalen Wirtschaft scheinen Daten über Personen eine neue „Währung“ geworden zu sein mit der scheinbar „kostenlose“ Dienste bezahlt werden. Die Einstellungen zur Veröffentlichung von persönlichen Daten besonders in sozialen Netzen haben sich gewandelt, es wird teilweise eine „Post-Privacy“-Gesellschaft propagiert. Demgegenüber stehen Befürchtungen vor lückenloser Überwachung und dem „gläsernen“ Menschen.
Auch wenn hier viel im Fluss ist, bleibt es Aufgabe, an den Entwicklungen dran zu bleiben und die dazu nötigen Regelungen zu treffen, um die Datenschutzgesetze umzusetzen.

1.2 Grundbegriffe des Datenschutzes

Der Begriff „Datenschutz“ wird im alltäglichen Sprachgebrauch oft weitergehender verwendet als im gesetzgeberischen Verständnis. Im Juristischen bezieht er sich nur auf den Schutz von personenbezogenen Daten, in Abgrenzung etwa zu Daten über Geschäftsvorfälle, internen Firmenangelegenheiten oder Informationen zu Erfindungen und Entwicklungen. Nicht synonym zum „Datenschutz“ ist die „Datensicherheit“, da es dabei vor allem um den Schutz von Daten unter technischen Gesichtspunkten geht.

Ziel des Datenschutzes ist es, Einzelpersonen vor der Beeinträchtigung ihres Persönlichkeitsrechtes beim Umgang mit ihren personenbezogenen Daten zu schützen.

Personenbezogene Daten
Personenbezogene Daten sind nach der Formulierung in Art 4 Abs. 1 DSGVO „Einzelangaben über persönliche oder sächliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen“. Einzelangaben sind dabei Informationen, die sich auf eine einzelne Person beziehen, sodass diese darüber identifiziert werden kann. Damit werden Bilder oder biometrische Merkmale auch zu personenbezogenen Daten, wenn sie eine Identifikation ermöglichen.
Die Nennung von „persönlichen und sächlichen Verhältnissen“ soll verdeutlichen, dass alle Informationen, die etwas über die Personen aussagen, erfasst sind. Egal ob sie die Person direkt charakterisieren oder Sachverhalte beschreiben, die sich auf sie beziehen. Erfasst werden außerdem nur natürliche Personen. Sie müssen zudem für die Zuordnung der Informationen entsprechend bestimmt sein oder können durch Hinzuziehen weiteren Wissens bestimmt werden. Ist keine Zuordnung möglich z. B. durch Anonymisierung, liegt kein personenbezogenes Datum vor.

Sensible personenbezogene Daten
Ein in der DSGVO (Art. 9 Abs. 1) festgehaltener Katalog von besonders sensiblen personenbezogenen Daten umfasst Informationen zur ethnischen Herkunft, politischen Meinungen, religiösen oder philosophischen Überzeugungen, Gewerkschaftszugehörigkeit, Sexualleben und Gesundheit. Für diese Daten gelten besondere rechtliche Anforderungen, um sie erheben und nutzen zu dürfen.

Im Folgenden sind einige Beispiele zusammengestellt, um den Begriff der personenbezogenen Daten näher zu erläutern:

Beispiele für **personenbezogene Daten** sind:

- Adresse, Telefonnummer, E-Mail und Kontoverbindung einer Person.
- Arbeitszeiten oder Fehltage eines_r Arbeitnehmers_in.
- Lebenslauf und das Foto eines_r Bewerbers_in.
- besondere Ernährungsgewohnheiten oder Allergien von Teilnehmer_innen einer Maßnahme und die Teilnahme an der Maßnahme.

Besonders sensible personenbezogene Daten sind:

- Ethnische Herkunft
- Politische Gesinnung
- Religiöse und/oder philosophische Meinungen
- Gewerkschaftszugehörigkeit
- Daten über Gesundheit oder Sexualleben von Personen

Verarbeitung
Was nach altem Recht unterteilt wurde, in Erhebung, Verarbeitung und Nutzung, fällt nun unter den einheitlichen Begriff der Verarbeitung. Gemeint ist damit die Abfrage, das Speichern, das Weitergeben, das Auslesen, das Vernichten von Daten etc. Dabei kommt es nach neuem Recht nicht darauf an, ob die Daten automatisiert (Erfassung über IT) oder nicht-automatisiert (Vordrucke, Formulare, die handschriftlich ausgefüllt werden) verarbeitet werden.

Verantwortliche_r
Die Rolle des_der Verantwortlichen wird in Kapitel 2 ausführlich erklärt. Auf Landesebene ist das der Präsident. In den Gliederungen ist dies in der Regel der_die jeweilige Vorsitzende und die Geschäftsführung

Datenschutzbeauftragte_r
Die Rolle des_der behördlichen Datenschutzbeauftragten (DSB) ist durch Einführung der DSGVO ebenfalls neu geregelt worden. Zum DSB können alle Mitarbeiter_innen benannt werden, bei denen keine Interessenkonflikte mit anderen Aufgaben entstehen.

Auftragsverarbeiter
Unter diesen Begriff fallen externe Dienstleister, deren personenbezogene Daten im Auftrag zur Verarbeitung weitergegeben werden. Eine Auftragsverarbeitung ist durch ein echtes Auftragsverhältnis gekennzeichnet, das heißt es muss ein Weisungsverhältnis zwischen Auftraggeber und Auftragnehmer in Form eines Vertrags bestehen. Entgegen der bisherigen Praxis stellt die Weitergabe von personenbezogenen Daten an den Auftragsverarbeiter nun eine Übermittlung an Dritte dar. Die Übermittlung muss deshalb auf Basis der DSGVO Art. 6 Abs. 1 f) begründet werden. Sie ist zulässig wenn ein berechtigtes Interesse vorliegt. Ebenfalls neu ist, dass der_die Verantwortliche für jede Verarbeitung von personenbezogenen Daten zuständig bleibt. Egal ob er_sie diese selbst vornimmt oder durch einen Auftragsverarbeiter durchführen lässt.

Es dürfen nur Verträge mit Unternehmen gemacht werden, die eine hinreichende Garantie auf Erfüllung der Datenschutzanforderungen gewährleisten.

Um die Weitergabe von Daten zu regeln, wird der Begriff des Dritten zur rechtlichen Bewertung eingeführt. Dritte sind grundsätzlich alle Personen und Stellen außerhalb der speichernden Stelle. Personen und unselbstständige Teile innerhalb der speichernden Stelle gelten nicht als Dritte, ebenso Betroffene und Auftragnehmer_innen im Falle von Auftragsdatenverarbeitung.
Mit Auftragsdatenverarbeitern muss ein

Vertrag zur Sicherstellung der Einhaltung der DSGVO geschlossen werden.

Betroffene
Als Betroffene werden in den Gesetzestexten die Personen benannt, mit deren personenbezogenen Daten umgegangen wird und deren Schutz vor Beeinträchtigungen Ziel der Gesetze ist. Betroffene_r ist man unabhängig von der Staatsangehörigkeit und unabhängig davon, ob man in Deutschland lebt. Entscheidend ist, dass die Daten im Geltungsbereich des Gesetzes erhoben oder verwendet werden.

Rechte der Betroffenen
Mit der Einführung der DSGVO werden die Rechte der betroffenen Personen gestärkt. Sie haben klar geregelte Ansprüche, etwa auf Auskunft, Berichtigung und/oder Löschung ihrer Daten. Die Artikel 12 ff regeln diese Rechte. Betroffene können formlos und ohne Begründung Auskunft über ihre gespeicherten personenbezogenen Daten verlangen. Auch haben sie das Recht, eine unverzügliche Berichtigung von unrichtigen personenbezogenen Daten zu verlangen. Eine Pflicht zur Löschung der Daten besteht grundsätzlich immer, wenn der Betroffene seine Einwilligung zur Verarbeitung seiner Daten widerruft. Das sogenannte „Recht auf Vergessenwerden“ ist nicht gleichbedeutend mit der Löschung der personenbezogenen Daten. Es bezieht sich auf die Tilgung von Spuren personenbezogener Daten, die durch Veröffentlichung im Internet entstanden und einer breiten Öffentlichkeit zugänglich gemacht worden sind. Neu ist beispielsweise das Recht auf kostenlose Kopie und Weitergabe der verarbeiteten Daten.

2 Rechtliche Informationen zum Datenschutz

2.1 Regelwerke zum Datenschutz

Regelungen zum Datenschutz stammen aus verschiedenen Quellen, da das Thema in Gesetzen, Verordnungen und weiteren Rechtsvorschriften, auch nicht gesetzlicher Natur, adressiert wird.

Nach Art. 1 Abs. 1 Satz 1 BayDSG gilt das neue Bayerische Datenschutzgesetz (BayDSG) für alle Behörden und öffentlichen Stellen des Freistaats Bayern. Somit gilt das BayDSG für den BJR und seine Gliederungen. Maßgeblich für die konkrete Bestimmung ist der organisatorische Behördenbegriff. Das bedeutet, dass als Behörde jede Stelle gilt, die durch das Organisationsrecht als institutionalisierte Einheit im eigenen Namen nach außen hin Aufgaben wahrnimmt. Das trifft auf die Gliederungen des BJR zu, sodass sie als eigene Behörden und als eigene öffentliche, speichernde Stellen gelten. Die Regelungen des BayDSG sind damit von jeder Gliederung umzusetzen.

EU-Datenschutzgrundverordnung (DSGVO)
Das Datenschutzrecht wurde zum 25. Mai 2018 europaweit grundlegend reformiert. Damit gilt sie in der gesamten Europäischen Union und somit selbstverständlich auch in Bayern. Zum Stichtag traten sowohl das neue Bundesdatenschutzgesetz (BDSG) als auch das neue Bayerische Datenschutzgesetz (BayDSG) in der an die DSGVO angepassten Version in Kraft.

Bundesdatenschutzgesetz (BDSG)
Das Bundesdatenschutzgesetz gilt für öffentliche Stellen des Bundes und für nichtöffentliche Stellen. Mit letzteren sind Organisationen der Wirtschaft wie Firmen und Gewerbebetriebe aber auch Vereine und Verbände gemeint.

Bayerisches Datenschutzgesetz (BayDSG)
Das Bayerische Datenschutzgesetz ist anzuwenden auf öffentliche Stellen des Freistaates und auf juristische Personen des öffentlichen Rechts, die unter der Rechtsaufsicht des Freistaates stehen. Unter den letztgenannten Punkt fällt der BJR mit seinen Gliederungen als Körperschaft des öffentlichen Rechts (KdöR). Somit ist das BayDSG maßgeblich für den Datenschutz im BJR.

Bereichsspezifische Gesetze
Für den BJR und seine Gliederung besonders relevante sind Regeln zum Datenschutz, die in einigen bereichsspezifischen Gesetzen stehen:

- **Das Sozialgesetzbuch (SGB)** regelt den Sozialdatenschutz eigens. Es enthält im allgemeinen Teil (SGB I), in den Verwaltungsverfahren (SGB X) und bei der Sozialhilfe (SGB XII) Regelungen zu Stellen, die Daten erheben und verarbeiten dürfen und präzisiert unter welchen Voraussetzungen Erhebung, Verarbeitung und Nutzung stattfinden dürfen und welche Auskunftspflichten bestehen.

- **Das Strafgesetzbuch (StGB)** enthält Tatbestände zum Bruch der Vertraulichkeit, der Offenbarung oder Verwertung von Geheinissen, der Schweigepflichtverletzung, Verletzung von Post- und Fernmeldegeheimnis sowie zum Computerbetrug und der Datenveränderung. Relevant bei der zugelassenen privaten Nutzung von Kommunikationsdiensten wie Telefon oder E-Mail wird das Telekommunikationsgesetz (TKG). Den Datenschutz bei Onlinediensten regelt das Telemediengesetz (TMG).Das Vorliegen weiterer bereichsspezifischer Datenschutzregelungen sollte vor dem Tätigkeitwerden in weiteren Rechtsgebieten abgeklärt werden.

Anwendung und Auslegung von Datenschutzregelungen
Zur korrekten Anwendung und Auslegung der geltenden Regeln des Datenschutzes sind neben der Kenntnis der Vorschriften weitere Quellen hilfreich. Zu den einschlägigen Gesetzen gibt es Kommentarliteratur, die Verständnis und Auslegung unterstützen sowie Rechtsmeinungen und wichtige Urteile enthalten. Zudem verfasst der Bayerische Landesbeauftragte für Datenschutz regelmäßig Tätigkeitsberichte, in denen er Stellungnahmen zu Anfragen an ihn und Ergebnisse seiner Kontrolltätigkeit erläutert. Diese Ausführungen sind hilfreich bei der konkreten Ausgestaltung des Datenschutzes.

2.2 Grundsätze

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten richtet sich grundsätzlich nach Art. 6 Abs. 1 DSGVO. Damit eine Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder aufgrund einer Rechtsgrundlage erfolgen, die sich aus der DSGVO, respektive dem BayDSG und dem BDSG ergibt. Jede Verarbeitung personenbezogener Daten braucht eine eigene Rechtsgrundlage.

Art.5 DSGVO regelt **die allgemeinen Grundsätze für die Verarbeitung** von personenbezogenen Daten. Hier werden zunächst allgemeine Grundsätze aufgestellt, die bei einer späteren Verarbeitung zwingend zu beachten sind. Personenbezogene Daten müssen:

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren transparente Weise verarbeitet werden. (Grundsatz der Rechtmäßigkeit).
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden.
c) dem Zweck angemessen und erheblich auf das notwendige Maß beschränkt werden.
d) sachlich richtig und auf dem neuesten Stand sein.
e) so gespeichert werden, dass die Identifizierung der betroffenen Person nur so lange ermöglicht wird, wie es für den Zweck notwendig ist.
f) so gespeichert werden, dass eine angemessene Sicherheit gewährleistet ist, sie müssen vor unbefugter und unrechtmäßiger Verarbeitung und unbeabsichtigtem Verlust oder Zerstörung bzw. Schädigung durch geeignete technische und organisatorische Maßnahmen gesichert werden (Art. 32 DSGVO).

Die Einhaltung dieser Grundsätze hat der_die Verantwortliche im Zweifel nachzuweisen. Der_Die Verantwortliche ist gegenüber der Aufsichtsbehörde insoweit rechenschaftspflichtig.
Dementsprechend haben Jugendringe dafür zu sorgen, schriftliche Bestimmungen zur Datenverarbeitung auszuarbeiten, mit denen sich die Einhaltung dieser Grundsätze im Zweifel nachweisen lässt. Gesetzlich vorgeschrieben sind folgende Pflichten:

- Aufstellen von Datenschutzrichtlinien/Datenschutzordnungen über die Erhebung, Nutzung, Speicherung, Aufbewahrung, Löschung von Daten etc.
- Zugangsbeschränkungen festlegen: Wer hat wann auf welche Daten Zugriff und warum?
- Datenschutzunterweisungen- und Verpflichtungen von Beschäftigten.
- Dienstanweisungen.

- Führen eines Verarbeitungsverzeichnisses.
- Verträge zur Auftragsdatenverarbeitung.
- Datenschutz-Folgeabschätzung.

2.3 Rechtsgrundlagen der Verarbeitung

Die **Rechtmäßigkeit der Verarbeitung** personenbezogener Daten richtet sich grundsätzlich nach Art. 6 DSGVO. Diese führt somit den bekannten Grundsatz fort, dass die Verarbeitung verboten ist, wenn nicht ein entsprechender Erlaubnistatbestand (Verbot mit Erlaubnisvorbehalt) vorliegt.

Maßgebliche Rechtsgrundlagen für die Datenverarbeitung für den Bayerischen Jugendring und seiner Gliederungen sind nach der DSGVO und dem BayDSG vor allem Art. 6 Abs. 1a), Art. 6 Abs. 1 b) und Art. 6 Abs. 1 f):

a) die betroffene Person hat ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben (Art. 6 Abs. 1a)).
b) die Verarbeitung ist zur Erfüllung eines Vertrags mit der betroffenen Person notwendig (Art. 6 Abs. 1b)).
c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt (Art. 6 Abs. 1c)).
d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen (Art. 6 Abs. 1d)).
e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (Art. 6 Abs. 1e)).
f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betreffenden Person um ein Kind handelt (Art. 6 Abs. 1f))

Verarbeitung aufgrund der Einwilligung des Betroffenen
In Art. 4 der DSGVO sind die Begriffsbestimmungen festgelegt, Nr. 11 beschäftigt sich mit der Einwilligung. Die Einwilligung muss so einfach wie möglich formuliert sein. Sie muss unmissverständlich sein und die betroffene Person darüber aufklären für welchen Zweck die personenbezogenen Daten erhoben werden.

Wichtig:
Ausreichend ist immer eine Rechtsgrundlage! Wenn die Daten aufgrund der Satzung verarbeitet werden dürfen braucht es keine zusätzliche Einwilligung.

Art. 7. DSGVO konkretisiert diesen Grundsatz und benennt die Voraussetzungen einer ordnungsgemäßen Einwilligung des Betroffenen:

- die Einwilligung muss schriftlich erfolgen
- die vorformulierte Einwilligung muss so klar, einfach und verständlich wie möglich formuliert sein. Vor diesem Hintergrund werden durch Art. 8 der DSGVO auch erstmalig Jugendliche in den Blick genommen**. Danach dürfen Kinder ab 16 Jahren ihr Einverständnis selbst erteilen**, die Anforderungen an die Verständlichkeit und Klarheit der Formulierung sind hier umso höher.

- Die Einwilligung muss ausdrücklich erfolgen, durch eine unmissverständliche Willensbekundung (Unterschrift, aktives Ankreuzen eines Feldes etc.).
  Die Einwilligung in die Datenverarbeitung über eine Eingabemaske auf einer Homepage muss so gestaltet sein, dass man seine Einwilligung nur durch Setzen des Hakens im entsprechenden Feld erteilen kann. Ein vorab angekreuztes Feld ist nicht ausreichend.
- Die Einwilligung muss jederzeit widerrufen werden können. Hierüber ist vorab zu informieren, der Widerruf muss so einfach wie möglich sein.

Veröffentlichung von Foto- und Filmaufnahmen

Fotografieren, das Speichern und natürlich auch die Veröffentlichung von Fotos sind in aller Regel eine Verarbeitung personenbezogener Daten im Sinne der DSGVO bzw. des BDSG. Sie ist nur zulässig, wenn eine Rechtsvorschrift sie erlaubt, anordnet oder der_die Betroffene eingewilligt hat. Beim Bayerischen Jugendring und seinen Gliederungen wird im Regelfall keine ausdrückliche gesetzliche Ermächtigung zur Anfertigung und Verwendung von Foto- oder Filmaufnahmen vorliegen. Im Sinne von Art. 6 Abs. 1 Buch. a) DSGVO sind Foto- oder Filmaufnahmen nur mit datenschutzkonformer Einwilligung des_der Betroffenen erlaubt. Bei Minderjährigen ist die Einwilligung eines Erziehungsberechtigten, ab Vollendung des 16. Lebensjahres zusätzlich die des Minderjährigen selbst notwendig. Diese Einwilligung muss gemäß den Art. 4 Nr. 11 und Art. 7 DSGVO freiwillig und informiert erteilt werden. Es empfiehlt sich aus Gründen der Nachweisbarkeit immer eine schriftliche Einwilligung einzuholen (Muster Anlage 4). In dieser müssen die betroffenen Personen darüber informiert werden, zu welchem Zweck die Foto- oder Filmaufnahmen gemacht werden sollen, in welcher Form und wie lange sie gespeichert werden, wer darauf Zugriff hat und an wen sie gegebenenfalls weitergegeben werden. Es muss ebenfalls darauf hingewiesen werden, dass die betroffenen Personen gemäß Art. 7 Abs. 3 DSGVO jederzeit ihre Einwilligung ohne Angabe von Gründen widerrufen kann. Zusätzlich zur DSGVO muss beim Thema Foto- und Filmaufnahmen das KUG (Kunsturhebergesetz) betrachtet werden. Wenn man Fotos von Personen machen und veröffentlichen will, berührt das immer das Recht am eigenen Bild der abgebildeten Person. Aus diesem folgt, das „Bildnisse“ (Aufnahmen von Personen und auch sonstige bildliche Darstellungen eines Menschen) nur mit Einwilligung des betroffenen (§ 22 KUG) verbreitet oder öffentlich zu Schau gestellt werden dürfen. Das KUG listet in § 23 Ausnahmen auf, die eine Veröffentlichung ohne Einwilligung erlauben:

- **Bildnisse aus dem Bereich der Zeitgeschichte** (als Faustregel gilt: Würde die (lokale) Presse darüber berichten?).
- **Bilder auf denen Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeiten erscheinen** (hier gilt, die Person darf keinen wichtigen Teil des Bildes ausmachen, man könnte sie theoretische weglassen und der Bildinhalt wäre trotzdem erklärend).
- **Bilder von Versammlungen, Aufzügen und ähnlichen Veranstaltungen**, an denen die dargestellten Personen teilgenommen haben (diese Form der Abbildung kommt z. b. bei Sportveranstaltungen, Umzügen und ähnlichem vor, wo sich Menschen versammeln um gemeinsam etwas zu tun. Häufig wird sich dies mit dem Begriff der Bildnisse aus der Zeitgeschichte überschneiden). Vorsicht ist hier im Bereich von Demonstrationen und dergleichen geboten, da auf den Bildern keine Person identifizierbar sein darf.

- **Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Veranstaltung oder Schaustellung einem höheren Interesse der Kunst dient** (dies spielt im Bereich der Jugendarbeit keine größere Rolle und ist hier vernachlässigbar).

Diese Ausnahmen sind jedoch nur dann erlaubt, wenn die Verbreitung oder zur Schaustellung die berechtigten Interessen des Abgebildeten nicht verletzen. Es geht letztlich immer um eine Abwägung der Interessensphären.

2.4 Datenverarbeitungen von und durch Dritte

Werden durch den Bayerischen Jugendring oder eine Gliederung erhobene personenbezogene Daten in unserem Auftrag an einen externen Dienstleister zur Verarbeitung weitergegeben, spricht die DSGVO hier in Art. 28 und 29 von der Auftragsverarbeitung.

Als Rechtsgrundlage für die Verarbeitung von Daten Dritter (Teilnehmer_inen, Ehrenamtliche etc.), die nicht Mitarbeiter_innen sind, gilt Art. 6 Abs. 1f) DSGVO. Die Verarbeitung von Daten Dritter kann erfolgen, wenn diese zur „Wahrnehmung berechtigter Interessen“ des Jugendrings erforderlich sind und sofern „nicht die Interessen oder Grundrechte“ und Grundfreiheiten der betroffenen Person überwiegen.

Das berechtigte Interesse eines Jugendrings ergibt sich aus der Satzung des Bayerischen Jugendrings sowie aufgrund seiner Stellung als Träger der öffentlichen Jugendarbeit. Die Definition sagt, „berechtigt“ ist jedes von der Rechtsordnung gebilligte Interesse. Im Fall einer Kontrolle oder eines Rechtsstreits muss es aber konkret dargelegt und begründet werden. Rein geschäftliche Interessen reichen hier nicht aus. Berechtigte Interessen können nur eigene Belange der verantwortlichen Stelle sein. Diese muss die Bedeutung der Interessenwahrung begründen. Dies kann dann in einer Datenschutzrichtlinie/
Datenschutzordnung näher konkretisiert und niedergeschrieben werden.
So ist etwa die Weitergabe von personenbezogenen Daten an Fördermittelgeber eine zulässige Datenverarbeitung, da dies zur Wahrnehmung berechtigter Interessen des Jugendrings notwendig ist.

Auftragsverarbeitung
Klassischer Partner ist die AKDB für die Personalverwaltung. Weiter sind dies beispielsweise Webhoster (Auslagerung der Website auf den Server des Providers), Cloud-Anbieter oder Anbieter im Falle der Auslagerung der Buchhaltung. Eine Auftragsdatenverarbeitung darf nur auf Basis eines bindenden Vertrags erfolgen. (Musterverträge werden auf der Homepage des Bayerischen Landesamts für Datenschutzaufsicht www.lfa.de zur Verfügung gestellt). Mindestanforderungen im Vertrag sind:

- Gegenstand und Dauer der Auftragsdatenverarbeitung.
- Umfang, Art und Zweck der Datenerhebung.
- Art der zu verarbeitenden personenbezogenen Daten und Kategorien der von der Datenverarbeitung betroffenen Personen.
- Pflichten und Recht des_der Verantwortlichen.
- Der_Die Auftragnehmer_-in verpflichtet das eingesetzte Personal auf das Datengeheimnis.
- zulässige Unterauftragsverhältnisse.
- Unterstützung des_der Verantwortlichen durch den Auftragsdatenverarbeiter, siehe Art. 32 ff DSGVO (Meldepflicht von Datenschutzverstößen).

- Abwicklung und Beendigung der Auftragsdatenverarbeitung.
- Kontrollrecht des Auftraggebers, nach bisheriger Rechtslage war der_die Auftragnehmer_in nicht als Dritte_r, sondern als Teil der verantwortlichen Stelle anzusehen, mit der Folge, dass keine Datenübermittlung vorlag und somit auch keine Einwilligung der Mitglieder in die Auftragsdatenverarbeitung erforderlich war. Das hat sich mit der DSGVO erledigt. Die Weitergabe von personenbezogenen Daten an den Auftragsverarbeiter stellt nun eine Übermittlung an Dritte dar. Rechtsgrundlage für diese Verarbeitung ist Art. 6 Abs. 1f) DSGVO. Denn ein berechtigtes Interesse im Sinne von Art. 6. Abs. 1f) DSGVO ist dann gegeben, wenn sich der_die Verantwortliche für seine_ihre Organisation mit einer externen Datenverarbeitung (z.B. AKDB) arbeitet. Auch in diesem Fall ist der_die Verantwortliche für jede Verarbeitung personenbezogener Daten, die er_sie selbst vornimmt oder durch einen von ihm_ihr bestellten Auftragdatensverarbeiter_in wahrgenommen werden, verantwortlich.

Verarbeitung von Personaldaten von Beschäftigten

Die Verarbeitung personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses ist in § 26 BDSG gesondert geregelt. Danach dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn diese für die Entscheidung über die Begründung des Beschäftigtenverhältnisses erforderlich sind. Oder wenn diese Daten für Durchführung oder Beendigung des Beschäftigungsverhältnisses, zur Ausübung oder Erfüllung, der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten notwendig sind.

3 Der_Die Verantwortlich_e Aufgaben und Pflichten

In Art. 3 Abs. 2 BayDSG wird definiert, dass der_die Verantwortliche für die Verarbeitung personenbezogener Daten die zuständige öffentliche Stelle ist, soweit hier nichts anderes bestimmt ist.

In der Regel sind dies in den Gliederungen die jeweiligen Vorsitzende_n und die Geschäftsführung. Für die Landesebene gilt der Präsident in seine Funktion als Dienststellenleiter als Verantwortlicher.

3.1 Aufgaben und Pflichten

Dem Verantwortlichen sind vielfältige Pflichten zur Sicherstellung des Datenschutzes zugeordnet. Teile dieser Aufgaben können von der Leitung auf andere Personen delegiert werden.

1. **Benennung eines_einer Datenschutzbeauftragten**
   Der behördliche DSB ist aufgrund seiner_ihrer beruflichen Qualifikation und seines_ihres datenschutzrechtlichen Fachwissens zu benennen. Zur Vermeidung von Interessenkonflikten dürfen diese Aufgaben nicht vom Verantwortlichen übernommen werden.
   Der_Die Verantwortliche muss die Kontaktdaten des_der Datenschutzbeauftragten veröffentlichen und die der zuständigen Aufsichtsbehörde (Landesbeauftragter für Datenschutz Bayern) benennen. Für die Veröffentlichung der Kontaktdaten genügt die Veröffentlichung des Namens und der E-Mail-Adresse auf der Homepage.

2. **Führen des Verzeichnisses der Verarbeitungstätigkeiten**
   Gemäß Art. 30 DSGVO hat jede_r Verantwortliche ein Verzeichnis aller automatisierten und nicht automatisierten Daten-Verarbeitungstätigkeiten zu führen (siehe Anlage 2). Zwar besteht bei Verantwortlichen, bei denen weniger als 250 Mitarbeiter_innen beschäftigt sind, zunächst eine Ausnahme von dieser Pflicht. Diese Ausnahme gilt aber nicht, wenn die Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, wenn die die Verarbeitung nicht nur gelegentlich oder eine Verarbeitung sensibler Daten im Sinne von Art. 9 und Art.10 DSGVO erfolgt. Da in jeder Gliederung die Verarbeitung personenbezogener Daten nicht nur gelegentlich erfolgt, ist auch bei solchen mit weniger als 250 Mitarbeiter_innen ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Das Verzeichnis muss zwingend folgende Angaben enthalten, die im Wesentlichen den Informationspflichten nach Art. 13 DSGVO entsprechen:
   - Kontaktdaten des_der Verantwortlichen sowie ggf. seines_ihres Vertreters.
   - Zweck der Verarbeitung.
   - Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten.
   - Kategorien von Empfänger_innen, gegenüber denen die personenbezogenen Daten offengelegt worden sind bzw. noch offengelegt werden.
   - Fristen für die Löschung der verschiedenen Datenkategorien.
   - Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO.

   Muster sind in **den Anlagen 3 und 3a** enthalten) Das Verarbeitungsverzeichnis muss schriftlich oder in einem elektronischen Format geführt werden. Der_die Verantwortliche ist verpflichtet, der Aufsichtsbehörde das Verzeichnis auf deren Anfrage zur Verfügung zu stellen. Das bisherige Einsichtsrecht für betroffene Personen besteht nach der neuen Rechtslage nicht mehr. Lediglich der_die

Datenschutzbeauftragte des Jugendrings hat ein Recht auf Einsicht in dieses Verzeichnis.

3. **Datenschutz-Folgenabschätzung**
   Eine Datenschutz-Folgenabschätzung bezieht sich auf die verarbeiteten Daten, die hierfür verwendete Hard- und Software und die eingesetzten Prozesse im konkreten Verarbeitungsvorgang. Sie beschreibt und bewertet die Verarbeitung von personenbezogenen Daten. Art. 35 Abs. 1 DSGVO sagt, dass Verarbeitungsvorgänge die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, vorab einer Datenschutzfolgen-Abschätzung unterzogen werden müssen. Bei der Einführung neuer oder bei wesentlichen Änderungen vorhandener Verarbeitungen wird die Frage nach einer Folgenabschätzung aufkommen. Der Gesetzgeber sieht eine Vorprüfung vor, diese ist insbesondere dann auch zu dokumentieren, wenn man zur Auffassung gelangt, dass der Vorgang nicht folgenabschätzungswürdig ist. Die Dokumentation kann mit der Mustervorlage der „Beschreibung einer Verarbeitungstätigkeit“ (**siehe Anlage 2**) unter Ziffer 11 vorgenommen werden.Der Landesbeauftragte für Datenschutz in Bayern hat diesbezüglich eine nicht abschließende Liste von Verarbeitungen veröffentlicht, für die eine Datenschutz-Folgenabschätzung notwendig ist. Für die Praxis beim Bayerischen Jugendring und seinen Gliederungen dürfte dies jedoch in den wenigsten Fällen erforderlich sein, zumal diese Pflicht dann erfüllt ist, wenn beispielsweise der_die Auftragsdatenverarbeiter_in diese Pflicht bereits erfüllt hat.

4. **Informationspflicht gegenüber dem Betroffenen**
   Seit Einführung der DSGVO gelten umfassende **Informationspflichten** (in der Praxis ist dies der Datenschutzhinweis; Anlage 3/3a) wenn personenbezogene Daten direkt bei der betroffenen Personen erhoben werden. Die betroffene Person soll wissen, was mit ihren Daten geschieht und wer hier eine Einsicht in die Daten hat. Das Gesetz nennt das ein berechtigtes Interesse. Die Art. 13 und 14 der DSGVO beschäftigen sich hiermit.

   Aus Art. 13 ergeben sich insbesondere folgende Hinweise:

   - Name und Kontaktdaten des_r Verantwortliche_n ggf. Stellvertreter_in.
   - Name und Kontaktdaten des_r Datenschutzbeauftragten_r.
   - Rechtsgrundlagen der Verarbeitung.
   - Berechtigtes Interesse im Sinne von Art. 6 (Rechtmäßigkeit der Verarbeitung).
   - Mögliche Empfänger der Daten.
   - Speicherdauer der Daten.
   - Belehrung über die Betroffenenrechte (Auskunft, Berichtigung, Löschung, Widerruf).
   - Jederzeitiges Widerrufsrecht der Einwilligung, wenn die Erhebung aufgrund der Einwilligung erfolgt ist.

   Werden die Daten über den_die Betroffene_n nicht bei ihm_ihr selbst, sondern einem Dritten abgefragt, ergeben sich die jeweiligen Informationspflichten aus Art. 14 DSGVO. Dieser regelt Art. 13:

- Die Angabe des Quellennachweises, also woher die Daten stammen.
- Ob die Offenlegung der Daten an einen_eine weitere_n Empfänger_in geplant ist.
- Ob die Absicht zur Verwendung für andere Zwecke als den Grund der Erhebung geplant ist.
- Die Auskünfte hierüber müssen innerhalb eines Monats erteilt werden.

5. Datenschutzverstöße

Die Folgen von Datenschutzverstößen decken rechtlich die Bandbreite von der Pflicht zur Unterlassung, über Bußgelder oder Schadensersatz, bis hin zu Straftatbeständen ab. Selbst wenn der Verstoß unterhalb der Ordnungswidrigkeitsgrenze bleibt, hat das Folgen für den weiteren Umgang mit Daten. Neu ist, dass mit Einführung der DSGVO Datenschutzverstöße (Art. 33I innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet werden müssen. Das geht online über www.datenschutz-bayern.de. Ausgenommen sind nur Verletzungen, die kein Risiko für die Rechte und Freiheiten natürlicher Personen führt.
Die Meldung muss enthalten:

- Beschreibung und Art des Datenschutzverstoßes.
- Namen und Kontaktdaten des_der Datenschutzbeauftragten oder der zuständigen Anlaufstelle.
- Eine Beschreibung der wahrscheinlichen Folgen der Verletzung.
- Eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung oder Abminderung ihrer möglichen nachteiligen Auswirkungen.
- Hat die Datenschutzverletzung voraussichtliche ein hohes Risiko für die persönlichen Rechte und Freiheiten einer natürlichen Person zur Folge (Art. 34 DSGVO), so muss diese unverzüglich informiert werden.

Hinweis
Aufsichtsbehörde für den Bayerischen Jugendring und seine Gliederungen ist:

- Der Bayerischer Landesbeauftragte für den Datenschutz,
  Wagmüllerstraße 18,
  80538 München

6. Technische und Organisatorische Maßnahme zur Sicherung der personenbezogenen Daten

In der neuen DSGVO finden sich an mehreren Stellen Aussagen zu den technischen und organisatorischen Anforderungen zur Sicherung der Verarbeitung personenbezogener Daten:

- Art. 5 Abs. 1f) Grundsätze für die Verarbeitung personenbezogener Daten.
- Art. 24 Verantwortung des für die Verarbeitung Verantwortlichen.
- Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.
- Art. 32 Sicherheit der Verarbeitung.
- Art 35 Datenschutz-Folgenabschätzung.
- Art 36 Vorherige Konsultation.

Die Sicherstellung eines angemessenen Schutzniveaus obliegt dem_der Verantwortlichen. Die Datenschutzgrundverordnung stellt die Rechte und Freiheiten der betroffenen Personen deren Daten verarbeitet werden in den Mittelpunkt. Es wird von einer formalen Risikoanalyse gesprochen, die vor der Verarbeitung der Daten durchgeführt werden muss. Sie zielt darauf ab, die unterschiedlichen Eintrittswahrscheinlichkeiten und die Schwere der Risiken zu prüfen, die bei der Verarbeitung personenbezogener Daten auftreten können. Nebenbei dient diese Risikoanalyse auch dazu, eine Einschätzung vornehmen zu können, ob im

jeweils vorliegenden Fall eine Datenschutz-Folgenabschätzung notwendig werden würde.
In der Praxis soll abgewogen werden, in welchem Umfang und zu welchem Zweck personenbezogene Daten erhoben werden sollen und welchen Schutzbedarf diese Daten haben und welche Gefahren/Risiken eintreten können. Art. 32 Abs. 2 DSGVO benennt als Risiken z.B. die Vernichtung, den Verlust, die Veränderung, das unbefugte Offenlegung oder den unbefugten Zugang zu den personenbezogenen Daten.

Das Bundesdatenschutzgesetz (BDSG) geht in § 64 Abs. 3 zudem auch auf Maßnahmen ein, die durch die Risikobewertung bei einer automatisierten Verarbeitung von personenbezogenen Daten zu ergreifen sind. Die genannten Maßnahmen beschreiben recht übersichtlich was der Gesetzgeber hier meint:

1. Verwehrung des Zugangs (für Unbefugte) zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird (Zugangskontrolle).

2. Verhinderung des unbefugten Lesens- Kopierens, Veränderns oder Löschen von Datenträgern (Datenträgerkontrolle).

3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von Datenträgern (Speicherkontrolle).

4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zu Datenübertragung durch Unbefugte (Benutzerkontrolle).

5. Gewährleistung g der Zugriffskontrolle: dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassenden personenbezogenen Daten Zugang haben.

6. Gewährleistung der Übertragungskontrolle: dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden.

7. Gewährleistung der Eingabekontrolle:. dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

8. Gewährleistung der Transportkontrolle: dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt sind.

9. Gewährleistung der Wiederherstellbarkeit: dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

10. Gewährleistung der Zuverlässigkeit: dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

11. Gewährleistung der Datenintegrität: dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

12. Gewährleistung der Auftragskontrolle: dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des_der Auftraggebers_in durchgeführt werden können

13. Gewährleistung der Verfügbarkeitskontrolle: dass personenbezogene Daten

gegen Zerstörung oder Verlust geschützt sind.

14. Gewährleistung der Trennbarkeit: dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

In den Art. 25 und 32 werden Maßnahmen und Schutzziele in Bezug auf die Technik und Sicherheit der Datenverarbeitung aufgeführt. Auch wenn die DSGVO teilweise neue Begriffe und Systematiken verwendet, handelt es sich letztlich um Sicherheitsanforderungen die alle bisher schon im BayDSG gefordert wurden.

Vertraulichkeit
Schutz vor unbefugter Kenntnisnahme der Daten.

Integrität
Gewährleistung der Echtheit, Vollständigkeit, Zurechenbarkeit, Urheberschaft, und (Rechts-)Gültigkeit der Daten.

Verfügbarkeit
zeitgerechte Bereitstellung der Daten, Möglichkeit zur ordnungsgemäßen Verarbeitung.

Belastbarkeit (Resilienz)
Die ist ein neuer Begriff, der bisher im Datenschutzbereich nicht verwendet wurde. Im IT Bereich ist mit „Resilienz“ üblicherweise eine gewisse Stabilität gegenüber Ausfällen oder Angriffen gemeint. Die Abgrenzung der Verfügbarkeit ist jedoch nicht eindeutig.

Wiederherstellbarkeit
Dieser Begriff wurde bisher ebenfalls nicht als eigenständiges Schutzziel verwendet, da er auch dem Begriff der Verfügbarkeit zugeordnet werden kann. Gemeint sind beispielsweise Notfallkonzepte für Rechenzentren, um nach einem Ausfall oder Angriff schnell wieder betriebsbereit zu sein.

Datenschutz durch Technikgestaltung
Bei der Konzipierung von Verfahren und Produkten muss zukünftig vermehrt auf den Datenschutz geachtet werden. Schlagworte hier sind: Datenminimierung, Pseudonymisierung, Möglichkeiten zur Datenlöschung, sichere Verschlüsselung und Berechtigungskonzepte.

Datenschutzfreundliche Voreinstellungen
Verfahren und Produkte sollen so gestaltet sein, dass sie die Grundprinzipien des Datenschutzes und der IT Sicherheit von vornherein berücksichtigen. z. B. keine Standard-Passwörter, Verschlüsselungen, Beschränkung der Nutzer_innen, deaktivierte Ortungsdienste.

Pseudonymisierung, Verschlüsselung
Diese beiden Maßnahmen dienen den Zielen der Vertraulichkeit und Integrität

Bei der Auswahl ist gemäß Art. 25 DSGVO auf den „Stand der Technik“ zu achten. Da dies jedoch nicht näher definiert ist, empfiehlt es sich, sich an den Standards im öffentlichen Dienst zu orientieren. Nähere Informationen können den Technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (www.bsi.bund.de) entnommen werden. Hier werden auch wichtige Tipps zum Thema Cyber-Sicherheit oder Hilfestellungen zur Erstellung von Sicherheitskonzepten gegeben.

4 Der_Die Datenschutzbeauftragte

Wie bereits in der Vergangenheit haben Behörden und andere öffentliche Stellen eine_n Datenschutzbeauftragte_ n zu benennen. Seine_Ihre Aufgaben haben sich mit Einführung der neuen DSGVO geändert und werden in den Art. 37 bis 39 DSGVO beschrieben. Die Datenschutz-Grundverordnung unterscheidet zwischen dem_r Verantwortliche_n und dem_r Datenschutzbeauftragten und weißt beiden klar voneinander abgegrenzte Rollen zu.

Datenschutz ist „Chefsache“ und obliegt der Leitung. Sie hat dafür Sorge zu tragen, dass die Verarbeitung personenbezogener Daten nach den Regelungen der DSGVO stattfindet.

Nach dem neuen Rollenbild hat der Datenschutzbeauftrage nun eine Beratungs- und Überwachungsfunktion (Art. 39 DSGVO). Die Aufgabe, für die Einhaltung der datenschutzrechtlichen Bestimmungen zu sorgen ist nun nicht mehr seine/ihre alleinige Aufgabe.

4.1 Aufgaben und Funktion

Der Gesetzgeber sieht in Art. 39 sowie in der Vorschrift des Art. 38 Abs. 4 DSGVO einen Mindestkatalog an Anforderungen für den_die Datenschutzbeauftragen vor.
Unterrichtung und Beratung des_der Verantwortlichen und seiner_ihrer Beschäftigten:

- Unterrichtung steht dafür, über allgemeine datenschutzrechtliche Vorgaben und Neuerungen hierzu, zu informieren und zu sensibilisieren.
- Beratung bezieht sich auf konkrete Situationen im Arbeitsalltag aus denen sich datenschutzrechtliche Fragen und Probleme ergeben.
  Folgende Leistungen könnten hier anfallen:
- Beratung vor erstmaligem Einsatz oder bei wesentlichen Änderungen eines automatisierten Verfahrens (ggf. Datenschutzfolgeabschätzung).
- Beratung bei der Erstellung von Dienstanweisungen oder Dienstvereinbarungen mit Datenschutzbezug.
- Beratung bei Melde- und Benachrichtungsvorfällen nach einer Verletzung.
- Beratung bei der Gestaltung von Vereinbarungen zur Auftragsdatenverarbeitung.

Überwachung bezieht sich auf die Einhaltung der gesetzlichen datenschutzrechtlichen Vorgaben sowie des innerbehördlichen Datenschutzkonzepts. Mögliche hier vorgesehene Mitarbeiterschulungen können durch den_die Datenschutzbeauftragten vorgenommen werden.

Zusammenarbeit mit der Aufsichtsbehörde
Das Gesetz meint hier die Anfrage und Beratung bei datenschutzrechtlichen Problemen durch den Landesbeauftragten für Datenschutz. Bei Fragen zu Verarbeitungsvorgängen ist wiederum der_die Datenschutzbeauftragte Anlaufstelle für den Landesbeauftragten. Dies kann beispielsweise bei einem Auskunftsersuch eines_einer Betroffenen vorkommen.

Beratung betroffener Personen
Betroffenen Personen können mit allen Fragen, die die Verarbeitung ihrer personenbezogenen Daten betreffen, zur Wahrung Ihrer Rechte an den_die Datenschutzbeauftragte_n herantreten.

Zusätzliche optionale Aufgaben
Wenn die Zuweisungen dem Rollenbild des_der Datenschutzbeauftragten nach der DSGVO entsprechen, können ihm_ihr durch den_die Verantwortliche_n zusätzliche Aufgaben übertragen werden.

Diese könnten sein:

- Führung des Verzeichnisses für Verarbeitungstätigkeiten(Anlage 2).
- Durchführung der Datenschutz-Folgenabschätzung.
- Klärung und Meldung von Datenschutzverstößen inklusive der gegebenenfalls notwendigen Benachrichtigung an die betroffene Person.
- Erfüllung von Auskunftsrechten gegenüber Betroffenen nach Art. 15 DSGVO; hier ist eine Koordinierungsaufgabe gemeint, diese umfasst die Abfrage aller notwendigen Angaben bei der Abteilung sowie die Auskunftserteilung an die betroffene Person.
- Schulung von Beschäftigten zu allen Themen des Datenschutzes.

4.2 Die Benennung

Anforderungen an die zu benennende Person
Der_Die Datenschutzbeauftragte sollte mit der Arbeitsweise seiner Gliederung vertraut sein. Arbeitsabläufe und Regelungen auch über das eigene „normale“ Aufgabengebiet sollten zumindest in Grundlagen bekannt sein. An den Jugendring überstellte Mitarbeiter_innen können benannt werden, wenn die Fachaufsicht für die an die Gliederung delegierten Aufgaben übertragen wurde.

Zum DSB können keine Mitarbeiter_innen ernannt werden, bei denen diese Funktion zu Interessenkonflikten mit deren sonstigen Aufgaben führen würde. Vorsitzenden und ihre Stellvertreter_innen sowie Geschäftsführer_innen von Stadt-, Kreis- und Bezirksjugendringen können damit nicht DSB werden. Darüber hinaus können Interessenkonflikte im Einzelfall auch mit anderen Personen vorliegen. Mitarbeiter_innen, die sich im Rahmen ihrer Tätigkeit als DSB selber in einer anderen Aufgabe kontrollieren müssten, können ebenso nicht benannt werden. Dies betrifft vor allem EDV-Administrator_innen. Zudem muss die Person Fachkenntnisse zum Datenschutz und der EDV haben oder über Fortbildungen erwerben können.

Vorbereitung der Benennung
Zur Vorbereitung der Benennung sollte sich die zuständige Person (Geschäftsführung, Vorsitzender) über die Grundlagen des Datenschutzes informieren. Auch der Vorstand als entscheidendes Organ muss ausreichend informiert werden.Bei der Suche nach einer geeigneten Person in der Gliederung sollten die oben genannten Anforderungen beachtet werden. Mit möglichen Kandidat_innen sind dann Gespräche zur Übernahme der Funktion zu führen, da letztendlich die Benennung nur im Einvernehmen stattfinden kann.

Benennung und Formalien
Die Entscheidung zur Benennung als Datenschutzbeauftragte_r trifft der Vorstand der Gliederung per Beschluss. Eine förmliche Benennung eines möglicherweise existierenden Personalrats ist nicht vorgesehen. Die Benennung erfolgt dann durch den_die Vorsitzende_n und ist in schriftlicher Form zu dokumentieren. Mit Gegenzeichnen der Benennung durch den DSB wird auch das Einvernehmen festgehalten.

Mit der Benennung soll der zeitliche Umfang für die Tätigkeit als Datenschutzbeauftragte_r sowie bereitzustellende Ressourcen geklärt werden. Zu regeln ist auch, dass der DSB in seiner_ihrer Funktion unmittelbar dem_der Vorsitzenden zugeordnet ist. Weitere Konkretisierungen zu Aufgaben und Zuständigkeiten sowie Absprachen zur Berichterstattung sind angeraten.

Einführung des_der neuen Datenschutzbeauftragten
Nach der Benennung des_der neuen Datenschutzbeauftragten empfiehlt es sich, dies in einem Schreiben oder Rundbrief an die hauptamtlichen und längerfristig ehrenamt-

lichen aktiven Mitarbeiter_innen bekannt zu geben. Eine kurze Info über die zukünftigen Aufgaben des DSB und das Thema Datenschutz im Text ist hilfreich. Neben der Veröffentlichung der Kontaktdaten des_der Beauftragten im Schreiben kann dies auch auf der Website oder am schwarzen Brett erfolgen.

In wichtigen Gremien der Gliederung wie der Vollversammlung oder des Personalrats ist zudem eine persönliche Vorstellung sinnvoll. In größeren Gliederungen können einführende Gespräche mit Abteilungs- oder Einrichtungsleiter_innen und mit Personen besonderer Zuständigkeiten (EDV-Verantwortliche o.ä.) sinnvoll sein.

Die Bereitstellung der nötigen Mittel für den_die Datenschutzbeauftragten muss zeitnah erfolgen, um schnell starten zu können.

Gemeinsame und externe Datenschutzbeauftragte
Genau wie bisher das BayDSG sieht auch die DSGVO in Art. 37 Abs. 3 die Benennung eines_einer gemeinsamen behördlichen Datenschutzbeauftragten aus der eigenen Gliederung bzw. Behörde vor, wenn die Organisationsstruktur der Beteiligten eine Zusammenlegung ermöglicht. Die gemeinsame Benennung eines_einer Beschäftigten zum DSB durch mehrere benachbarte Jugendringe ist somit möglich.

Vor einer gemeinsamen Benennung ist jedoch erst das eigene Personal auf eine geeignete Person hin zu überprüfen. Findet sich keine geeignete Person, ist als nächstes abzuklären, ob die gemeinsame Benennung mit umliegenden Jugendringen möglich ist.

Ergibt sich auch hier keine Lösung, kann im Rahmen einer „Amtshilfe“ das Landratsamt oder die Stadtverwaltung angefragt werden. Über eine gemeinsame Benennung könnte der DSB dieser öffentlichen Stellen auch den Jugendring abdecken. Bei der gemeinsamen Bestellung sind jedoch die Grenzen der Leistbarkeit für eine Person bei entsprechenden Größenordnungen und die Effektivität des Wirkens des DSB bei mehreren Einheiten mitzudenken. Ferner sind ggf. Umlagen oder finanzielle Beteiligungen zwischen den gemeinsam benennenden Stellen sowie die personelle Zuordnung des DSB zu vereinbaren.

Im Gegensatz zur bisherigen Rechtslage kann nun ein_eine Datenschutzbeauftragte_r mittels Dienstleistungsvertrag „eingekauft“ werden. Art 37. Abs. 5 DSGVO stellt jedoch klar, dass nur natürliche Personen die Anforderungen erfüllen können. Die Benennung einer juristischen Person (Firma) als Datenschutzbeauftragte_r ist daher nicht möglich. In der Praxis muss der Dienstleistungsvertrag dahingehend formuliert werden, dass die beauftragte Firma einen festen Beschäftigten konkret als Datenschutzbeauftragte_n für die öffentliche Stelle benennen muss.

4.3 Rechte und Position

Ausstattung und Ressourcen
Für die Arbeit als Datenschutzbeauftragte_r ist die benannte Person im zeitlich angemessenen Umfang freizustellen. Nötigenfalls ist dies mit der Erweiterung des Stundenumfangs der Anstellung zu verbinden, wenn sonstige Aufgaben gleich bleiben. Einzuplanen ist dabei auch der Aufwand für den Besuch von Schulungen sowie Mittel für Fachliteratur. Die Erreichbarkeit des DSB per Telefon und E-Mail und ein Aufsuchen unter Wahrung der Vertraulichkeit muss sichergestellt werden.

Weisungsfreiheit
In der Ausübung seiner Funktion handelt der_die Datenschutzbeauftragte weisungsfrei, kann also nicht angewiesen werden, datenschutzrechtliche Sachverhalte nach

Vorgaben entsprechend zu bewerten oder zu behandeln. Er_Sie hat aber auch keine Weisungsbefugnis gegenüber anderen Personen den Datenschutz betreffend. Die verantwortliche Leitung der speichernden Stelle kann entgegen der Empfehlungen des DSB handeln, dann jedoch in Kenntnis der der datenschutzrechtlichen Bewertung und möglicher Folgen. Sollten dem DSB bei der Auslegung von Datenschutzvorschriften trotz innerbehördlicher Bemühungen Zweifel bleiben, so kann er sich direkt zur Klärung an den Landesbeauftragten für Datenschutz werden.

Benachteiligungsverbot
Um als Datenschutzbeauftragte_r, die vom Gesetzgeber geforderte Unabhängigkeit zu erlangen, dürfen ihm_ihr aus seiner_ihrer fachlichen Tätigkeit keine Nachteile entstehen. Kündigung, Versetzung, disziplinarische Maßnahmen oder Abberufung aufgrund der Wahrnehmung der Funktion als Datenschutzbeauftragte_r sind unzulässig.

Position, Verschwiegenheit
Der_Die Datenschutzbeauftragte ist direkt der Leitung der öffentliche Stelle, im Fall des Jugendrings, dem_der Vorsitzenden der Gliederung oder dem Präsidenten zu unterstellen. Dies ist insoweit angebracht, als der DSB weiter dem_der Verantwortlichen direkt berichten muss.

4.4 Dokumentation und Berichterstattung

Strukturierung, Vorlagen
Zum Nachweis der Tätigkeiten des_der Datenschutzbeauftragten und der Maßnahmen des Datenschutzes in der speichernden Stelle empfiehlt es sich eine entsprechende Dokumentation anzulegen. Strukturiert werden kann die Dokumentation nach den Ergebnissen eines ersten datenschutzrechtlichen Überblicks, wiederkehrenden Vorgängen wie z.B. der Freigabe von automatisierten Verfahren, dem zu führenden Verfahrensverzeichnis und Aktennotizen. Um sich nach Benennung einen ersten Überblick in Sachen Datenschutz und die Struktur der eingesetzten IT zu verschaffen, sowie für spätere Kontrollen haben sich Checklisten als hilfreich erwiesen. Für die Erfassung welche Daten in der Gliederung erfasst und verwendet werden, sind Formblätter und Fragebögen geeignet. Sie können auch zur Freigabe von Verfahren eingesetzt werden und liefern die nötigen Informationen für das Verfahrensverzeichnis. Vorlagen dazu gibt es im Internet und der Kommentarliteratur.

Aktennotizen
In seiner_ihrer Tätigkeit wird der_die Datenschutzbeauftragte Anfragen erhalten, Beratung leisten, Stellungnahmen abgeben, Abwägungen vornehmen etc. Die Person ist damit mit Vorgängen befasst, bei denen nicht nur das Ergebnis, sondern auch der Weg dorthin und ggf. auch der Vorgang an sich dokumentiert werden muss. Dies kann gut über eigene Aktennotizen des_der Datenschutzbeauftragten erreicht werden. Sie dienen dem Nachweis über das datenschutzrechtliche Handeln bei Kontrollen und sichern den_die DSB ab, wenn anders als von ihm_ihr nahegelegt verfahren wird.

Regelmäßiger Bericht
Es ist üblich, dass der_die Datenschutzbeauftragte dem verantwortlichen Gremium regelmäßig Bericht zu Tätigkeit und dem Stand des Datenschutzes gibt. Mit dem Bericht wird Rechenschaft zur Erfüllung des Datenschutzes in der Gliederung abgelegt, und die Arbeit des DSB wird transparent, indem z.B. die Anzahl der Anfragen, Beratungen und Freigaben erläutert werden kann. Prüfungen und Kontrollen des DSB gehören ebenfalls her, um etwaige, sich daraus ergebende Anregungen den verantwortlichen Personen zur Kenntnis zu bringen.

5 Datenschutz im Jugendring

5.1 Personal und Mitarbeiter_innen

Innerhalb der Organisation
Personenbezogene Daten von Mitarbeiter_innen finden sich vor allem in der Personalakte und in Nebenakten zur Personalverwaltung. Dabei ist der Begriff Mitarbeiter_innen weit auszulegen und bezieht sich auch auf Praktikant_innen und Teilnehmer_innen des Freiwilligen Sozialen Jahrs (FSJ), des Freiwilligen Ökologischen Jahrs (FÖJ), des Bundesfreiwilligendiensts (BFD) etc.

Zur Personalakte gehören:
- Personalstammdaten
- Bewerbungsunterlagen
- Arbeitsvertrag und ergänzende Vereinbarungen
- Abmahnungen
- Mutterschutz-, Elternzeitunterlagen
- Nebentätigkeitsanzeige
- Führungszeugnis
- Pflegezeiten
- Kindergeldangelegenheiten
- Vorschussangelegenheiten
- Auflösungs-, Beendigungsunterlagen
- Zeugnisse, Fortbildungsnachweise
- Eingliederungsvereinbarungen
- Beurteilungen
- Betrieblich veranlasste ärztliche Untersuchungen
- Entgeltunterlagen

In Nebenakten werden aufbewahrt:
- Stunden-, Urlaubszettel
- Pläne zu Schicht-, Bürozeiten
- Krankmeldungen
- Fahrt-, Reisekostenunterlagen
- Spesen-, Sachkostenabrechnungen

Sämtliche sich im Personalakt befindlichen Unterlagen sind als besonders schutzwürdig einzustufen. Der Personenkreis, der hierauf zugreifen kann, ist besonders einzuschränken.
Generell sind Personalakten und Nebenakten der Personalverwaltung verschlossen aufzubewahren. Akten, die für den aktuellen Vorgang nicht benötigt werden, sind wieder zu verschließen. Beim Verlassen des Arbeitsplatzes – auch kurzzeitig – sind diese Akten vor Einsichtnahme oder Zugriff durch Dritte zu schützen. Dies gilt sowohl für Daten auf Papiere als auch für digitalisierte Daten.
In der Praxis sieht das folgendermaßen aus:

- Einschließen der Akten.
- Absperren des Büros.
- Sperren des PC.
- Blickgeschützter Aufstellort des Monitors, wenn möglich.

Bei Personalakten sind besondere Aufbewahrungs- und Löschfristen zu beachten. Verlassen Personaldaten die Personalstelle, ist der Transport oder die Übermittlung sicher zu gestalten. Zum Beispiel sind Bewerbungsunterlagen in extra verschlossenen Kuverts zu versenden, oder Datenübermittlungen nur über sichere, verschlüsselte Verbindungen vorzunehmen.

Externe Dienstleister
Werden Teile der Personalverwaltung, z.B. die Lohnabrechnung, an externe Dienstleister ausgelagert, so stellt dies eine Auftragsdatenverarbeitung dar. In diesem Fall muss die Auftragsdatenverarbeitung durch einen Vertrag geregelt werden. Bei der AKDB ist von einer sorgfältigen Auswahl aufgrund einer Verwaltungsvorschrift zum BayDSG auszugehen. Bei der Zusammenarbeit mit anderen Dienstleistern, ist die sorgfältige Auswahl zu dokumentieren.

Personalakte, Führungszeugnis
Führungszeugnisse von hauptamtlichen

Mitarbeiter_innen sind in der Personalakte abzulegen.

Bei Einstellungen ist darauf zu achten, dass das vorgelegte erweiterte Führungszeugnis nicht älter als sechs Monate ist.

Praktikant_innen
Beim Einsatz von Praktikant_innen sind diese in besonderem Maße auf die Verschwiegenheit und den Datenschutz hinzuweisen. Sie müssen im Zuge der Arbeitsvertragsunterzeichnung die gleiche Verpflichtung auf den Datenschutz unterzeichnen wie alle anderen Arbeitnehmer_innen und Angestellten. Des Weiteren ist die Einsichtnahme von personenbezogenen Daten auf die Notwendigkeit im Rahmen ihrer Tätigkeit hin zu überprüfen.

Bewerbungsverfahren/unterlagen
Eingehende Bewerbungsunterlagen sind möglichst ungeöffnet den zuständigen Stellen zuzuleiten. Nach Beendigung des Auswahlverfahrens sind die jeweiligen Anschreiben sechs Monate aufzubewahren und die Bewerbungsmappen unverzüglich an die Bewerber_innen zurückzusenden oder zu vernichten. Wird das Bewerbungsverfahren online durchgeführt sind diese Dateien nach Abschluss des Bewerbungsverfahrens unverzüglich zu löschen. Längere Aufbewahrung oder Weitergabe von Bewerberdaten an andere Arbeitgeber ist nur mit Rücksprache bei dem_der Betroffenen möglich.

5.2 Ehrenamtliche

Arten von Daten
Zu den ehrenamtlichen Mitarbeiter_innen fallen je nach Umfang des Engagements verschiedene Arten von personenbezogenen Daten in unterschiedlicher Menge an.

Grundlegend kann man sich an den Daten von hauptamtlichen Mitarbeiter_innen orientieren. Es gibt jedoch Besonderheiten.

Personenbezogene Daten bei ehrenamtlichen Mitarbeiter_innen

- Kontaktdaten
- Kontodaten für Abrechnungen
- Betreuervertrag und ergänzende Vereinbarungen
- Zeugnisse, Fortbildungsnachweise
- Beurteilungen
- Anwesenheitslisten
- Pläne zu Einsätzen
- Krankmeldungen
- Fahrt-, Reisekostenunterlagen
- Spesen-, Sachkostenabrechnungen

Erweitertes Führungszeugnis
Anders als bei hauptamtlichen Mitarbeiter_innen ist ein vorgelegtes erweitertes Führungszeugnis aufgrund des Bundeskinderschutzgesetzes (BKSchG) nicht beim Jugendring abzulegen. Es wird der Person wieder mitgegeben.

Es ist im gesetzlichen Rahmen nur möglich, die Vorlage mit Datum zu vermerken, um daraus den Zeitpunkt der Wiedervorlage in der Zukunft zu ermitteln.

Ehrenamtliche für Datenschutz sensibilisieren
Ehrenamtliche sind nach dem BayDSG genauso Mitarbeiter_innen wie Hauptamtliche. Deswegen sind sie genauso auf den Datenschutz hinzuweisen und mit Ihnen sind gleichfalls geeignete Maßnahmen zu treffen.

5.3 Datenschutz bei Maßnahmen

Bei der Organisation und Durchführung von Maßnahmen im Bereich der Kinder- und Jugendarbeit werden personenbezogene

Daten von Teilnehmer_innen und deren Eltern erhoben und verarbeitet.

In den einzelnen Planungs- und Durchführungsphasen gilt es die folgenden Besonderheiten aus datenschutzrechtlicher Sicht zu beachten:

Bei Freizeiten und Jugendbildungsmaßnahmen

Programmheft, Maßnahmen-Flyer
Programmhefte, Maßnahmenflyer oder Anmeldeformulare müssen die Datenschutzhinweise nach Art. 13 DSGVO enthalten. Die Kenntnisnahme der Datenschutzhinweise muss durch den_die Erziehungsberechtigten, ab dem 16. Lebensjahr durch den_die Teilnehmer_in mit deren Unterschrift bestätigt werden. Werden während der Maßnahmen Bild- und Filmaufnahmen erstellt, so ist dafür und für deren Nutzung ebenfalls eine Einwilligung einzuholen.
Eine Mustervorlage des Erfassungsbogens zur Durchführung von „Freizeiten“ inklusiver der Datenschutzhinweise ist als Anlage 3a angefügt.

⇢ Die Mustervorlage der Einwilligungserklärung für Foto- und Filmaufnahmen ist als **Anlage 4** beigefügt.

Online-Anmeldeverfahren
Wie im schriftlichen Anmeldeverfahren auch, müssen die Teilnehmer_innen auch im Online Anmeldeverfahren auf die Datenschutzhinweise gemäß Art. 13 DSGVO hingewiesen werden. Es empfiehlt sich die Datenschutzhinweise mit dem Anmeldeformular zu verknüpfen und die Anmeldung an die Kenntnisnahme der Datenschutzhinweise zu binden. In der Regel läuft eine Online-Anmeldung nicht über eigene Server, sodass hier wieder eine Auftragsverarbeitung vorliegt, für die wiederum ein Vertrag mit dem Dienstleister abgeschlossen werden muss. Im Falle einer unverschlüsselten Datenübermittlung sind die Betroffenen auf diesen Sachverhalt explizit hinzuweisen. Sollten diese damit nicht einverstanden sein, so sind sie auf andere Anmeldewege, die die Vertraulichkeit sicherstellen, hinzuweisen. Besondere Sensibilität in Sachen Datenschutz muss durch besondere Transparenz und Angabe von weiteren Informationen (z.B. Löschfristen) gezeigt werden.

Vernichtung von Teilnehmerausweisen, Ferienpässen
Die Ausweise/Pässe werden in der Regel drei bis sechs Monate nach Ende der Maßnahme datenschutzgerecht vernichtet. Bei besonderen Vorkommnissen (Krankheit, Verletzungen etc.) kann diese Frist auf bis zu zwei Jahre verlängert werden, um die Unterlagen zur Abwehr oder Klärung von Ansprüchen gegenüber Dritten nutzen zu können.

Zahlungsvorgang
Alle den Zahlungsvorgang betreffenden Informationen und Abläufe sind ausschließlich in der Buchhaltung zu bearbeiten. Eine Weitergabe von Informationen über unklare, offene Zahlungen an die durchführenden Mitarbeiter_innen der Maßnahme hat zu unterbleiben.

Datenübermittlung an Kooperationspartner/Dritte
Werden Maßnahmen in Kooperation mit Dritten durchgeführt und werden deswegen Daten übermittelt, so ist dies in den Datenschutzhinweisen anzugeben.
Der Austausch von Daten mit anderen öffentlichen Stellen (Jugendamt, Sozialamt, Gesundheitsamt) kann aufgrund Art. 5 Abs. 1 BayDSG mit Zweckbindung erfolgen.

Weitergabe von Daten an Betreuer_innen
Generell sind Bestimmungen zum Daten-

schutz und Datengeheimnis in Betreuer-/ Honorarverträge aufzunehmen.
Teilnehmerausweise mit besonders sensiblen personenbezogenen Daten sind vor unbefugtem Zugriff zu schützen und nur für Leitungspersonen zugänglich aufzubewahren.

Evaluation/Dokumentation
Für Statistiken können Daten verwendet werden, solange die Bestimmbarkeit von Personen nicht gegeben ist. Bei Jugendbildungsmaßnahmen werden in der Regel weniger Daten erhoben, sodass nichtzutreffendes unbeachtet bleiben kann.

5.4 Datenschutz bei Projekten

Bei Maßnahmen, die mehrere Projektträger gemeinsam durchführen, gibt es Besonderheiten bezüglich des Datenschutzes.

Verträge
In den Verträgen der Projektträger ist auf den Datenschutz hinzuweisen, und wie die Daten der jeweiligen Träger miteinander ausgetauscht werden.

Teilnehmer_innen
Von jede_r_m Teilnehmer_in ist eine Einwilligung einzuholen, aus der ersichtlich ist, dass an der Maßnahme mehrere Träger beteilig sind.

Einverständniserklärung
Auf der Einwilligung müssen die Träger benannt sowie eine Kurzbeschreibung der Maßnahme enthalten sein. Es sollte darauf hingewiesen werden dass die Träger zusammen arbeiten und Daten austauschen. Eine Adresse für den Widerruf muss festgelegt werden. Eine einzige Einverständniserklärung reicht nur aus, wenn alle Träger die gleichen Daten erheben. Bei weiteren Datenerhebungen müssen weitere Einverständniserklärungen eingeholt werden.
⇢ **Muster Anlage 3 und 3a**

Gesetzliche Grundlagen
Werden Maßnahmen im Rahmen z.B. des SGB gemeinsam durchgeführt, so sind die hierfür geltenden Vorschriften zu beachten.

Daten
Jeder Träger, der Daten erhebt ist für diese auch verantwortlich.

Schweigepflicht
Beim Austausch der Daten ist weiter die Schweigepflicht besonderer Berufsgruppen (z. B. staatliche Sozialarbeiter_innen, Sozialpädagog_innen) zu beachten. Sollen vertraulich offenbarte Sachverhalte der Klient_innen ausgetauscht werden, wird einen Schweigepflichtentbindung benötigt.

5.5 Datenschutz für Teilnehmer_innen

Für die Durchführung von Angeboten oder Veranstaltungen werden in der Regel Daten der Teilnehmer_innen benötigt.

Diese umfassen meist Grunddaten wie:

- Adresse, Telefon, E-Mail
- ggf. auch von Eltern
- Kontoverbindungen
- Zugehörigkeit Jugendgruppen
- Geburtsdatum
- Teilnahme

Häufig werden darüber hinaus gehende Daten benötigt, um die Veranstaltung entsprechend vorbereiten zu können (z.B. Essen) oder für den Notfall gerüstet zu sein:

- Religion
- Angaben zur Ernährungsweise

- Allergien
- Erkrankungen
- Letzte Impfungen
- Einschränkungen (ADHS)

Dabei handelt es sich um besondere personenbezogene Daten, die sensible zu handhaben sind. Hinweise dazu sind auch im Abschnitt zu Maßnahmen enthalten.

Bilder, Videos von Teilnehmer_innen:
Es ist das Recht am eigenen Bild zu beachten und die nötigen Einverständniserklärungen einzuholen.

5.6 Bußgelder und Spenden

Spenden
Erhält der Jugendring Spenden von Personen ist abzuklären, ob die Nennung als Spender_in, z.B. in Publikationen gewünscht ist.

Bußgelder
Manche Jugendringe erhalten von Gerichten und Staatsanwaltschaften Bußgeldzuweisungen. Sie sind dann für die Abwicklung der Zahlungen selber verantwortlich.
In diesem Rahmen erhalten sie in der Regel den Namen und die Adresse der Zahlungspflichtigen, die Höhe des Bußgelds und das Aktenzeichen. Darüber hinaus gehende Informationen wie z.B. Fallakten oder Angaben zum Vergehen werden nicht benötigt und sollten auch nicht angenommen werden. Für die Abwicklung der Zahlung kann das Aktenzeichen oder ein anderer pseudonymer Schlüssel verwendet werden, um nicht den Namen nutzen zu müssen.
Es empfiehlt sich, Listen zur Kontrolle des Zahlungseingangs, besonders bei Ratenzahlungen, darauf aufbauend pseudonym zu führen. Mit Bußgeldern befasste Mitarbeiter_innen sind auf die besondere Schutzwürdigkeit der Informationen hinzuweisen.

5.7 EDV und Auftragsdatenverarbeitung

EDV – technische und organisatorische Maßnahmen. Hier gelten die analogen Vorschriften die bereits in Kapitel 3. Der_Die Verantwortliche ausführlich beschrieben sind.

6. Quellen und Anlagen

Quellen

- **Datenschutzgrundverordnung DSGVO** Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG –

- **Bayerisches Datenschutzgesetz** BayDSG in der Neufassung ab 26. April 2018

- **Bundesdatenschutzgesetz** BDSG in der Nufassung vom 27. April 2017

- **Arbeitshilfen des Bayerischen Landesbeauftragten für Datenschutz;** www.datenschutz-bayern.de [Abrufdatum 18.09.2009]

Anlagen

- Anlage 1 **Sieben Tipps für mehr Datenschutz am Arbeitsplatz**
- Anlage 2 **Muster Verzeichnis einer Verarbeitungstätigkeit**
- Anlage 3 **Muster Datenschutzhinweise bei Veranstaltungen**
- Anlage 3a **Muster Erfassungsbogen für „Freizeiten“ mit Datenschutzhinweisen**
- Anlage 4 **Muster Einwilligungserklärung Foto- und Filmaufnahmen**
- Anlage 5 **Checkliste DSGVO**
- Anlage 6 **Aufbewahrungsfristen**
- Anlage 7 **Merkblatt allgemeine Infos**

Anlage 1

Sieben Tipps für mehr Datenschutz am Arbeitsplatz

1. Benutzerkennungen und Passwörter gehen nur Sie etwas an

Denn über diese Informationen melden Sie sich nicht nur an, sondern Sie machen sich auch identifizierbar. Wenn Sie Unberechtigte mit Ihren Zugangsdaten arbeiten lassen, fällt dies unter Umständen auf Sie zurück. Schließlich tritt die unberechtigte Person mit Ihrem Namen auf. Kommt es zu einem Schaden, müssen Sie unter Umständen die Konsequenzen tragen. Daher behalten Sie Ihre Zugänge bei sich.

2. Nutzen Sie sichere Passwörter

Die goldene Regel für ein sicheres Passwort lautet: es sollte von Außenstehenden nicht als sinnvolles Wort erkannt werden, oder beispielsweise keine Namen von Ehepartner_innen, Haustieren oder Ihr Geburtsdatum verwendet werden. Idealerweise setzen Sie Ihre Passwörter auch aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (*, #, §, $,%,&) zusammen. Um ein solches Passwort zu erhalten, gibt es einen einfachen Trick: Denken Sie sich einen Satz aus, den Sie sich gut merken können. Von diesem Satz verwenden Sie nur die Anfangsbuchstaben und ersetzen einzelne Buchstaben durch Zahlen und Sonderzeichen.

Ein Beispiel wäre: „Wir zwei essen gerne Nudeln mit Soße“. Die Anfangsbuchstaben ergeben die Kombination „WzegNmS“. Nun kommen Zahlen und Sonderzeichen ins Spiel. Hier können Sie Ihrer Fantasie freien Lauf lassen. Bei unserem Beispiel ersetzen wir das z durch eine 2 und fügen ein „#“ ein. Somit würde sich folgendes Passwort ergeben: „ W2egNmS#“.

3. Bildschirmschoner mit Kennwortschutz bei längerer Abwesenheit

Damit Sie Ihren PC und damit Ihre Daten vor dem Zugriff Dritter schützen, sollten Sie ihn immer durch ein Passwort sperren. Der Bildschirmschoner kann so eingerichtet werden, dass dieser nach einer gewissen Zeit den Computer automatisch sperrt. Empfohlen wird, dass die Sperre fünf Minuten nach der letzten Benutzereingabe mit dem Bildschirmschonereinsetzt.

Wenn Sie für längere Zeit den Arbeitsplatz verlassen, dann melden Sie sich von Ihrem Rechner ab und aktivieren die Sperre durch Drücken der Windowstaste + L.

4. Helfen Sie unbekannten Personen

Begegnen Sie in Ihrer Abteilung oder auf dem Flur unbekannten Personen, nehmen Sie sich derer an und fragen Sie nach, ob Sie helfen können und zu wem die Person möchte. Begleiten Sie diese Person zum_zur genannten Kollegen_in, so tragen Sie dazu bei, dass sich Unbefugte und Unbekannte nicht unbeaufsichtigt in unseren Einrichtungen aufhalten.

5. Geben Sie Informationen nicht telefonisch heraus!

Sollte Ihnen die anrufende Person nicht bekannt sein, sollten Sie Vorsicht walten lassen und die Auskunft am Telefon verweigern. Bitten Sie um eine schriftliche Anfrage (E-Mail möglich), so haben Sie auch Zeit zu prüfen, ob eine Information überhaupt gegeben werden darf.

6. Prüfen Sie Downloads und E-Mail-Anhänge

Viren werden gerne per Dateianhänge verbreitet. Öffnen Sie daher nur vertrauenswürdige Anhänge von Personen, die Sie tatsächlich kennen. Selbst von bekannten Personen können in dessen Unwissenheit Mails verschickt werden (Spear Phishing)

7. Machen Sie reinen Tisch

Akten und alle anderen Unterlagen, die Daten zu Personen enthalten, sollten nach Möglichkeit stets unter Verschluss gehalten werden. Dies gilt vor allem dann, wenn Sie längere Zeit nicht im Büro sind. Spätestens nach Feierabend sollten solche Dinge nicht mehr auf Ihrem Schreibtisch zu finden sein. Denken Sie auch an das Abschließen von Ablagen und Aktenschränken. Schließlich gehen die personenbezogenen Daten auch niemanden vom Reinigungspersonal etwas an.

Anlage 2

Bezeichnung der Verarbeitungstätigkeit

1. Allgemeine Angaben

Bezeichnung der Verarbeitungstätigkeit		**Stand:**
Verantwortliche_r (Bezeichnung, Anschrift, E-Mail-Adresse und Telefonnummer der öffentlichen Stelle)		
Falls zutreffend: Angaben zu weiteren gemeinsam für die Verarbeitung Verantwortlichen (jeweils Bezeichnung, Anschrift, E-Mail-Adresse und Telefonnummer)		
Behördlicher Datenschutzbeauftragte_r (Name, dienstliche Anschrift, E-Mail-Adresse, Telefonnummer)		

2. Zwecke und Rechtsgrundlagen der Verarbeitung

Zwecke
Rechtsgrundlagen

3. Kategorien der personenbezogenen Daten

Lfd. Nr.	Bezeichnung der Daten

4. Kategorien der betroffenen Personen

Lfd. Nr.	Betroffene Personen

5. Kategorien der Empfänger, denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen

Lfd. Nr.	Empfänger_in	Anlass der Offenlegung

6. Falls zutreffend: Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation

Lfd. Nr.	Drittland oder internationale Organisation	Geeignete Garantien im Falle einer Übermittlung nach Art. 49 Abs. 1 Unterabsatz 2 DSGVO

7. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

Lfd. Nr.	Löschungsfrist

8. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO, ggf. einschließlich der Maßnahmen nach Art. 8 Abs. 2 Satz 2 BayDSG-E 2018

Weitere Angaben

9. Verantwortliche Organisationseinheit

Dienststelle / Sachgebiet / Abteilung

10. Datenschutz-Folgenabschätzung

Ist für die Form der Verarbeitung eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich? ☐ Ja, ☐ Nein Falls ja, bis wann durchzuführen oder zu überprüfen
Begründung

11. Stellungnahme des_der behördlichen Datenschutzbeauftragten

Liegt eine Stellungnahme des_der behördlichen Datenschutzbeauftragten vor? ☐ Ja ☐ Nein
Ggf. nähere Erläuterung

Anlage 3

Datenschutzhinweise hinsichtlich einer Veranstaltung gemäß Art. 13 DSGVO

1. Name und Kontaktdaten des_der Verantwortlichen

Verantwortlich für die Datenverarbeitung ist:

2. Datenschutzbeauftragte_r:

3. Zweck der Verarbeitung

a) Einzelne personenbezogene Daten werden zur Durchführung des jeweils zugrunde liegenden Vertrags, zu Zwecken des Nachweises von Belegen und/oder und zur Beantragung von Fördermitteln an Dritte *(Ministerien, Fördermittelgeber oder ähnliches)* weitergeben und dienen damit dem Zweck des *SJR/KJR/BezJR*.

b) Fotos und/oder Videos dienen ausschließlich der Öffentlichkeitsarbeit des Veranstalters.

4. Rechtsgrundlagen der Verarbeitung

a) Sämtliche personenbezogenen Daten bis auf Fotos und/oder Videos werden auf Grundlage von Art. 6 Abs. 1 Buchstabe b DSGVO erhoben, da diese für die Begründung und Durchführung des zugrundeliegenden Vertrages zwingend erforderlich sind.

b) Die Verarbeitung von Fotos und/oder Videos (Erhebung, Speicherung und Weitergabe an Dritte (s. unter 5.) erfolgt aufgrund ausdrücklicher Einwilligung des_der Betroffenen, mithin gemäß Art. 6 Abs. 1 Buchstabe a DSGVO. Die Veröffentlichung ausgewählter Bilddateien in (Print-)Publikationen des Veranstalters sowie auf dessen Social-Media-Seiten o.ä. ist für die Öffentlichkeitsarbeit des Veranstalters erforderlich und dient damit der Wahrnehmung berechtigter Interessen der Beteiligten, Art. 6 Abs. 1 Buchstabe f DSGVO.

c) Die Weitergabe personenbezogener Daten an Dritte (s. unter 5.) erfolgt auf Grundlage von Art. 6 Abs. 1 Buchstabe f DSGVO, da dies zur Wahrnehmung berechtigter Interessen des *SJR/KJR/BezJR* erforderlich ist.

5. Kategorien von Empfänger_innen der personenbezogenen Daten

Ihre personenbezogenen Daten werden weitergegeben an:

a) **Dritte:** *Ministerien, Fördermittelgeber oder ähnliches*

b) Auch der Upload von Daten im Internet stellt eine Weitergabe an Dritte dar.

c) Für den Fall, dass eine ärztliche Versorgung notwendig ist, werden die notwendigen Daten an Ärzte, Krankenhäuser oder sonstiges medizinisches Versorgungspersonal weitergegeben.

6. Dauer der Speicherung der personenbezogenen Daten

a) Mit Ausnahme der Fotos und/oder Videos werden personenbezogene Daten nach der Erhebung nur so lange gespeichert, wie dies für die jeweilige Vertragserfüllung *(Dokumentationspflicht gegenüber Dritten o.ä.)* erforderlich ist. Im Anschluss hieran werden sämtliche damit im Zusammenhang stehende Daten unwiderruflich gelöscht.

b) Fotos und/oder Videos, welche für die Zwecke der Öffentlichkeitsarbeit des Veranstalters gemacht werden, werden vorbehaltlich eines Widerrufs der Einwilligung des_der Betroffenen auf unbestimmte Zeit zweckgebunden gespeichert.

7. Pflicht zur Bereitstellung von Daten

Vorbehaltlich der Einverständniserteilung zur Verarbeitung von Fotos und/oder Videos sind Sie dazu verpflichtet, die geforderten Daten anzugeben. Nur so kann eine Anmeldung erfolgen.

8. Widerrufsrecht bei Einwilligung

Die Einwilligung zur Verarbeitung der Fotos und/oder Videos kann jeder Zeit für die Zukunft widerrufen werden. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung wird durch diesen nicht berührt.

9. Betroffenenrechte

Nach der Datenschutzgrundverordnung stehen Ihnen folgende Rechte zu:

a) Werden Ihre personenbezogenen Daten verarbeitet, so haben Sie das Recht Auskunft über die zu Ihrer Person gespeicherten Daten zu erhalten (Art. 15 DSGVO).

b) Sollten unrichtige personenbezogenen Daten verarbeitet werden, steht Ihnen ein Recht auf Berichtigung zu (Art. 16 DSGVO).

c) Liegen die gesetzlichen Voraussetzungen vor, so können Sie die Löschung oder Einschränkung der Verarbeitung verlangen sowie Widerspruch gegen die Verarbeitung einlegen (Art. 17, 18, 21 DSGVO).

d) Wenn Sie in die Datenverarbeitung eingewilligt haben oder ein Vertrag zur Datenverarbeitung besteht und die Datenverarbeitung mithilfe automatisierter Verfahren durchgeführt wird, steht Ihnen gegebenenfalls ein Recht auf Datenübertragbarkeit zu (Art. 20 DSGVO).

Sollten Sie von den genannten Rechten Gebrauch machen, prüft der_die Verantwortliche, ob die gesetzlichen Voraussetzungen hierfür vorliegen. Weiterhin besteht ein Beschwerderecht beim Bayerischen Landesbeauftragten für den Datenschutz.

Anlage 3a

Diese Vorlage enthält lediglich die Mindestanforderungen, die für entsprechende Anmeldeformulare für Freizeiten/Aktionen o.ä. empfohlen werden. Anpassungen an den Einzelfall sind stets erforderlich. Darüber hinaus besteht für den_die Verwender_in je nach Einzelfall sogar die Pflicht, (etwa bei Unternehmungen ins Ausland), diese zu erweitern bzw. im Rahmen von Allgemeinen Teilnahmebedingungen o.ä. zusätzliche Inhalte aufzunehmen. Diese Mustervorlage kann daher keine Gewähr für Vollständigkeit und dauerhafte sowie vollumfängliche Rechtssicherheit bieten.

Verbindliche Anmeldung zur Freizeit/Aktion

am/von bis: _____

in: _____

Daten des Kindes

Name, Vorname: _____

Alter: _____

Wohnsitz des Kindes: _____
(falls abweichend von der Adresse der Eltern)**:**

Mobil: _____
(wenn vorhanden)**:**

E-Mail: _____
(wenn vorhanden)**:**

Krankenversicherung: _____

Name des_der Hauptversicherten: _____

Versicherungs-nummer: _____

Hier besteht die Möglichkeit, darauf hinzuweisen, dass Teilnehmer_innen verpflichtet sind, Impfpass, Versicherungskarte, Auslandskrankenschein o.ä. bei sich zu führen.

Daten der_des Erziehungsberechtigten

Vor- und Nachnamen: _____

Adresse: _____

Festnetz: _____

Mobil: _____

E-Mail: _____

In dringenden Fällen kann sich die Leitung an folgende erreichbare Personen wenden:

Vor- und Nachnamen:

Mobil: _____

Vor- und Nachnamen: _____

Mobil: _____

Folgende Informationen sind für die Übernahme der Aufsichtspflicht während der Teilnahme Ihres Kindes an der oben genannten Aktion/Freizeit unerlässlich und **müssen** von den_der Personensorgeberechtigten angegeben werden:

_____

_____

Krankheiten oder Besonderheiten meines Kindes, etwa. Allergien, chronische Erkrankungen, regelmäßiger Medikamentenbedarf, soziale Schwächen, bekannte Neigung zu Heimweh etc.:

_____

_____

_____

Besondere Essgewohnheiten/Lebensmittel-Unverträglichkeiten:

Wir möchten auch Kindern und Jugendlichen mit Beeinträchtigungen eine Teilnahme an unseren Maßnahmen ermöglichen. Dies kann aber nur mit einem offenen Gespräch im Vorfeld der Anmeldung funktionieren, in dem wir nach Grad der Beeinträchtigung bewerten können, ob unsere (überwiegend) ehrenamtlichen Jugendleiter_innen eine Aufsicht und angemessene Betreuung leisten können.

Mein Kind kann (Zutreffendes bitte ankreuzen bzw. ausfüllen)**:**

- ☐ gut schwimmen
- ☐ schlecht schwimmen
- ☐ nicht schwimmen

Mein Kind besitzt folgendes Schwimmabzeichen**:**

Mein Kind ist geimpft gegen (Zutreffendes bitte ankreuzen)**:**

- ☐ Tetanus
- ☐ FSME (Zecken)

Einverständniserklärungen (bitte ankreuzen)**:**

☐ Ich erkläre mich damit einverstanden, dass mein Kind an den in der Ausschreibung beschriebenen Aktivitäten teilnehmen darf.

☐ Ich erkläre mich damit einverstanden, dass die Leitung etwaige Zecken am Körper meines Kindes entfernen darf.

☐ Ich erkläre mich damit einverstanden, dass im Rahmen der Aktion/Freizeit Bilder und/oder Videos von dem_n Teilnehmer_innen gemacht werden und zur Veröffentlichung

- auf der Homepage des Veranstalters
- in (Print-)Publikationen des Veranstalters
- auf der Facebook-Seite des Veranstalters
- …

verwendet und zu diesem Zwecke auch abgespeichert werden dürfen. Die Fotos und/oder Videos dienen ausschließlich der Öffentlichkeits- und/oder Elternarbeit des Veranstalters. Diese Einverständniserklärung ist freiwillig und kann gegenüber dem Veranstalter jederzeit mit Wirkung für die Zukunft widerrufen werden. Sind die Aufnahmen im Internet verfügbar, erfolgt die Entfernung soweit dies dem Veranstalter möglich ist. Ich bin mir darüber im Klaren, dass Fotos und/oder Videos im Internet von beliebigen Personen abgerufen werden können. Es kann trotz aller technischen Vorkehrungen nicht ausgeschlossen werden, dass solche Personen die Fotos und/oder Videos weiterverwenden oder an andere Personen weitergeben.[1]

☐ Ich erkläre mich damit einverstanden, dass die Teilnehmer_innen in Gruppen altersgemäße Aktivitäten auch ohne Aufsicht, jedoch nach Erlaubnis durch die Leitung, eigenständig unternehmen dürfen.

Optional:

☐ Ich habe die Allgemeinen Reisebedingungen des Veranstalters gelesen und erkläre mich ausdrücklich damit einverstanden.

Sollte an dieser Stelle auf die Allgemeinen Geschäftsbedingungen auf der Homepage des Veranstalters verwiesen werden, so muss der exakte Link genannt werden und nicht nur der Link zur Startseite. Überdies muss diese Erklärung ausdrücklich bestätigt werden (durch Ankreuzen auf Papier oder Opt-In-Funktionen im Online-Verfahren).

[1] Auch bei der Veröffentlichung sonstiger **Daten im Internet**, wie z.B. Namen, Platzierungen bei Wettbewerbern, besondere Leistungen o.ä. sind nach der EU-Datenschutzgrundverordnung (DSGVO) ähnlich hohe Anforderungen an die Einverständniserklärung zu stellen.

Nach Inkrafttreten der EU-Datenschutzverordnung ab dem 25.05.2018:

☐ **Ich habe die beigefügten Datenschutzhinweise gemäß Art. 13 DSGVO des Veranstalter erhalten und gelesen.**

Ort/Datum

Unterschrift des_der Teilnehmers_in (ab 16 Jahre)[2]

Unterschrift der Personensorgeberechtigten

*Nach dem neuen Datenschutzrecht, welches ab dem **25.05.2018** gilt, muss jede_r Betroffene umfassend gemäß Art. 13 DSGVO informiert werden, wenn Daten von ihm_ihr verarbeitet (erhoben, gespeichert, weitergegeben, gelöscht etc.) werden. Der Bayerische Jugendring hat hierzu bereits einen Leitfaden „Datenschutz in der Jugendarbeit" veröffentlicht, der sich unter www.bjr.de/service/presse/details/datenschutz-in-der-jugendarbeit-2062.html abrufen lässt.*

Die folgenden Musterformulierungen richten sich nach der Mustervorlage „Erfassungsbogen für Freizeiten" und orientieren sich an klassischen Ferienfreizeitmaßnahmen, Aktionen o.ä. Diese Formulierungen dürfen allerdings nicht blind kopiert werden. An einzelnen Stellen bedarf es einer Vervollständigung bzw. Differenzierung je nach Einzelfall. Jedoch kann und sollte diese Mustervorlage als Grundlage für spezifischere Datenschutzhinweise je nach Verwendungszweck eingesetzt werden.

[2] Gemäß Art. 8 der DSGVO dürfen Jugendliche ab 16 Jahren ihr Einverständnis zur Datenverarbeitung selbst erteilen. Für Kinder und Jugendliche unter 16 Jahren bedarf es des Einverständnisses der Eltern.

Datenschutzhinweise hinsichtlich der Freizeit/Aktion gemäß Art. 13 DSGVO

1. Name und Kontaktdaten des_der Verantwortlichen

Verantwortlich für die Datenverarbeitung ist … (Name und Kontaktdaten des_der Verantwortlichen = Verein, vertreten durch den Vorsitzenden, Hauptverantwortliche_r Gruppenleiter_in etc.)

2. Kontaktdaten des_der Datenschutzbeauftragten[3]

3. Zweck der Verarbeitung

a) Ihre Daten, respektive die Ihres Kindes werden verarbeitet, um den Anforderungen an die übernommene Aufsichtspflicht während der Freizeit/Aktion umfassend gerecht zu werden, etwaigen Unfällen oder sonstigen Beeinträchtigungen an Rechtsgütern Ihres Kindes möglichst umfassend vorzubeugen, sowie den Kontakt zu den Personensorgeberechtigten frühzeitig herstellen zu können.

b) Weiterhin werden einzelne personenbezogene Daten zu Zwecken der Beantragung von Fördermitteln[4] an Dritte *(Dachverband/Fördermittelgeber o.ä.)* weitergeben und dienen damit dem Zweck der Vereins-/Verbandsförderung.

c) Fotos und/oder Videos dienen ausschließlich der Öffentlichkeits- und/oder Elternarbeit des Veranstalters.

4. Rechtsgrundlagen der Verarbeitung

a) Sämtliche personenbezogenen Daten bis auf Fotos und/oder Videos werden auf Grundlage von Art. 6 Abs. 1 Buchstabe b DSGVO erhoben, da diese für die Begründung und Durchführung des zugrundeliegenden Vertrages zur Übernahme der Aufsichtspflicht für den genannten Zeitraum zwingend erforderlich sind.

b) Die Verarbeitung von Fotos und/oder Videos (Erhebung, Speicherung und Weitergabe an Dritte (s. unter 5.) erfolgt aufgrund ausdrücklicher Einwilligung des_der Personensorgeberechtigten bzw. des_der Betroffenen, mithin gemäß Art. 6 Abs. 1 Buchstabe a DSGVO. Die Veröffentlichung ausgewählter Bilddateien in (Print-

[3] nur soweit der Veranstalter zur Bestellung eines Datenschutzbeauftragten verpflichtet ist. Dies ist dann **nicht** der Fall, wenn weniger als 10 Personen im Verein/Verband ö.a. ständig mit der automatisierten Datenverarbeitung beschäftigt sind. Besteht keine Verpflichtung zur Bestellung eines eigenen Datenschutzbeauftragten, genügen die Kontaktdaten des_der Verantwortlichen.

[4] Sollten Daten aus anderen Gründen an Dritte weitergegeben werden, sind auch diese Gründe/Zwecke hier aufzuführen.

)Publikationen des Veranstalters sowie auf deren Homepage/Facebook-Seite o.ä. ist für die Öffentlichkeitsarbeit der Veranstalter erforderlich und dient damit der Wahrnehmung berechtigter Interessen der Beteiligten, Art. 6 Abs. 1 Buchstabe f DSGVO.

c) Die Weitergabe personenbezogener Daten an Dritte (s. unter 5.) erfolgt auf Grundlage von Art. 6 Abs. 1 Buchstabe f DSGVO, da dies zur Wahrnehmung berechtigter Interessen des Vereins/Verbands erforderlich ist.

5. Kategorien von Empfänger_innen der personenbezogenen Daten

Ihre personenbezogenen Daten bzw. die Ihres Kindes werden weitergegeben an:

a) **Dritte:** *(z.B. Dachverband, Fördermittelgeber o.ä., Webhoster, Cloud-Computing-Anbieter, Eltern, Sonstige im Zusammenhang mit der Erstellung und Veröffentlichung von (Print-)Publikationen),* um … *nähere Beschreibung des Grundes der Datenweitergabe, vgl. unter 3.*

b) **Verbands-/Vereinsmitglieder …** *nähere Beschreibung des Grundes der Datenweitergabe, vgl. unter 3.*

c) Auch der Upload von Daten im Internet stellt eine Weitergabe an Dritte dar.

d) Für den Fall, dass eine ärztliche Versorgung notwendig ist, werden die notwendigen Daten an Ärzt_innen, Krankenhäuser oder sonstiges medizinisches Versorgungspersonal weitergegeben. Auch dies dient dem Schutz und der Sicherheit Ihres Kindes.

6. Dauer der Speicherung der personenbezogenen Daten

a) Mit Ausnahme der Fotos und/oder Videos werden personenbezogene Daten nach der Erhebung nur so lange gespeichert, wie dies für die jeweilige Vertragserfüllung *(Übernahme der Aufsichtspflicht, Dokumentationspflicht gegenüber Dritten o.ä.)* erforderlich ist. Im Anschluss hieran werden sämtliche damit im Zusammenhang stehende Daten unwiderruflich gelöscht.

b) Fotos und/oder Videos, welche für die Zwecke der Öffentlichkeits- und/oder Elternarbeit des Veranstalters gemacht werden, werden vorbehaltlich eines Widerrufs der Einwilligung des_der Betroffenen auf unbestimmte Zeit zweckgebunden gespeichert.

7. Pflicht zur Bereitstellung von Daten

Vorbehaltlich der Einverständniserteilung zur Verarbeitung von Fotos und/oder Videos sind Sie vertraglich (Vertrag zur Übernahme der Aufsichtspflicht) dazu verpflichtet, die geforderten Daten anzugeben. Nur so kann die Übernahme der Aufsichtspflicht gewährleistet werden.

Wenn Sie die erforderlichen Daten nicht angeben, kann der zugrunde liegende Vertrag mit Ihnen nicht geschlossen werden, was eine Teilnahme Ihres Kindes an der Freizeit/Aktion verhindert.

8. Widerrufsrecht bei Einwilligung

Die Einwilligung zur Verarbeitung der Fotos und/oder Videos kann jeder Zeit für die Zukunft widerrufen werden. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung wird durch diesen nicht berührt.

9. Betroffenenrechte

Nach der Datenschutzgrundverordnung stehen Ihnen folgende Rechte zu:

a) Werden Ihre personenbezogenen Daten verarbeitet, so haben Sie das Recht Auskunft über die zu Ihrer Person gespeicherten Daten zu erhalten (Art. 15 DSGVO).

b) Sollten unrichtige personenbezogenen Daten verarbeitet werden, steht Ihnen ein Recht auf Berichtigung zu (Art. 16 DSGVO).

c) Liegen die gesetzlichen Voraussetzungen vor, so können Sie die Löschung oder Einschränkung der Verarbeitung verlangen sowie Widerspruch gegen die Verarbeitung einlegen (Art. 17, 18, 21 DSGVO).

d) Wenn Sie in die Datenverarbeitung eingewilligt haben oder ein Vertrag zur Datenverarbeitung besteht und die Datenverarbeitung mithilfe automatisierter Verfahren durchgeführt wird, steht Ihnen gegebenenfalls ein Recht auf Datenübertragbarkeit zu (Art. 20 DSGVO).

Sollten Sie von den genannten Rechten Gebrauch machen, prüft der_die Verantwortliche, ob die gesetzlichen Voraussetzungen hierfür vorliegen. Weiterhin besteht ein Beschwerderecht beim Bayerischen Landesbeauftragten für den Datenschutz.

Anlage 4

Einverständniserklärung zu Foto- und Videoaufnahmen

Hintergrund

Nach dem neuen EU-Datenschutzrecht, welches ab dem **25.05.2018** gilt, sind Foto- und/oder Videoaufnahmen, auf denen Personen zu erkennen sind, grundsätzlich nur noch mit schriftlicher Einwilligung des/der Abgebildeten rechtmäßig. (In die Kamera lächeln ist keine ausreichende Einwilligung!). Ausnahmen von diesem Grundsatz gelten insoweit nur für Presse, Rundfunk, Wissenschaft und Kunst. Da das EU-Datenschutzrecht höherrangiger ist als das alt bekannte deutsche Kunsturheberrechtsgesetz (KUG), kann man sich in Zukunft auch nicht mehr darauf berufen, die abgebildeten Personen seien nur „Beiwerk“ des Bildes, § 23 KUG. Das EU-Recht verdrängt deutsches Recht an dieser Stelle.

Fotos und/oder Videoaufnahmen sind nur ausnahmsweise auch ohne Einwilligung des/der Abgebildeten zulässig, wenn dies

- zur Erfüllung eines Vertrages erforderlich ist
- zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist
- zur Wahrung berechtigter Interessen des Vereins/Verbandes/Jugendrings erforderlich ist und die schutzwürdigen Interessen des/der Abgebildeten nicht überwiegen.

Für Foto- und/oder Filmaufnahmen von Kindern, Jugendlichen sowie Erwachsenen während Freizeitmaßnahmen, sonstigen Aktionen oder Veranstaltungen dürfte **in der Regel** keine dieser Ausnahmen greifen, weswegen stets eine schriftliche Einverständniserklärung einzuholen ist.

Bei Kindern und Jugendlichen unter 16 Jahren braucht es hierfür das Einverständnis der Eltern, Jugendliche ab 16 dürfen das Einverständnis selbst erteilen.

Zu beachten ist auch, dass sich aus der Einwilligung ergeben muss, für welche Zwecke die Aufnahmen verwendet werden sollen, damit dem/der Einwilligenden klar ist, worauf er_sie sich einlässt.

Einverständniserklärung zu Foto- und/oder Filmaufnahmen

Ich erkläre mich damit einverstanden, dass im Rahmen der *Aktion/Freizeit/Veranstaltung etc. der Veranstalter* Bilder und/oder Videos von den anwesenden Teilnehmer_innen gemacht werden und zur Veröffentlichung

- auf der Homepage des Veranstalters *(Benennung der URL)*
- in (Print-)Publikationen des Veranstalters
- auf der Facebook-Seite des Veranstalters
- …*(weitere Verwendungszwecke)*

verwendet und zu diesem Zwecke auch abgespeichert werden dürfen. Die Fotos und/oder Videos dienen ausschließlich der Öffentlichkeits- und/ oder Elternarbeit des Veranstalters.

Ich bin mir darüber im Klaren, dass Fotos und/oder Videos im Internet von beliebigen Personen abgerufen werden können. Es kann trotz aller technischer Vorkehrungen nicht ausgeschlossen werden, dass solche Personen die Fotos und/oder Videos weiterverwenden oder an andere Personen weitergeben.

Diese Einverständniserklärung ist freiwillig und kann gegenüber dem Veranstalter jederzeit mit Wirkung für die Zukunft widerrufen werden. Sind die Aufnahmen im Internet verfügbar, erfolgt die Entfernung, soweit dies dem Veranstalter möglich ist.

Ort/Datum:

Unterschrift des/der Teilnehmers_in ab 16 Jahre[5]:

Unterschrift des/der Personensorgeberechtigten:

---

[5] Gemäß Art. 8 der DSGVO dürfen Jugendliche ab 16 Jahren ihr Einverständnis zur Datenverarbeitung selbst erteilen. Für Kinder und Jugendliche unter 16 Jahren bedarf es einer Einverständniserklärung der Eltern.

Nach dem neuen Datenschutzrecht, welches ab dem **25.05.2018** gilt, muss jede_r Betroffene umfassend gemäß Art. 13 DSGVO informiert werden, wenn Daten von ihm/ihr verarbeitet (erhoben, gespeichert, weitergegeben, gelöscht etc.) werden. Hierzu zählen auch Foto- und/oder Videoaufnahmen. Der Bayerische Jugendring hat hierzu bereits einen Leitfaden „Datenschutz in der Jugendarbeit“ veröffentlicht, der unter www.bjr.de/service/presse/details/datenschutz-in-der-jugendarbeit-2062.html abrufbar ist.

Die folgenden Musterformulierungen dürfen nicht blind kopiert werden. An einzelnen Stellen bedarf es einer Vervollständigung bzw. Differenzierung je nach Einzelfall. Jedoch kann und sollte diese Mustervorlage als Grundlage für spezifischere Datenschutzhinweise je nach Verwendungszweck eingesetzt werden.

Datenschutzhinweise hinsichtlich der Herstellung und Verwendung von Foto- und/oder Videoaufnahmen gemäß Art. 13 DSGVO

1. Name und Kontaktdaten des/der Verantwortlichen:

Verantwortlich für die Datenverarbeitung ist…(Name und Kontaktdaten des/der Verantwortlichen = Verein, vertreten durch den/die Vorsitzende_n, Hauptverantwortliche_n Gruppenleiter_in / Jugendring, vertreten durch den/die Vorsitzende_n etc.)

2. Kontaktdaten des/der Datenschutzbeauftragten[6]:

3. Zweck der Verarbeitung:

Die Fotos und/oder Videos dienen ausschließlich der Öffentlichkeits- und/oder Elternarbeit des Veranstalters.

4. Rechtsgrundlagen der Verarbeitung:

Die Verarbeitung von Fotos und/oder Videos (Erhebung, Speicherung und Weitergabe an Dritte (s. unter 5.) erfolgt aufgrund ausdrücklicher Einwilligung des/der Personensorgeberechtigten bzw. des/der Betroffenen, mithin gemäß Art. 6 Abs. 1 Buchstabe a DSGVO. Die Veröffentlichung ausgewählter Bilddateien in (Print)Publikationen des Veranstalters sowie auf deren Homepage /Facebook-Seite o.ä. ist für die Öffentlichkeitsarbeit der Veranstalter erforderlich und dient damit der Wahrnehmung berechtigter Interessen der Beteiligten, Art. 6 Abs. 1 Buchstabe f DSGVO.

5. Kategorien von Empfänger_innen der personenbezogenen Daten:

Fotos und/oder Videos werden weitergeben an:

a) **Dritte:** *(z.B. Dachverband, Fördermittelgeber o.ä., Webhoster, Cloud-Computing-Anbieter, Eltern, Sonstige im Zusammenhang mit der Erstellung und Veröffentlichung von (Print)Publikationen),* um…*nähere Beschreibung des Grundes der Datenweitergabe, vgl. unter 3.*

b) **Verbands-/Vereinsmitglieder***: nähere Beschreibung des Grundes der Datenweitergabe, vgl. unter 3.*

a) Auch der Upload von Daten im Internet stellt eine Weitergabe an Dritte dar.

6. Dauer der Speicherung der personenbezogenen Daten:

6nur soweit der Veranstalter zur Bestellung eines_einer Datenschutzbeauftragten verpflichtet ist. Dies ist dann **nicht** der Fall, wenn weniger als zehn Personen im Verein/Verband ö.a. ständig mit der automatisierten Datenverarbeitung beschäftigt sind. Besteht keine Verpflichtung zur Bestellung eines eigenen Datenschutzbeauftragten, genügen die Kontaktdaten des_der Verantwortlichen. Jugendringe brauchen stets einen Datenschutzbeauftragten.-

Fotos- und/oder Videos, welche für die Zwecke der Öffentlichkeits- und/oder Elternarbeit des Veranstalters gemacht werden, werden vorbehaltlich eines Widerrufs der Einwilligung des/der Betroffenen auf unbestimmte Zeit zweckgebunden gespeichert.

7. Widerrufsrecht bei Einwilligung:

Die Einwilligung zur Verarbeitung der Fotos und/oder Videos kann jederzeit für die Zukunft widerrufen werden. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung wird durch diesen nicht berührt.

9. Betroffenenrechte:

Nach der Datenschutzgrundverordnung stehen Ihnen folgende Rechte zu:

a) Werden ihre personenbezogenen Daten verarbeitet, so haben sie das Recht Auskunft über die zu ihrer Person gespeicherten Daten zu erhalten. (Art. 15 DSGVO)

b) Sollten unrichtige personenbezogenen Daten verarbeitet werden, steht Ihnen ein Recht auf Berichtigung zu (Art. 16 DSGVO)

c) Liegen die gesetzlichen Voraussetzungen vor, so können Sie die Löschung oder Einschränkung der Verarbeitung verlangen sowie Widerspruch gegen die Verarbeitung einlegen (Art. 17, 18, 21 DSGVO)

d) Wenn Sie in die Datenverarbeitung eingewilligt haben oder ein Vertrag zur Datenverarbeitung besteht und die Datenverarbeitung mithilfe automatisierter Verfahren durchgeführt wird, steht Ihnen gegebenenfalls ein Recht auf Datenübertragbarkeit zu. (Art. 20 DSGVO)

Sollten Sie von den genannten Rechten Gebrauch machen, prüft der_die Verantwortliche, ob die gesetzlichen Voraussetzungen hierfür vorliegen. Weiterhin besteht ein Beschwerderecht beim Bayerischen Landesbeauftragten für den Datenschutz.

Anlage 5

Checkliste DSGVO

Maßnahmen	• **Anmerkungen**
• Festlegen wer im Jugendring die „Verantwortlichen“ im Sinne der DSGVO sind. Diese Information wird auch	• nach Art. 4 Abs. 7 DSGVO ist dies „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“; Damit ist im Jugendring die Leitungsebene gemeint, grundsätzlich der_die Vorsitzende sowie die Geschäftsführung • er ist für die Umsetzung der Vorschriften der DSGVO zuständig/“verantwortlich“ • durch entsprechende schriftliche Vereinbarungen (Art. 5 DSGVO) können Aufgaben des/der Verantwortliche_ auf andere Mitarbeiter übertragen werden • diese Aufgaben sind klar und eindeutig zu benennen •
• Benennung eines/einer DSB nach DSGVO	ist bereits ein_e Datenschutzbeauftragte_r benannt, so gilt die bisherige Bestellung fort Auswahl geeigneter Personen; hier ist darauf zu achten, dass dessen andere Aufgaben und Pflichten nicht zu einem Interessenkonflikt (Art. 38 Abs. 6. DSGVO) führen; Dies trifft zu auf: - herausgehobene Führungsfunktion - Umfangreiche Aufgaben und Verarbeitungsvorgänge mit sensiblen Daten (z.B. Personalangelegenheiten) - Positionen mit Entscheidungskompetenzen, die für den Betrieb der IT zuständig sind nach der DSGVO ist es nun möglich einen externen „Dienstleister“ mit dem Datenschutz in der Gliederung zu beauftragen die Zusammenfassung mehrere Jugendringe auf Bezirksebene mit einem DSB ist wie bisher möglich Bestellung und konkreten Aufgabenbereich schriftlich dokumentieren (Art. 39 DSGVO, Art. 12 BayDSG n.F.) die Kontaktdaten sind an das BayLfD zu übermitteln

• Erstellung eines internen Datenschutzkonzepts oder einer Datenschutzrichtlinie	• Notwendig zur Rechenschaftspflicht nach Art. 5 DSGVO über die Rechtmäßigkeit der Verarbeitung • die rechtlichen Grundlagen werden ausführlich in Kapitel 2 dieser Arbeitshilfe erklärt • Festlegung von Zuständigkeiten und Verfahrensabläufen
• Überarbeitung/Neufassung von Datenschutzbelehrungen, Dienstanweisungen etc.	• Notwendig zur Rechenschaftspflicht nach Art. 5 DSGVO über die Rechtmäßigkeit der Verarbeitung • Festlegung von Zuständigkeiten und Verfahrensabläufen • wichtig bei Neueinstellungen; Aushilfen und Praktikanten fallen ebenfalls unter die Belehrungspflicht
• Screening bestehender Unterlagen wie z.B. Satzungen, Haushalsvollzugsregelungen etc.	• Überprüfung der „Gesetzes-Hausnummern“ (Paragraphennummern, Artikel etc.) • Inhaltliche Anpassungen vornehmen
• Anpassung/Neufassung von Datenschutzhinweisen/Informationspflichten nach Art. 13,14 DSGVO	• Vordrucke/Musterformulare erstellen • Datenschutzerklärung auf der Homepage anpassen/erneuern, es wird empfohlen dies durch einen externe Dienstleister durchführen zu lassen • eine Mustervorlage für Datenschutzhinweise für Veranstaltung ist dieser Arbeitshilfe beigefügt •
• Veröffentlichung der Kontaktdaten des/der DSB an den Bayerischen Landesbeauftragten für Datenschutz	• Über die Homepage des Landesbeauftragten für Datenschutz in Bayerin www.datenschutz-bayern.de •
• Anpassung/Abschluss von Verträgen über Auftragsverarbeitungen	• Verwendung von Mustervordrucken; entsprechende Downloads sind auf der Homepage des Bayerischen Landesamts für Datenschutzaufsicht zu finden www.lda.bayern.de • 18 DSGVO

• Anpassung der technischen und organisatorischen Maßnahmen (TOM), Art. 32 DSGVO	• SSL-Verschlüsselung der Homepage • Impressum auf der Homepage, Facebook etc. • Datenschutzerklärung auf der Homepage • E-Mail – Versände immer mit BCC bzw. über „Send Personally“-Funktion • „Geschäftliche“ E-mails für den Jugendring/Verein mit ordentlicher Signatur • Zugangsbeschränkungen/Kontrolle (Passwörter, offene Ordner vermeiden, keine öffentlich zugänglichen PC´s) • Aktenablage z.B., abschließbare Schränke • Datensicherung, event. Sicherungskopien in Safe, Festplattenspiegelung, etc • Virenschutz, Firewall • etc.

Anlage 6

Aufbewahrungsfristen

Schriftgut	Aufbewahrungsfrist in Jahren
Abrechnungsbelege (soweit Buchungsbelege)	10
Abschlussprüfungen	10
Ausschreibungsunterlagen	10
Abtretungserklärungen nach Erledigung	6
Änderungsnachweise der EDV-Buchführung	10
Aktenplan	10
Aktenvermerke (soweit Buchungsbelege)	10
Angebote, die zu einem Auftrag geführt haben	6
Anlagenvermögensbücher und -karteien	10
Arbeitsanweisungen für EDV-Buchführung	10
Arbeitsberichte des Jugendrings	Archiv
Arbeitsberichte Bayerischer Jugendring	Archiv
Arbeitssicherheit, Arbeitsschutz	10
Arbeitszeit, Gleitzeit, Teilzeit-Unterlagen	10
Urlaub, Dienstbefreiung	10
Ausbildungsplanung, -maßnahmen, -prüfungen	10
Ausgangsrechnungen	10
Außendienstabrechnungen, soweit Buchungsbelege	10
Bankbürgschaften	6
Bayerischer Jugendring; Bezirksjugendringe (Haushaltsrelevante Akten)	6

Bayerischer Jugendring, Bezirksjugendringe (alle übrigen Akten)	3
Belege, soweit Buchfunktion (offene-Posten-Buchhaltung)	10
Beschaffungsmaßnahmen	10
Bestell- und Auftragsunterlagen	6
Betriebsabrechnungen mit Belegen als Bewertungsunterlagen	10
Betriebskostenrechnungen	10
Betriebsprüfungsberichte	6
Bewirtungsrechnungen (soweit Buchungsbelege)	10
Bilanzen (Jahresabschlüsse)	10
Bilanzunterlagen	10
Buchungsanweisungen	10
Buchungsbelege	10
Bußgelder, Zwangsgelder	5
Darlehensunterlagen (nach Ablauf des Vertrags)	6
Datenschutz	10
Dauerauftragsunterlagen (soweit nicht Buchungsgrundlage, nach Ablauf des Vertrags)	6
Debitorenlisten (soweit Bilanzunterlage); Zahlungs-pflichtigen-Listen	10
Depotauszüge (soweit nicht Inventare)	10
Dienstanweisungen	30
Doppel von Rechnungen	10
Einnahmeüberschussrechnungen	10

Einrichtungen der Jugendarbeit (HH-relevante Akten)	6
Einrichtungen der Jugendarbeit (alle übrigen Akten)	3
Eröffnungsbilanzen 10	10
Erwachsenenbildung	10
Essensmarkenabrechnungen (soweit Buchungsbelege)	10
Fahrtkostenerstattungen (soweit Buchungsbelege)	10
Ferienmaßnahmen, Freizeitmaßnahmen (HH-relevanten Akten)	6
Ferienmaßnahmen, Freizeitmaßnahmen (alle übrigen Akten)	3
Förderprojekte Sonstige (HH-relevante Akten)	6
Förderprojekte Sonstige (alle übrigen Akten)	3
Fortbildungsmaßnahmen, -planungen, -prüfungen	10/5
Frachtbriefe	6
Gehaltslisten	10
GEMA (Rundfunk- u. Fernsehgebührenermäßigungen)	5
Geschäftsberichte	30
Geschäftsbriefe (außer Rechnungen und Gutschriften)	6
Geschenknachweise	6
Gewaltprävention (HH-relevante Akten)	6
Gewaltprävention (alle übrigen Akten)	3
Gewerbesteuer	10
Grundbuchauszüge	10
Grundsteuer	10

Grundstücksverzeichnis (soweit Inventar)	10
Gutschriften	10
Haftpflichtversicherungen, Kassenversicherungen	10
Handelsregisterauszüge	6
Hauptabschlussübersicht (wenn anstelle von Bilanz)	10
Haushaltssatzung, Haushaltsplan (HH-Verhandlungen, HH-Entwürfe, Berechnungsgrundlagen, Beschlüsse, Bekanntmachungen)	30
Insolvenzverfahren	5
Integration junger Aussiedler_innen und Ausländer_innen (HH-relevante Akten)	6
Integration junger Aussiedler_innen und Ausländer_innen (alle übrigen Akten)	3
Internationale Begegnungen	6
Inventar	10
Investitionszulage (Unterlagen)	6
Jahresabschlüsse und Erläuterungen	30
Jahresberichte der Mitgliedsorganisationen	10
Journale für Hauptbuch und Kontokorrent	10
Jugendfreizeitstätten	10
Jugend-Initiativen, andere Träger der freien Jugendhilfe (HH-relevante Akten)	6
Jugend-Initiativen, andere Träger der freien Jugendhilfe (alle übrigen Akten)	3
Jugendverbände, Jugendgruppen (alle übrigen Akten)	3

Kassenbelege	5
Kassenberichte	30
Kassenbücher und -blätter	10
Kassenprüfungen	10
Kassenreste	5
Kassenzettel	6
Kreis- und Stadtjugendringe	10
Kinder- und Jugendbeauftragte (HH-relevante Akten)	6
Kinder- und Jugendbeauftragte (alle übrigen Akten)	3
Kinderspielplätze	10
Körperschaftssteuer	10
Kontenpläne und Kontenplanänderungen	10
Kontenregister	10
Kontoauszüge	10
Kreditunterlagen (soweit Buchungsbelege, nach Ablauf des Kreditvertrags)	10
Kulturarbeit für Kinder- und Jugendliche (HH-relevante Akten)	6
Kulturarbeit für Kinder- und Jugendliche (alle übrigen Akten)	3
Lagerbuchführungen	10
Lieferscheine (soweit Buchungsbelege)	10
Lohnbelege (soweit Buchungsbelege)	10
Lohnlisten	10

Mahnungen und Mahnbescheide	6
Medienpädagogik (HH-relevante Akten)	6
Mietunterlagen (nach Ablauf des Vertrags)	10
Mitgliedschaften	30
Nachnahmebelege (soweit Buchungsbelege)	10
Offene Kinder- und Jugendarbeit (HH-relevante Akten)	6
Offene Kinder- und Jugendarbeit (alle übrigen Akten)	6
Öffentliche Abgaben, Gebühren, Kosten, Beiträge	10
Pachtunterlagen (nach Ablauf des Vertrags)	10
Preislisten	6
Protokolle (allgemeiner Art)	6
Protokolle Vollversammlungen	30
Protokolle BezJR-Ausschüsse	30
Protokolle Vorstandssitzungen	30
Prozessakten (nach Beendigung des Verfahrens)	10
Prüfberichte	30
Quittungen	10
Rahmenverträge	5
Rechnungen	10

Rechnungsprüfung, örtlich und überörtlich	10
Reisekostenabrechnungen, Umzugskosten, Trennungsgelder	10/5
Sachkonten	10
Schadensunterlagen	6
Satzungen	10
Schulsozialarbeit (HH-relevante Akten)	6
Schulsozialarbeit (alle übrigen Akten)	3
Sonderprüfungen	10
Spendenbescheinigungen	10
Stellenausschreibungen	3
Stellenpläne, Stellenbewertungen, Stellenobergrenzen	30
Steuerwesen allgemein	10
Steuerunterlagen und Steuererklärungen	10
Stiftungen, Schenkungen	10
Suchtprävention (HH-relevante Akten)	6
Suchtprävention (alle übrigen Akten)	3
Träger örtlich, Jugendamt, Jugendhilfeausschuss	20
Träger überörtlich, Landesjugendamt, Landesjugendhilfeausschuss)	20
Träger der freien Kinder- und Jugendhilfe	10
Telefonkostennachweise (soweit Buchungsbelege)	10
Überstundenlisten	6
Überweisungsbelege	10

Umsatzsteuervoranmeldungen	10
Umsatzsteuer, Steuerabzug bei Bauleistungen	10
Unfallanzeigen, Unfalluntersuchungen, Unfallverhütung	10
Verbindlichkeiten (Zusammenstellungen)	10
Verkaufsbücher	10
Vermögensverzeichnis	30
Vermögenswirksame Leistungen (Unterlagen, soweit nicht Buchungsbelege)	6
Verordnungen	10
Versand- und Frachtunterlagen	6
Versicherungspolicen/Versicherungen	6/10
Verträge (soweit nicht Buchungsgrundlage)	6 / 30
Grundlagenverträge	Archiv
Betriebsträgerverträge	Archiv
Personalüberstellungsverträge u. -vereinbarungen	Archiv
Projektträgerverträge	Archiv
Finanzierungsvereinbarungen	Archiv
Kreditverträge	Archiv
Vorschüsse, Darlehen, sonstige Fürsorgeleistungen (Personal)	10
Warenbestandsaufnahme (Inventuren)	10
Wareneingangs- und Ausgangsbücher	10
Wartungsverträge	5
Wechsel (soweit Buchungsbelege)	10

Zuschüsse, Zuweisungen nach Finanzausgleichsgesetz (FAG)	10

Anlage 7

Merkblatt allgemeine Infos

Bei Ihrer Tätigkeit in unserem Unternehmen werden Sie zwangsläufig mit personenbezogenen Daten oder ansonsten gesetzlich geschützten Daten in Berührung kommen, sei es als „Betroffener" oder weil Sie beim Umgang mit solchen Daten mitwirken bzw. weil Ihnen solche Angaben während Ihrer Tätigkeit zur Kenntnis gelangen. Bereits auf Grund allgemeiner arbeitsvertraglicher Regelungen und gesetzlicher Vorschriften dürfte Ihnen das Gebot zur vertraulichen Handhabung von Personaldaten und Geschäfts- und Betriebsgeheimnissen bekannt sein. Für die Mitarbeiter_innen, die bei der Verarbeitung personenbezogener Daten im Geltungsbereich des Bayerischen Datenschutzgesetzes (BayDSG) beschäftigt sind, gilt darüber hinaus die Verpflichtung zur Wahrung des Datengeheimnisses (Artikel 11 BayDSG), auf die Sie in einer schriftlich abzugebenden Erklärung besonders hingewiesen werden.

Verpflichtung zur Wahrung des Datengeheimnisses

Allen Mitarbeitern, die dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, solche Daten unbefugt zu verarbeiten oder zu nutzen; dies gilt auch nach Beendigung ihrer Tätigkeit.

Hierin besteht Ihre spezielle Verpflichtung, zur Wahrung des Datenschutzes beizutragen.

Zweck des Datenschutzes ist es, den Einzelnen davor zu schützen, dass durch den Umgang mit seinen personenbezogenen Daten seine Persönlichkeitsrechte beeinträchtigt werden.

Das erfordert ein verantwortliches Handeln beim Umgang mit personenbezogenen Daten, aber auch die risikobewusste Nutzung von IT-Systemen und -Anwendungen. Fehlverhalten kann zu materiellen und immateriellen Schäden mit teilweise beträchtlichen negativen Kundeneffekten führen.

Zur Gewährleistung der Vorschriften des Datenschutzes und zur Sicherung der Daten gegen Verlust oder unbefugten Zugriff sind in unserem Unternehmen Maßnahmen bzw. Richtlinien getroffen worden. Informieren Sie sich hierüber bei Ihrem Vorgesetzten und machen sich mit den Regelungen vertraut.

Denken Sie stets daran: **Sie sind dafür verantwortlich,** dass

- die Ihnen anvertrauten Daten, Datenträger und Ausdrucke unter Verschluss gehalten werden, wenn Sie nicht unmittelbar daran arbeiten. Hierzu sind insbesondere Bildschirme und PC bei Abwesenheit vom Arbeitsplatz zu sperren.

- Ihr PC/Ihre Anwendungen/Ihr Passwort keinem Unbefugten zugänglich wird. Daher sollen Sie nur sichere Passwörter auswählen (z.B. mit Sonderzeichen, keine Namen) und diese regelmäßig wechseln.

- nicht mehr benötigte Datenträger und Ausdrucke so vernichtet werden, dass eine missbräuchliche Verwendung nicht möglich ist.

- Laptops bei Reisen bzw. Dienstfahrten sorgfältig gesichert werden, besonders im Auto, Hotel oder auf Flughäfen.

- keine vertraulichen Informationen per Fax verschickt werden. Falls Sie dies doch in Ausnahmefällen tun müssen, treffen Sie besondere Vorkehrungen (z.B. telefonische Absprache wegen Anwesenheit des Empfängers, Doppelkontrolle der Richtigkeit der eingegebenen Fax-Nummer vor Versand).

- Sie nicht einfach mit Antwortfunktion auf E-Mail mit vertraulichem Inhalt reagieren, vorher Absenderlisten überprüfen (Achtung: vertrauliche Informationen über E-Mail grundsätzlich nicht versenden, wenn keine Verschlüsselung genutzt werden kann)!

- keine vertraulichen Telefonate vom Handy in der Öffentlichkeit geführt werden z.B. auf Reisen im Zug.

Ihnen ist untersagt, Unternehmensgeräte privat zu nutzen oder private Computer, Software und Datenträger in das Unternehmen einzubringen.

Bei Fragen zum Thema Datenschutz bzw. Datensicherheit oder in Zweifelsfällen wenden Sie sich bitte an Ihren Verantwortlichen für den Datenschutz oder den_die benannte_n Datenschutzbeauftragte_n.

Impressum

Herausgeber
Bayerischer Jugendring K.d.ö.R.
vertreten durch den Präsidenten
Matthias Fack

Anschrift
Herzog-Heinrich-Str. 7
80336 München
tel 089/51458-0
publikationen@bjr.de
www.bjr.de

Bildnachweis
© momius - Fotolia.com

Stand
September 2018