Leitfaden zur

DSGVO

Datenschutzgrundverordnung für Einrichtungen der Offenen Jugendarbeit

Dieser Leitfaden wurde von **POJAT – Plattform Offene Jugendarbeit Tirol** in Kooperation mit **bOJA – bundesweites Netzwerk Offene Jugendarbeit** erstellt.

Mit freundlicher Unterstützung der Fachabteilungen für Jugendarbeit der Bundesländer Tirol, Burgenland, Vorarlberg, Salzburg, Wien und Kärnten.

Impressum:

Herausgeber: **Dachverband Offene Jugendarbeit Tirol (POJAT), ZVR-Nr. 507 802 833**
Kirschentalgasse 10, 6020 Innsbruck, W: www.pojat.at, E: office@pojat.at, T: +43 660 2633617

Juni 2018, Version 1.0

Text und Konzeption (Verfasser): Dr. Werner Pilgermair, Mag. Lukas Trentini

Inhaltsverzeichnis

1 VORWORT 5

2 EINFÜHRUNG 5

2.1 DIE NEUE RECHTSLAGE IM DATENSCHUTZ 6
2.1.1 DATENSCHUTZGRUNDVERORDNUNG 6
2.1.2 EINHEITLICHE STANDARDS FÜR DIE JUGENDARBEIT IN EUROPA 6
2.1.3 EIGENVERANTWORTLICHKEIT UND RECHENSCHAFTSPFLICHT 6
2.1.4 AUSWIRKUNGEN AUF DIE OFFENE JUGENDARBEIT 7
2.2 PERSONENBEZOGENE DATEN 7
2.2.1 BESONDERE KATEGORIEN PERSONENBEZOGENER DATEN 7
2.2.2 VERARBEITUNG PERSONENBEZOGENER DATEN 8
2.2.3 SOFTWARESYSTEME, EXCEL-LISTEN UND PAPIERORDNER 8
2.2.4 KEIN PERSONENBEZUG 8
2.3 DATENSCHUTZRECHTLICHE ROLLEN 9
2.3.1 VERANTWORTLICHER 9
2.3.2 AUFTRAGSVERARBEITER 9

3 DATENVERARBEITUNG IN DER OFFENEN JUGENDARBEIT 10

3.1 TAGESDOKUMENTATION 10
3.2 EINZELFALLDOKUMENTATION 10
3.2.1 ERSTBERATUNG 10
3.2.2 BERATUNG UND BEGLEITUNG 11
3.3 TEAMBESPRECHUNGEN 11
3.4 PROJEKTE 11
3.4.1 EINZELPROJEKTE 11
3.4.2 LANGFRISTIGE PROJEKTE 12
3.5 HELFERKONFERENZEN UND VERNETZUNGSTREFFEN 12
3.6 PERSONAL 12
3.7 SONSTIGE INVOLVIERTE PERSONEN 13
3.8 WEBSITE UND SOCIAL MEDIA PLATTFORMEN 13
3.9 FOTOS 13
3.10 DATENSCHUTZ-LANDKARTE 14

4 KEINE DATENVERARBEITUNG OHNE RECHTSGRUNDLAGE 14

4.1 GESETZLICHE BESTIMMUNGEN (ART. 6 ABS. 1 LIT. C UND ART. 9 ABS. 2 LIT. G DSGVO) 14
4.1.1 § 132 BUNDESABGABENORDNUNG 14
4.1.2 § 37 BUNDES-KINDER- UND JUGENDHILFEGESETZ 2013 15
4.1.3 § 2 TIROLER JUGENDFÖRDERUNGS- UND JUGENDSCHUTZGESETZ 15
4.1.4 § 20 TIROLER JUGENDFÖRDERUNGS- UND JUGENDSCHUTZGESETZ 15
4.1.5 ART. 9 ABS. 2 LIT. H DSGVO 15
4.2 BERECHTIGTE INTERESSEN DER EINRICHTUNG (ART. 6 ABS. 1 LIT. F DSGVO) 16
4.3 ERFÜLLUNG VERTRAGLICHER PFLICHTEN DER EINRICHTUNG (ART. 6 ABS. 1 LIT. B DSGVO) 16
4.4 ERFÜLLUNG VON PFLICHTEN AUS DEM ARBEITS- UND SOZIALRECHT (ART. 9 ABS. 2 LIT. B DSGVO) 17

4.5 Einwilligung der betroffenen Person (Art. 6 Abs. 1 lit. a DSGVO und Art. 9 Abs. 2 lit. a DSGVO) 17
4.5.1 Erfordernisse 17
4.5.2 Mündliche Einwilligung als Alternative 19
4.6 Übersicht Rechtsgrundlagen 20

5 WICHTIGE AUFGABEN UND PFLICHTEN 20

5.1 Einhaltung der Grundsätze der Datenverarbeitung 20
5.1.1 Rechtmäßigkeit 20
5.1.2 Datenminimierung 21
5.1.3 Speicherbegrenzung 21
5.1.4 Integrität und Vertraulichkeit 21
5.2 Verzeichnis aller Verarbeitungstätigkeiten 21
5.2.1 Notwendige Angaben 21
5.2.2 Verzeichnisvorlagen 22
5.3 Technische und organisatorische Maßnahmen (TOMs) 22
5.3.1 Beispiele für TOMs 22
5.4 Datensicherheitsmaßnahmen 22
5.4.1 Beispiele für Datensicherheitsmaßnahmen: 22
5.5 Datenschutz-Folgenabschätzung 24
5.6 Datenschutzbeauftragter 25
5.7 Meldung von Datenschutz-Vorfällen 25
5.8 Informierung der Betroffenen 26
5.9 Transparenz 27
5.10 Interne Datenschutzstrategien 27

6 ARBEITSHILFEN 28

6.1 Checkliste 28
6.1.1 Dringende Maßnahmen 28
6.1.2 Weiterführende Maßnahmen 28
6.2 Vorlagen und Muster 29

1 Vorwort

Die seit 25. Mai 2018 geltende neue europaweite Gesetzgebung zum Datenschutz macht es auch für Trägerorganisationen von Einrichtungen der Offenen Jugendarbeit notwendig sich dem Datenschutz und der Datensicherheit zu widmen. In den letzten Monaten vor Inkrafttreten des neuen Gesetzes wurde klar, dass es eine bedarfsorientierte und maßgeschneiderte Unterstützung für Einrichtungen der Offenen Jugendarbeit braucht, um die datenschutzrelevanten Aufgaben möglichst effektiv und gesetzeskonform erledigen zu können. Die POJAT hat dieses Anliegen aufgegriffen und den vorliegenden Leitfaden mit maßgeblicher Unterstützung durch den Datenschutzexperten Dr. Werner Pilgermair entwickelt. Der Leitfaden versteht sich als dynamisches Papier, da aufgrund der künftigen Judikatur einige Änderungen und Konkretisierungen möglich sind. Dieser Leitfaden wurde in Tirol entwickelt und bezieht sich daher in einigen Punkten explizit auf das Tiroler Jugendschutz- und Jugendförderungsgesetz. Sofern vergleichbare Bestimmungen in anderen Bundesländern bestehen wird daraufhin an den betreffenden Stellen hingewiesen.

Im Sinne der Qualitätssicherung in der Offenen Jugendarbeit will der Leitfaden einen wichtigen Beitrag für die professionelle Gestaltung der Rahmenbedingungen leisten.

2 Einführung

Für Einrichtungen der Offenen Jugendarbeit ergibt sich im Datenschutz ein Kraftfeld aus unterschiedlichen Erwartungshaltungen. Jugendliche erwarten sich Aufmerksamkeit, Anteilnahme und im Einzelfall auch Unterstützung und Beratung. Auf der anderen Seite wollen Jugendliche möglichst anonym bleiben oder zumindest sicher sein, dass ihre Daten, Informationen und Mitteilungen vertraulich behandelt werden. In der Mobilen Jugendarbeit ist dieses Kraftfeld meist stärker ausgeprägt als in der standortbezogenen Jugendarbeit (Jugendzentren, Jugendtreffs, Jugendräume), da dort in der Regel mehr an Beratung und Begleitung angeboten und durchgeführt wird.

Dieser Leitfaden soll das Arbeitsfeld der Offenen Jugendarbeit aus dem Blickwinkel des Datenschutzes beleuchten und datenschutzrechtliche Aspekte und Zusammenhänge verständlich machen. Gleichzeitig soll er das Rüstzeug vermitteln, um die Aufgaben und Pflichten nach der neuen Rechtslage selbständig erfüllen zu können.

2.1 Die neue Rechtslage im Datenschutz

2.1.1 Datenschutzgrundverordnung

Die Wurzeln des Datenschutzes, so wie wir ihn heute als Schutz unserer Privatsphäre und unserer Persönlichkeitsrechte verstehen, gehen bis ins 13. Jahrhundert zurück, als mit dem Beichtgeheimnis erstmals eine Verschwiegenheitspflicht festgeschrieben wurde.
Mit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) mit 25. Mai 2018 hat in Europa ein neues Datenschutzzeitalter begonnen. In Österreich wird die DSGVO durch das angepasste Datenschutzgesetz (DSG), das ebenfalls mit 25. Mai 2018 in Kraft getreten ist, begleitet.

Die deutschsprachige Version der DSGVO ist auf der Website der Europäischen Union abrufbar: Link zur DSGVO.

2.1.2 Einheitliche Standards für die Jugendarbeit in Europa

In den EU-Mitgliedstaaten haben bislang völlig unterschiedliche Datenschutzgesetze gegolten. Durch die DSGVO werden diese unterschiedlichen Datenschutzniveaus und die daraus resultierenden unerwünschten Folgen beseitigt. Künftig werden für alle beteiligten Akteure im Datenschutz – und damit auch für sämtliche Einrichtungen der Jugendarbeit in der EU – einheitliche Standards gelten.

Da die Erfüllung datenschutzrechtlicher Aufgaben und Pflichten auch mit einem gewissen personellen und finanziellen Aufwand verbunden sein wird, ist diese europäische Vereinheitlichung schon aus Fairnessgründen (Wettbewerbsneutralität) zu begrüßen.

2.1.3 Eigenverantwortlichkeit und Rechenschaftspflicht

Die DSGVO verlangt eine viel stärkere Eigenverantwortlichkeit von datenschutzrechtlichen Akteuren als bisher. Aufgaben und Pflichten im Datenschutz sollen selbständig und nachweislich umgesetzt werden. Die Datenschutzbehörden in den EU-Mitgliedstaaten ziehen sich weitestgehend auf ihre Überwachungs- und Kontrollfunktion zurück.

Exorbitant hohe Geldbußen (Strafrahmen bis zu 20 Millionen Euro) sollen die eigenverantwortliche Umsetzung der DSGVO sicherstellen. Auch wenn die maximalen Strafandrohungen auf internationale Konzerne abzielen dürften, verlangt die DSGVO, dass Geldbußen im Einzelfall „*wirksam, verhältnismäßig und abschreckend*" sein müssen. Wie dies mit der österreichischen Regelung im DSG, wonach die Datenschutzbehörde bei erstmaligen Verstößen gegen den Datenschutz nur ermahnen soll, vereinbar ist, wird die Entscheidungspraxis der Datenschutzbehörde und die Judikatur der unabhängigen Gerichte zeigen.

2.1.4 Auswirkungen auf die Offene Jugendarbeit

„Datenschutz“ wird in der Gesellschaft zunehmend als Seriositäts- und Qualitätsmerkmal wahrgenommen. Verstöße gegen den Datenschutz können bei Jugendlichen, gesetzlichen Vertreter*innen, Netzwerkpartner*innen und insbesondere auch bei Fördergeber*innen schnell zu Vertrauensverlusten führen.

Neben der Überwachung der Einhaltung von Datenschutzvorschriften durch die Datenschutzbehörde und die unabhängigen Gerichte und der daraus resultierenden Sanktionen, muss dem negativen Imagetransfer, der als Folge von Datenschutzverstößen entstehen kann, das größte Bedrohungspotential unterstellt werden.

*Beispiel: Jugendliche verschaffen sich unbefugt Zugriff auf streng vertrauliche Aufzeichnungen aus einer Beratung und veröffentlichen diese Informationen in ihrem sozialen Netzwerk im Internet, da sie mit dem betroffenen Jugendlichen Streit hatten. Wenn sich herausstellt, dass die Einrichtung ihre Pflicht zur Umsetzung ausreichender Datensicherheitsmaßnahmen gröblich vernachlässigt hat (etwa, weil die Mappe mit der betroffenen Einzelfalldokumentation weder versperrt aufbewahrt wurde, noch die Tür zum Verwaltungsbereich, in dem sich alle diese Unterlagen befinden, abgeschlossen war, und die Jugendlichen daher praktisch ungehindert Zugang zur Mappe hatten), könnte dieser Vorfall zu massiven Vertrauensverlusten im Umfeld der Einrichtung (z.B. auch bei Fördergeber*innen) führen.*

2.2 Personenbezogene Daten

Personenbezogene Daten sind nach Artikel 4 DSGVO „*alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen*“.

Empfehlung: Der Begriff der personenbezogenen Daten sollte im Zweifel weit gefasst und interpretiert werden.

Personenbezogene Daten können demnach beispielsweise sein: Name, Geburtsdatum, Telefonnummer, E-Mail-Adresse, Wohnort, Ausbildung, Qualifikation, Beruf, Lebensgeschichte, Beziehungen, Talente, Vorlieben, Wünsche, Erwartungen, Abneigungen, Vorwürfe, Fotos, etc.

2.2.1 Besondere Kategorien personenbezogener Daten

Bestimmte personenbezogene Daten werden von der DSGVO besonders geschützt (nach alter Rechtslage werden diese Daten als „sensible Daten“ bezeichnet). Im Einzelnen handelt es sich um folgende Daten wobei dies eine vollständige und nicht bloß beispielhafte Aufzählung ist:

- Rassische und ethnische Herkunft
- Politische Meinungen
- Religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetische Daten
- Biometrische Daten
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung

2.2.2 Verarbeitung personenbezogener Daten

Unter dem „Verarbeiten" von personenbezogenen Daten wird jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten verstanden, wie z.B. das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

Der Begriff der Datenverarbeitung schließt damit praktisch jede Handhabung von personenbezogenen Daten ein.

2.2.3 Softwaresysteme, Excel-Listen und Papierordner

Ob personenbezogene Daten im Rahmen einer professionellen Softwarelösung (z.B. einer Personalverwaltungssoftware), mit Hilfe von den Programmen Word oder Excel, oder in strukturierter Papierform verarbeitet werden, ist nicht von Belang.

Beispiel: In einem physischen Tagebuch werden chronologisch Aufzeichnungen über die Vorkommnisse in der Einrichtung geführt. Dabei kommt es auch zur Dokumentation von personenbezogenen Daten. Aus datenschutzrechtlicher Sicht ist dies ebenso relevant, als wenn die Aufzeichnungen in einem elektronischen Tagebuch (z.B. Word-Dokument) geführt werden.

2.2.4 Kein Personenbezug

Daten, die keinen Personenbezug aufweisen, sind datenschutzrechtlich nicht von Bedeutung.

*Beispiel: Von einem Jugendzentrum wird eine Statistik über die Besucher*innenzahlen geführt. Zu diesem Zweck wird auf einer Strichliste händisch eingetragen, wie viele weibliche und wie viele männliche Jugendliche im laufenden Kalendermonat kommen. Diese Art der Dokumentation ist in aller Regel nicht dazu geeignet, Rückschlüsse auf konkrete Jugendliche zuzulassen und somit aus Sicht des Datenschutzes nicht relevant. Sinngemäß dasselbe gilt,*

wenn im Rahmen der Mobilen Jugendarbeit die Anzahl der Kontakte zu statistischen Zwecken dokumentiert wird.

Die Nutzung der bOJA-Datenbank durch Träger und Einrichtungen der Offenen Jugendarbeit ist – mangels Erfassung personenbezogener Daten – ebenfalls nicht datenschutzrelevant.

2.3 Datenschutzrechtliche Rollen

An der Verarbeitung von personenbezogenen Daten können unterschiedliche Akteure beteiligt sein.

2.3.1 Verantwortlicher

„Verantwortlicher" in Bezug auf die Datenverarbeitungen, die in der Einrichtung durchgeführt werden, ist grundsätzlich immer der Rechtsträger der Einrichtung (zumeist Verein oder Gemeinde), nicht aber einzelne Organisationseinheiten bzw. Tätigkeitsbereiche (z.B. Sozialraumarbeit oder Streetwork) oder einzelne Mitarbeiter*innen der Einrichtung.

Der Verantwortliche ist primärer Adressat der DSGVO und hat alle Aufgaben und Pflichten im Datenschutz zu erfüllen.

2.3.2 Auftragsverarbeiter

„Auftragsverarbeiter" ist derjenige, der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

In der Praxis betrifft dies externe Dienstleister, die von der Einrichtung z.B. auf Basis eines Werkvertrages oder Auftragsvertrages herangezogen werden.

Beispiel: Ein größerer Verein hat aufgrund der hohen Beschäftigtenzahl einen EDV-Dienstleister damit beauftragt, eine geeignete Personaldatenbank zu programmieren und zu betreuen. Der EDV-Dienstleister hat dadurch zwangsläufig Zugriff auf alle Personaldaten (z.B. im Rahmen der laufenden Wartung) und wird dadurch zum Auftragsverarbeiter des Vereins.

Beispiel: Ein Verein erstellt seinen Jahresbericht und übermittelt zu diesem Zweck alle Texte und Fotos an eine Druckerei. Die Druckerei verarbeitet alle Fotos und wird dadurch zur Auftragsverarbeiterin des Vereins.

Der Verein als datenschutzrechtlicher Verantwortlicher in Bezug auf die Personaldaten und die Fotos hat mit seinen Dienstleistern gemäß Artikel 28 DSGVO einen Vertrag abzuschließen, der die wesentlichen Punkte der Datenverarbeitung regelt (siehe Kapitel 6.2 Vorlagen und Muster).

Freie Berufe (Rechtsanwälte, Steuerberater, Wirtschaftsprüfer, etc.), Gesundheitsdienste-anbieter (Ärzte, Psychologen, Therapeuten) sowie gewerbsmäßige Buchhalter und Lohnverrechner sind keine Auftragsverarbeiter.

3 Datenverarbeitung in der Offenen Jugendarbeit

Im Folgenden werden typische Verarbeitungstätigkeiten von Einrichtungen der Offenen Jugendarbeit dargestellt. In der Praxis können aufgrund der individuellen Rahmenbedingungen und spezifischen Voraussetzungen einer jeden Einrichtung noch andere Verarbeitungstätigkeiten hinzukommen (z.B. Sonderprojekte oder andere Tätigkeitsbereiche, die nicht Teil von Offener Jugendarbeit sind).

3.1 Tagesdokumentation

Im Rahmen der Tagesdokumentation (in der Praxis z.B. als „Tagebuch“ oder „Logbuch“ bezeichnet) werden die laufenden Vorkommnisse und Geschehnisse in überblicksartiger Form beschrieben, wobei dies entweder analog (in Papierform) oder digital (z.B. im Excel) erfolgen kann.

Auf vollständige Namensnennungen wird in der Regel verzichtet, wenn überhaupt werden nur Vornamen, Anfangsbuchstaben von Vornamen oder Initialen von Jugendlichen und Mitarbeiter*innen dokumentiert. Dies kann im Einzelfall bereits datenschutzrelevant sein.

Anonyme Aufzeichnungen (Verzicht auf jedweden Personenbezug) sind datenschutzrechtlich nicht von Bedeutung (siehe Kapitel 2.2.4 Kein Personenbezug).

3.2 Einzelfalldokumentation

3.2.1 Erstberatung

Nehmen Jugendliche in konkreten Anlassfällen eine sozialpädagogische Erstberatung in Anspruch, kommt es zwangsläufig zur Verarbeitung personenbezogener Daten. Welche Daten dabei im Einzelnen erfasst und dokumentiert werden hängt vom jeweiligen Anlassfall ab.

Beispiel: Ein Jugendlicher vertraut sich einem Jugendarbeiter an und erzählt ihm von seinen Beziehungsproblemen, die ihn stark belasten.

Beispiel: Eine Jugendliche erzählt, dass sie sich in ihrer Schule mit naturwissenschaftlicher Ausrichtung nicht mehr wohl fühlt und sie gerne in eine Schule mit musischer Ausrichtung

wechseln würde. Sie fragt eine Jugendarbeiterin, ob sie dabei sein kann, wenn sie ihre Eltern darüber informiert.

3.2.2 Beratung und Begleitung

Insbesondere in der Mobilen Jugendarbeit werden Jugendarbeiter*innen zum Teil mit sensiblen und strafrelevanten Daten konfrontiert. Die Unterstützungsleistungen gehen in diesen Fällen über Erstberatungen hinaus und können insbesondere auch eine psychosoziale Beratung umfassen.

Neben einem standardisierten Klienten-Stammblatt, das bei jeder Beratung angelegt wird, führt die Einrichtung in der Regel auch eine Verlaufsdokumentation. Dabei können sensible Gesundheitsdaten (z.B. über Verletzungen oder Misshandlungen) und strafrelevante Informationen verarbeitet werden. Auch Angaben über dritte Personen (Angehörige, Täter, Gefährder, etc.) sind davon umfasst.

Beispiel: Einem Jugendarbeiter in der Mobilen Jugendarbeit fallen bei einer Jugendlichen verschiedenfarbige Hämatome auf, was ein Indiz für wiederholte Gewaltanwendung sein kann. Er spricht die Jugendliche darauf an und sie erzählt von körperlichen Misshandlungen durch ihren Freund. Im Rahmen der Beratung wird der Jugendlichen im weiteren Verlauf (Trennungsprozess, Anzeigenerstattung) geholfen. Zwangsläufig müssen dafür alle notwendigen Daten und Informationen verarbeitet werden.

3.3 Teambesprechungen

Im Zuge von Teambesprechungen, die in der Praxis routinemäßig im Wochen- oder Monatsrhythmus stattfinden können, werden Arbeitserfahrungen ausgetauscht und reflektiert sowie Einzelfallbesprechungen durchgeführt.

In der Dokumentation dieser Teambesprechungen werden in der Regel keine Namen von Jugendlichen oder nur die Anfangsbuchstaben ihrer Vornamen verwendet. Von Mitarbeiter*innen werden häufig die Vornamen vermerkt.

3.4 Projekte

3.4.1 Einzelprojekte

Wenn eine Einrichtung Projekte oder Veranstaltungen durchführt, werden dafür Teilnehmer*innenlisten erstellt und die Einwilligung der Eltern eingeholt. Dabei kommt es zur Verarbeitung personenbezogener Daten.

*Beispiel: Von einem Jugendzentrum wird eine Exkursion angeboten. Aufgrund der limitierten Teilnehmer*innenzahl müssen sich interessierte Jugendliche anmelden und die Einverständniserklärung ihrer Eltern vorlegen. Die zur Durchführung der Exkursion benötigten Daten und Informationen werden von der Einrichtung dokumentiert.*

3.4.2 Langfristige Projekte

Gelegentlich werden von Einrichtungen langfristige Projekte durchgeführt, die zwar nicht unmittelbarer Gegenstand der Kernaufgaben der Offenen Jugendarbeit sind, diese aber sinnvoll ergänzen können. Nehmen Jugendliche daran teil, werden personenbezogene Daten verarbeitet.

*Beispiel: In einer von der Einrichtung initiierten Jobbörse werden an Jugendliche Gelegenheits- und Ferialjobs vermittelt. Zu diesem Zweck werden die dafür benötigten Daten von den Jugendlichen (insb. Name, Wohnort, Kontaktdaten, Versicherungsdaten) und den potentiellen Arbeitgeber*innen, die in das Netzwerk der Einrichtung aufgenommen wurden, erfasst. Auch die Einverständniserklärung der Eltern wird dokumentiert.*

3.5 Helferkonferenzen und Vernetzungstreffen

Werden Einrichtungen der Offenen Jugendarbeit zu Helferkonferenzen bzw. Vernetzungstreffen oder Gesprächsrunden eingeladen, kann es im Rahmen von Einzelfallbesprechungen zur Dokumentation von personenbezogenen Daten der betroffenen Jugendlichen kommen (Gegenstand von Gesprächen, weitere Schritte, etc.).

In der Regel stimmen sich die Jugendarbeiter*innen im Vorfeld solcher Gespräche mit den betroffenen Jugendlichen ab. Ausnahmen bestehen dann, wenn von der einladenden Institution keine konkreten Tagesordnungspunkte bekannt gegeben wurden oder Gefahr im Verzug besteht (insbesondere im Zusammenhang mit Gefährdungsmeldungen nach den Kinder- und Jugendhilfegesetzen).

3.6 Personal

Die Trägerorganisation als datenschutzrechtlicher Verantwortlicher verarbeitet zahlreiche personenbezogene Daten ihrer Mitarbeiter*innen. Die Bandbreite der Datenverarbeitungen in der Personalverwaltung reicht von Arbeitszeitaufzeichnungen über die Krankenstandsverwaltung bis hin zur Lohn- und Gehaltsabrechnung und ist im Regelfall gesetzlich geregelt. Auch von Bewerber*innen werden bereits personenbezogene Daten verarbeitet.

Neben den hauptamtlichen Mitarbeiter*innen werden auch ehrenamtliche bzw. freiwillige Mitarbeiter*innen eingesetzt. Von diesen Personen werden Daten wie Name, Kontaktdaten und relevante Daten für die Unfallversicherung erfasst.

3.7 Sonstige involvierte Personen

Auch von anderen Personen werden Daten erhoben, in Betracht kommen z.B. Ansprechpersonen von Netzwerk- und Systempartner*innen sowie Förder*innen, Spender*innen und Sponsor*innen.

3.8 Website und Social Media Plattformen

Bei Internetauftritten von Einrichtungen der Offenen Jugendarbeit können Cookies, Webtracking-Tools und Kontaktformulare eingesetzt werden, mit denen personenbezogene Daten der Internetnutzer verarbeitet werden.

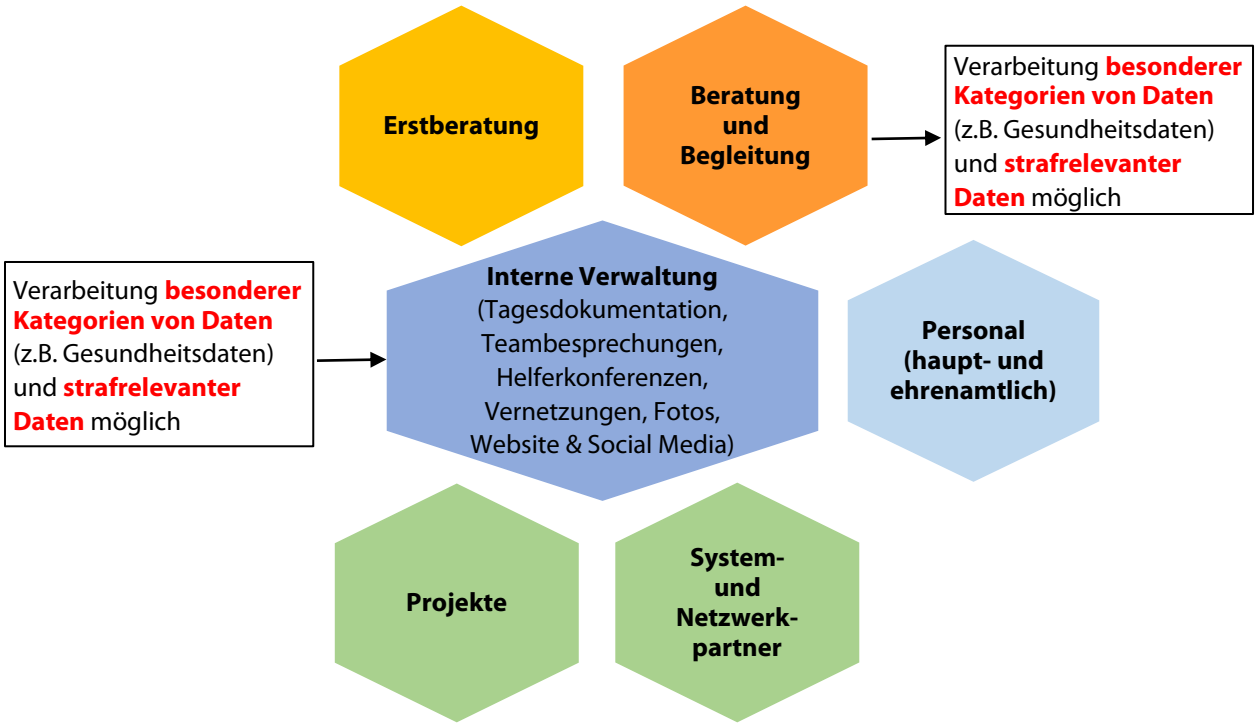
3.9 Fotos

Fotos von Jugendlichen und Mitarbeiter*innen können in der Praxis in vielfacher Weise verarbeitet werden: Einerseits in den Räumlichkeiten der Einrichtung (Fotowand, Fotoalbum, etc.), andererseits in Drucksorten (z.B. Flyer, Informationsbroschüren, Jahresberichte) und schließlich im Internet (Veröffentlichung auf der Website oder auf Social Media Plattformen der Einrichtung).

Ob Fotos überhaupt datenschutzrelevant sind hängt davon ab ob nur ein Szenario oder konkrete Personen fotografiert werden.

*Beispiel: Das Jugendzentrum organisiert das sommerliche Grillfest und fotografiert aus der Entfernung die Szenerie. Man sieht viele Jugendliche, Mitarbeiter*innen und sonstige eingeladene Personen lose zusammen stehen. Betrachtet man das Foto geht es nicht darum einzelnen Personen zu identifizieren (selbst wenn dies beim genauen Hinschauen einem Kreis von Insidern möglich wäre), sondern das Event (Grillfest) zu dokumentieren.*

3.10 Datenschutz-Landkarte



4 Keine Datenverarbeitung ohne Rechtsgrundlage

Personenbezogene Daten müssen nach Artikel 5 Abs. 1 lit. a DSGVO in „rechtmäßiger Weise" verarbeitet werden. Für jede Datenverarbeitung in der Einrichtung muss daher eine taugliche Rechtsgrundlage vorliegen.

Die möglichen Rechtsgrundlagen für das Verarbeiten „normaler" personenbezogener Daten werden in Artikel 6 DSGVO beschrieben. Die Rechtsgrundlagen für besondere Kategorien personenbezogener Daten (insbesondere Gesundheitsdaten) werden in Artikel 9 DSGVO beschrieben.

Die wichtigsten Rechtsgrundlagen für Einrichtungen der Offenen Jugendarbeit sind:

4.1 Gesetzliche Bestimmungen (Art. 6 Abs. 1 lit. c und Art. 9 Abs. 2 lit. g DSGVO)

Bestehen gesetzliche Pflichten zur Datenverarbeitung, kann sich die Einrichtung unmittelbar darauf stützen. Beispielsweise betrifft dies:

4.1.1 § 132 Bundesabgabenordnung

Bücher und Aufzeichnungen sowie die dazu gehörigen Belege sind sieben Jahre aufzubewahren bzw. darüber hinaus so lange, als sie für anhängige Abgabenverfahren

benötigt werden (in der Praxis betrifft dies z.B. lohnsteuerrelevante Aufzeichnungen in der Personalverwaltung).

4.1.2 § 37 Bundes-Kinder- und Jugendhilfegesetz 2013

Mitteilungen bei Verdacht der Kindeswohlgefährdung gegenüber der örtlich zuständigen Kinder- und Jugendhilfe (Jugendämter) bei den betreffenden Bezirkshauptmannschaften.

4.1.3 § 2 Tiroler Jugendförderungs- und Jugendschutzgesetz

„Das Land Tirol hat sicherzustellen, dass in allen politischen Bezirken in den Einrichtungen der offenen Jugendarbeit ein niederschwelliger Jugendberatungsdienst als Erstberatung bereitsteht. Die im Jugendberatungsdienst tätigen Personen müssen entsprechend fachlich ausgebildet und geeignet sein, die Amtsverschwiegenheit für Landesbeamte gilt für sie sinngemäß."

Diese Bestimmung kann als taugliche Rechtsgrundlage für die Erstberatung angesehen werden.[1]

4.1.4 § 20 Tiroler Jugendförderungs- und Jugendschutzgesetz

„Den Organen und sonstigen Beauftragten der Behörde sowie den Organen des öffentlichen Sicherheitsdienstes ist ungehinderter Zutritt zu allen Räumen und Grundstücken zu gewähren sowie auf Verlangen Auskunft zu erteilen, wobei die Ausübung unmittelbarer Zwangsgewalt zulässig ist."

Auch hierbei handelt es sich um eine taugliche Rechtsgrundlage zur Datenverarbeitung, konkret für eine Übermittlung von Daten an die im Gesetztestext genannten Stellen. Der Träger, der gesetzlich zur Auskunft verpflichtet ist, benötigt dafür keine Einwilligung des Jugendlichen.

4.1.5 Art. 9 Abs. 2 lit. h DSGVO

Nach dieser Bestimmung ist die Verarbeitung von Daten für die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich zulässig, wenn diese Daten von Fachpersonal verarbeitet werden und dieses Fachpersonal dem Berufsgeheimnis unterliegt.

Ob die Datenverarbeitung im Rahmen der Beratung und Begleitung auf diese Rechtsgrundlage gestützt werden kann, muss bezweifelt werden, da in der Offenen Jugendarbeit grundsätzlich keine „*Versorgung oder Behandlung im Sozialbereich*" oder eine „*Verwaltung von Systemen und Diensten im Sozialbereich*" erfolgt, wie sie z.B. für Pflege- und Betreuungseinrichtungen typisch ist, die mit den betreuten Personen eine Vereinbarung

[1] In den einschlägigen Gesetzen der anderen Länder können ähnliche Regelungen vorgesehen sein, vgl. § 10 Steiermärkisches Jugendgesetz. Weitere Jugendschutz- und Jugendfördergesetze finden sich unter www.ris.bka.gv.at.

abgeschlossen haben, in der die wesentlichen Rechte und Pflichten aus dem Betreuungsverhältnis geregelt werden.

Für die Offene Jugendarbeit ist dieser Tatbestand daher kaum von Praxisrelevanz.

4.2 Berechtigte Interessen der Einrichtung (Art. 6 Abs. 1 lit. f DSGVO)

Bei einigen ihrer Datenverarbeitungen werden sich die Einrichtungen Offener Jugendarbeit auf berechtigte Interessen stützen können.
Von der DSGVO wird zwar verlangt, dass die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen dürfen (bei Kindern ist ein besonders strenger Maßstab anzulegen), in der Praxis wird jedoch ein Mindestmaß an Datenverarbeitung unerlässlich sein, um einen funktionierenden Betriebsablauf in der Einrichtung sicher zu stellen.

Dies betrifft insbesondere folgende Verarbeitungstätigkeiten:
- Tagesdokumentation
- Teambesprechungen (soweit keine sensiblen/strafrelevanten Daten besprochen werden)
- Projekte
- Kontaktformulare
- Ehrenamtliche Mitarbeiter*innen

4.3 Erfüllung vertraglicher Pflichten der Einrichtung (Art. 6 Abs. 1 lit. b DSGVO)

Alternativ zu den „*berechtigten Interessen*" kann sich die Einrichtung auf die „*Erfüllung vertraglicher Pflichten*" stützen.

Dieser Tatbestand setzt voraus, dass zwischen den Jugendlichen und der Einrichtung der Offenen Jugendarbeit eine zivilrechtliche Vereinbarung zustande kommt. Dafür spricht, dass von der Einrichtung Leistungen angeboten werden und die Jugendlichen – als Gegenleistung für die Inanspruchnahme dieser Leistungen – die von der Einrichtung vorgegebenen Hausregeln bzw. Hausordnung akzeptieren müssen.

Ähnliches gilt für ehrenamtliche Mitarbeiter*innen. Auch hier kann das Zustandekommen einer zivilrechtlichen Vereinbarung mit der Einrichtung unterstellt werden.

In jedem Fall kann sich die Einrichtung aber bei der Erfüllung ihrer Pflichten aus dem Dienstvertrag bei Mitarbeiter*innen (z.B. betreffend die monatliche Gehaltsabrechnung) auf diese Rechtsgrundlage stützen.

4.4 Erfüllung von Pflichten aus dem Arbeits- und Sozialrecht (Art. 9 Abs. 2 lit. b DSGVO)

Auf diese Rechtsgrundlage kann sich die Einrichtung bei der Verarbeitung besonderer Kategorien personenbezogener Daten (insbesondere sensibler Gesundheitsdaten) ihrer Mitarbeiter*innen beziehen.

In der Praxis betrifft dies z.B. die Datenverarbeitung im Rahmen der Krankenstandsverwaltung.

4.5 Einwilligung der betroffenen Person (Art. 6 Abs. 1 lit. a DSGVO und Art. 9 Abs. 2 lit. a DSGVO)

Die Einwilligung der betroffenen Personen ist vor allem in jenen Fällen einzuholen, in denen sich die Einrichtung nicht auf „berechtigte Interessen" oder die „Erfüllung vertraglicher Pflichten" stützen kann. In der Praxis betrifft dies folgende Fälle:

- Beratung und Begleitung, wenn sensible/strafrelevante Daten besprochen werden
- Teambesprechungen, wenn sensible/strafrelevante Daten besprochen werden
- Fotos[2]
- Internet (Cookies und Webtracking-Tools, wenn damit personenbezogene Daten erfasst werden)
- Bewerbungsunterlagen (Evidenthaltung[3])

4.5.1 Erfordernisse

4.5.1.1 Eindeutige bestätigende Handlung

Nach Artikel 4 Z 11 DSGVO ist die Einwilligung der betroffenen Person *„jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden*

[2] Früher wurden Zustimmungen für die Fotoverwendung häufig mündlich oder im Wege einer schlüssigen Handlung des Betroffenen eingeholt. Unklar ist, ob in diesen „alten Fällen" nachträgliche schriftliche Einwilligungen einzuholen sind, insbesondere dann, wenn keine Kontaktdaten – der inzwischen erwachsenen – Jugendlichen mehr vorliegen. In jedem Fall muss hier einem Auskunft- und Löschungsbegehren dieser Personen Folge geleistet werden.

[3] Evident halten bedeutet, dass eine Bewerbung zu einem späteren Zeitpunkt noch einmal mit einer anderen Stellenausschreibung abgeglichen wird. Ein solcher späterer Abgleich ist nur mit Einwilligung des/der Bewerbers/in zulässig, da es sich hier um einen neuen Verarbeitungszweck handelt.
Davon zu unterscheiden ist die bloße Speicherung der Bewerbungsunterlagen zum Zweck der Abwehr allfälliger Ansprüche nach dem Gleichbehandlungsgesetz wegen diskriminierender Ablehung des/der Bewerbers/in für die Dauer von sieben Monaten ab dem Zeitpunkt der Absage. Hier kann sich der Träger auf berechtigte Interessen stützen. Würde er die Bewerbungsunterlagen löschen bzw. vernichten, wäre er allfälligen Ansprüchen (Behauptungen) des/der Bewerbers/in schutzlos ausgesetzt.

Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist".

Eine „eindeutig bestätigende Handlung" kann nicht nur die Unterfertigung einer Einwilligungserklärung, sondern auch die Antwort auf eine E-Mail-Anfrage oder z.B. auch das Ankreuzen einer Check-Box im Internet oder auf einem Formular sein.

4.5.1.2 Nachweislichkeit

Der Verantwortliche muss nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Mündliche, stillschweigende oder konkludente Einwilligungen sind daher in der Praxis nicht mehr ratsam.

4.5.1.3 Jederzeitige Möglichkeit des Widerrufs

Der Verantwortliche hat die Pflicht, auf das Widerrufsrecht hinzuweisen. Fehlt dieser Hinweis, ist die Einwilligungserklärung wirkungslos.

4.5.1.4 Koppelungsverbot

Erfolgt die Einwilligung der betroffenen Person durch schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.

4.5.1.5 Freiwilligkeit

Die Einwilligung muss freiwillig erteilt werden. Die Erfüllung eines Vertrages darf somit nicht von der Einwilligung abhängig sein, wenn diese Einwilligung für die Vertragserfüllung gar nicht erforderlich ist.

Beispiel: Das Zustandekommen eines Dienstverhältnisses darf nicht davon abhängig gemacht werden, ob vom Mitarbeiter eine Einwilligungserklärung zur Veröffentlichung seines Fotos auf der Website der Einrichtung abgegeben wird.

4.5.1.6 Ausdrücklichkeit

Wird in die Verarbeitung besonderer Kategorien personenbezogener Daten (insbesondere sensible Gesundheitsdaten) eingewilligt, muss die Einwilligung ausdrücklich erklärt werden. Ausdrücklichkeit bedeutet in diesem Sinne, dass die Einwilligung zweifelsfrei und frei von Interpretationspieleräumen erfolgt.

Unter Berücksichtigung dieser Erfordernisse (Kapitel 4.5.1 Erfordernisse) ist die Einwilligung in Schriftform zu empfehlen (siehe Kapitel 6.2 Vorlagen und Muster).

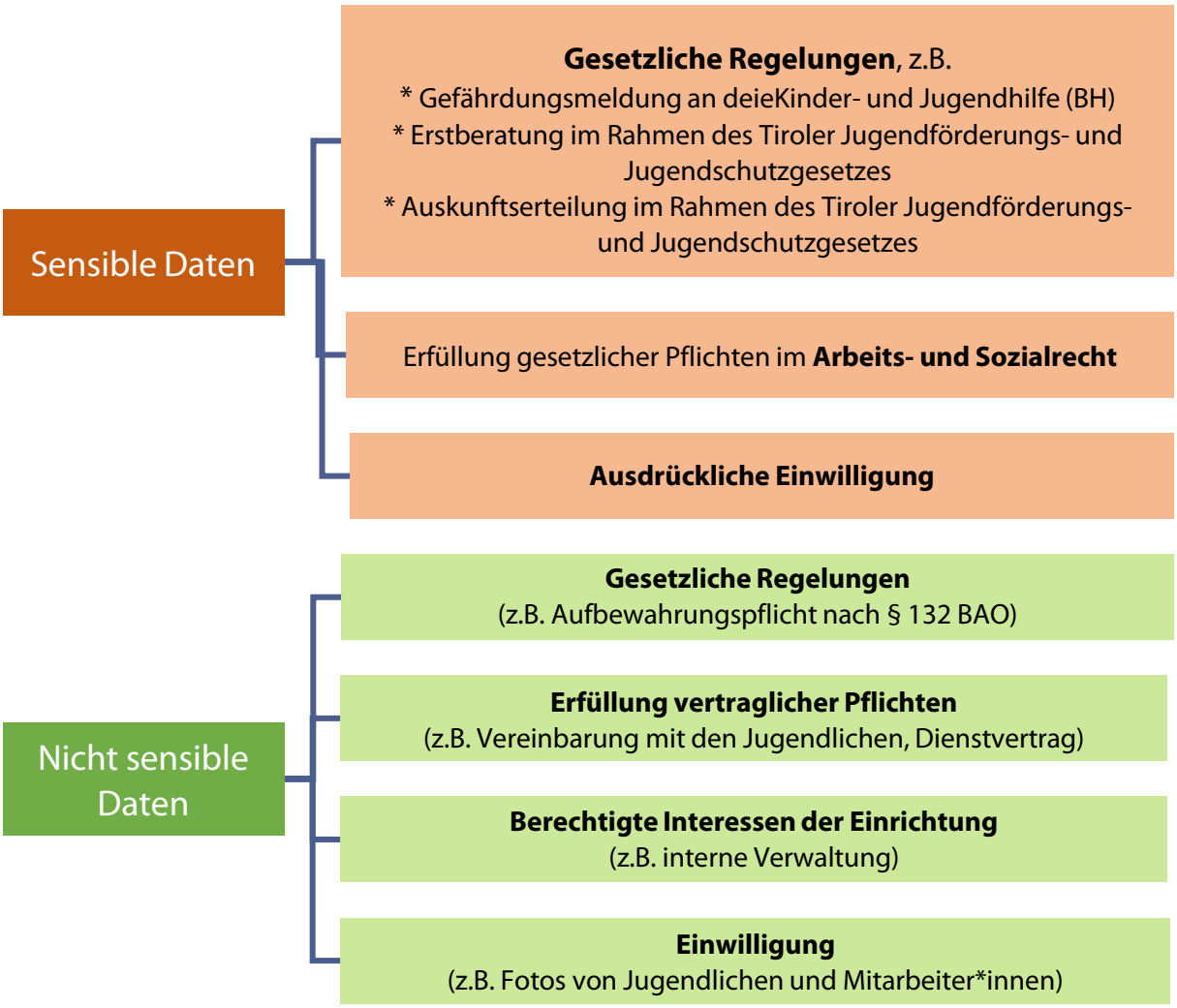
4.5.2 Mündliche Einwilligung als Alternative

Unter Berücksichtigung der besonderen Gegebenheiten im Arbeitsfeld der Offenen Jugendarbeit (Niederschwelligkeit, Freiwilligeit und Unverbindlichkeit) ist auch eine mündliche Einwilligung, die schriftlich dokumentiert wird, vorstellbar.
Um dem Erfordernis der Nachweislichkeit gerecht zu werden empfehlen wir über das Gespräch mit dem Jugendlichen eine interne Gesprächsnotiz im Beisein einer Kollegin (Zeugin) zu verfassen und abzulegen[4].

Beispiel für Gesprächnotiz: "Die Jugendliche XY hat uns mit ihren schulischen Problemen konfrontiert und um Unterstützung gebeten. Wir haben mit XY die Sinnhaftigkeit eines Gesprächs mit der Schulpsychologin diskutiert. XY ist damit ausdrücklich einverstanden, dass wir diese konsultieren und es dabei zwangsläufig zu einem Informationsauatsauch kommen wird. Wir haben XY über ihre Rechte im Datenschutz (insbesondere auf jederzeitigen Widerruf ihrer Einwilligung) aufgeklärt. Meine Kollegin war während dem gesamten Gespräch anwesend und kann dessen Inhalt bezeugen.
Zeit / Ort:_____ Unterschriften:_____

[4] Diese Variante stellt einen Kompromiss zwischen dem Handlungsfeld der Offenen Jugendarbeit und den strengen Formalitäten des Datenschutzrechtes dar. Die Entscheidungspraxis der Datenschutzbehörde wird zeigen ob diese Variante ausreichend ist.

4.6 Übersicht Rechtsgrundlagen



5 Wichtige Aufgaben und Pflichten

5.1 Einhaltung der Grundsätze der Datenverarbeitung

Artikel 5 DSGVO beschreibt Grundsätze, die bei jeder Datenverarbeitung erfüllt sein müssen. Die Einrichtung muss die Einhaltung dieser Grundsätze nachweisen können (Rechenschaftspflicht). Die wichtigsten Grundsätze sind:

5.1.1 Rechtmäßigkeit

Personenbezogene Daten müssen rechtmäßig, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.
„*Rechtmäßig*" bedeutet, dass Daten nur aufgrund einer tauglichen Rechtsgrundlage verarbeitet werden dürfen (siehe Kapitel 4 Kein Datenschutz ohne Rechtsgrundlage) und dabei die Bestimmungen der DSGVO eingehalten werden.

„*Nach Treu und Glauben*" bedeutet, dass die Betroffenen über die Datenverarbeitung aufgeklärt werden müssen und hinsichtlich der näheren Umstände der Datenverarbeitung nicht in die Irre geführt werden dürfen.

5.1.2 Datenminimierung

Personenbezogene Daten müssen dem Zweck nach angemessen sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden.

5.1.3 Speicherbegrenzung

Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Gesetzliche Aufbewahrungspflichten wie z.B. nach § 132 der Bundesabgabenordnung (7-jährige Aufbewahrungspflicht für alle steuerrelevanten Belege und Unterlagen) bleiben davon unberührt.

5.1.4 Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Davon umfasst ist auch der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Im Rahmen der Datensicherheitsmaßnahmen wird darauf noch ausführlich Bezug genommen (siehe Kapitel 5.4 Datensicherheitsmaßnahmen).

5.2 Verzeichnis aller Verarbeitungstätigkeiten

Von jeder Einrichtung der Offenen Jugendarbeit bzw. von ihrem Träger (Verein oder Gemeinde) ist ein Verzeichnis der Verarbeitungstätigkeiten zu erstellen.

5.2.1 Notwendige Angaben

- Namen und Kontaktdaten des Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten
- Die Zwecke der Verarbeitung
- Eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- Die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern

- Wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- Wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO

5.2.2 Verzeichnisvorlagen

Folgende Vorlagen wurden für die in der Praxis wichtigsten Verarbeitungstätigkeiten in der Offenen Jugendarbeit erstellt; diese betreffen: Personalverwaltung, Tagesdokumentation, Erstberatung sowie Beratung und Begleitung (siehe Kapitel 6.2 Vorlagen und Muster).

HINWEIS: Bei diesen Vorlagen handelt es sich um Orientierungshilfen, die an die spezifischen Voraussetzungen und individuellen Rahmenbedingungen jeder einzelnen Einrichtung anzupassen sind.

5.3 Technische und organisatorische Maßnahmen (TOMs)

Artikel 24 DSGVO verlangt geeignete technische und organisatorische Maßnahmen (TOMs). Einrichtungen müssen die Implementierung solcher TOMs nachweisen können.

5.3.1 Beispiele für TOMs

- Verpflichtung aller Mitarbeiter*innen zur Wahrung des Datengeheimnisses (Verschwiegenheitspflicht)
- Ausarbeitung eines Löschungskonzeptes (Regelungen zur Speicherdauer von personenbezogenen Daten)
- Schulung und Sensibilisierung von Mitarbeiter*innen im Bereich Datenschutz
- Einführung von Prüf- und Kontrollverfahren zur Gewährleistung, dass Maßnahmen nicht nur am Papier stehen, sondern in der Praxis angewandt werden und funktionieren (Compliance System)

5.4 Datensicherheitsmaßnahmen

Nach Artikel 32 DSGVO sind geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko der Datenverarbeitung angemessenes Schutzniveau zu gewährleisten.

5.4.1 Beispiele für Datensicherheitsmaßnahmen:

- Zutrittskontrolle (Verhinderung des Zutritts zu Räumlichkeiten und Datenverarbeitungsanlagen für Unbefugte), z.B. durch Sicherheitsschlösser. In der

Einrichtung sind Räumlichkeiten, die Jugendlichen zur Verfügung stehen, und interne Verwaltungsbereiche strikt voneinander zu trennen (Versperren von Türen).

- Zugangskontrolle (Verwehrung des Zugangs zu Datenverarbeitungsanlagen für Unbefugte), z.B. durch die eindeutige Authentifizierung von Mitarbeiter*innen mittels Benutzerkennung und Passwort. Keine Doppelverwendung von Benutzer-Accounts.
- Zugriffskontrolle (Gewährleistung, dass zugangsberechtigte Mitarbeiter*innen im Wege der Rechteverwaltung ausschließlich Zugriff auf jene personenbezogenen Daten haben, die sie zur Aufgabenerledigung unbedingt benötigen).
- Weitergabekontrolle[5] (Dokumente von Jugendlichen und interne Dokumente wie Personalabrechnungsdokumente müssen auf sicheren Wegen übermittelt werden, z.B. durch Nutzung von virtuellen privaten Netzwerken (VPN), E-Mail Verschlüsselung oder Passwortschutz einzelner Dokumente (PDF-Verschlüsselung, Zip-Verschlüsselung).
- Verfügbarkeitskontrolle (Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt und wiederherstellbar sind), z.B. durch Backup- und Recovery-Systeme.
- Physische Maßnahmen (Absicherung von Serverstandorten, Zurverfügungstellung einer ausreichenden Anzahl an Feuerlöschern, Kontrolle und Verwaltung der Schlüsselvergabe).
- Sicherheitsmaßnahmen im Arbeitsalltag, z.B.
    - **Clear Desk Policy**: Vertrauliche Unterlagen sind bei Abwesenheit zu verschließen und zwar z.B. auch dann, wenn man nur kurz „*zur Teambesprechung*" oder „*auf eine Zigarette*" geht. Besonders ist die Clear Desk Policy auch bei Arbeitsplätzen zu beachten, die von mehreren Teilzeitkräften benutzt werden (Desk-Sharing).
    - **Clear Screen Policy**: Automatisches Aktivieren der Bildschirmsperre („Windows-Taste + L") auch bei sehr kurzer Abwesenheit, wie z.B. beim Toilettengang. Einrichtung von Bildschirmschonern mit passwortgeschützter Aufhebung. Ebenso, wenn Laptops in den Ruhezustand versetzt werden. PIN- oder Passwort-Eingabe bei Smartphones und Tablets mit möglichst kurzem Zeitintervall. Keine unbeaufsichtigte Weitergabe von mobilen IT-Geräten („*nur kurz was im Internet schauen…*").
    - **Passwortschutz**: Passwörter sollten mindestens acht Zeichen lang sein und aus Klein- und Großbuchstaben, Zahlen sowie Sonderzeichen bestehen. Passwortnotizen dürfen nicht am Arbeitsplatz aufbewahrt werden (z.B. unter der Schreibtischunterlage oder als „Post-it" an der Schreibtisch-Pinnwand oder am Bildschirm).

[5] Auch messenger-Dienste (zB whatsapp) stellen eine Form der Datenübermittlung dar. Dabei ist sicherzustellen, dass Dienste eingesetzt werden, die eine end-to-end Verschlüsselung vorsehen. Ob whatsapp aus heutiger Sicht trotz end-to-end Verschlüsselung datenschutzkonform ist bleibt fraglich, da offenbar personenbezogene Daten des/der Nutzers/in an den Eigentümer in den USA weitergeleitet werden können. Alternative Anbieter (zB gemeinnützige open source Projekte) verzichten auf eine solche Datenübertragung.

- **Kopien / Ausdrucke**: Kein Herumliegenlassen von Dokumenten z.B. im „Sammelkarton“ neben dem Gang- oder Gemeinschaftsdrucker. Papier mit vertraulichen Informationen ist zu shreddern und nicht mit dem normalen Altpapier zu entsorgen.
- **Mobile IT-Geräte**: Diebstahlsichere Aufbewahrung von Geräten sowohl im Innendienst und insbesondere auch im Außendienst. Im PKW blickdichte Aufbewahrung (Kofferraum, verschließbare Konsole), in öffentlichen Verkehrsmitteln kein Herumliegenlassen von Geräten (z.B. während Toilettengang im Zug). Einsatz von Virenschutzprogrammen sowie von Diensten (Apps), die es erlauben, alle Daten auf einem gestohlenen oder verlorenen Smartphone aus der Distanz zu löschen.
- **Personelle Änderungen**: Beim Ausscheiden von Mitarbeiter*innen sind sämtliche Schlüssel und IT-Geräte (z.B. Laptop, Smartphone, Speichermedien) zurückzustellen. Zugangsberechtigungen und Zugriffsrechte müssen angepasst, entzogen oder gelöscht werden, insbesondere auch Berechtigungen für Telearbeitszugänge (Home Office) sowie Daten auf privaten Smartphones und Laptops (Bring Your Own Device). Neue Mitarbeiter*innen sind neu im System einzurichten und freizuschalten (keine neuerliche Vergabe von bestehenden Benutzerkonten).

5.5 Datenschutz-Folgenabschätzung

Nach Artikel 35 DSGVO haben Unternehmen eine Datenschutz-Folgenabschätzung durchzuführen, wenn eine Form der Datenverarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat (*Privacy impact assessment*).

Eine Datenschutz-Folgenabschätzung ist insbesondere dann durchzuführen, wenn eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten (z.B. von Gesundheitsdaten) und/oder von strafrelevanten Daten erfolgt.

Wenn überhaupt, könnte eine „umfangreiche Verarbeitung“ solcher besonderer Daten am ehesten in der Mobilen Jugendarbeit im Wege der **Beratung und Begleitung** vorliegen.

EMPFEHLUNG: Ob in der Offenen Jugendarbeit eine Datenschutz-Folgenabschätzung durchzuführen ist, wird erst die Entscheidungspraxis der Datenschutzbehörde und die Judikatur der unabhängigen Gerichte klären. Im Zweifel wird daher aus Absicherungsgründen empfohlen, eine Datenschutz-Folgenabschätzung für die Beratung und Begleitung in der Mobilen Jugendarbeit durchzuführen, die zumindest folgende Inhalte aufweist:

- Eine systematische Beschreibung der Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von der Einrichtung verfolgten berechtigten Interessen
- Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- Eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- Die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen (strengere Anwendung von TOMs und Datensicherheitsmaßnahmen)

HINWEIS: Es ist zu erwarten, dass die nationalen Kontrollbehörden (in Österreich die Datenschutzbehörde) einen Leitfaden zur Erstellung einer Datenschutz-Folgenabschätzung zur Verfügung stellen werden. Der Zeitpunkt dieser Veröffentlichung ist offen.

5.6 Datenschutzbeauftragter

Nach Artikel 37 DSGVO haben Verantwortliche unter anderem dann verpflichtend einen Datenschutzbeauftragten zu benennen, wenn ihre **Kerntätigkeit** in der umfangreichen Verarbeitung besonderer Kategorien und/oder strafrelevanter Daten besteht.

Diese besondere Datenverarbeitung, die insbesondere in der Mobilen Jugendarbeit im Wege der Beratung und Begleitung vorliegen kann, ist in der Praxis aber nur eine von mehreren Unterstützungsleistungen der Offenen Jugendarbeit. Es ist somit – mangels „Kerntätigkeit" – nicht davon auszugehen, dass Einrichtungen der Offenen Jugendarbeit verpflichtend einen Datenschutzbeauftragten benennen müssen.

Sind **Gemeinden** Rechtsträger der Einrichtung, spielen diese Überlegungen allerdings keine Rolle, da Gemeinden als Gebietskörperschaften von vorneherein einen Datenschutzbeauftragten haben müssen. In weiterer Folge ist dieser Datenschutz-beauftragte der Gemeinde dann auch für die Einrichtungen der Offenen Jugendarbeit zuständig.

5.7 Meldung von Datenschutz-Vorfällen

Nach Artikel 33 DSGVO sind seit 25. Mai 2018 alle Verletzungen des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, der Datenschutzbehörde zu melden (Data breach notification).

*Beispiel: In der Nacht wird eingebrochen und aus dem Verwaltungsbereich eines Jugendzentrums zwei Laptops entwendet. Auf den Geräten waren alle internen Dokumentationen und damit personenbezogene Daten von Jugendlichen und Mitarbeiter*innen gespeichert. Ein solcher Vorfall wäre künftig der Behörde zu melden.*

Keine Meldepflicht besteht, wenn der Datenschutzvorfall voraussichtlich zu keinem Risiko für die Betroffenen führt, z.B., weil die betroffenen personenbezogenen Daten auf Festplatten gespeichert wurden, die ausreichend verschlüsselt waren.

Der Tatbestand der Meldepflicht wird noch nicht verwirklicht, wenn bloß eine Verletzung der jederzeitigen Verfügbarkeit von Daten (z.B. Serverausfall) vorliegt.

5.8 Informierung der Betroffenen

Werden künftig Daten bei Jugendlichen erhoben (insbesondere, weil sie von ihnen selbst, z.B. im Rahmen der Beratung und Begleitung mitgeteilt werden), sind ihnen nach Artikel 13 DSGVO zumindest folgende Informationen mitzuteilen, wenn die Jugendlichen nicht schon darüber verfügen:

- Namen und Kontaktdaten der Einrichtung und gegebenenfalls des/der Datenschutzbeauftragten
- Die Verwendungszwecke und die Rechtsgrundlage für die Verarbeitung
- Wenn die Rechtsgrundlage eine Interessenabwägung ist, die entsprechenden berechtigten Interessen
- Gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- Gegebenenfalls die Absicht, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln

Die Information ist nach Artikel 12 DSGVO in „*präziser, transparenter, verständlicher und leicht zugänglicher Form*" zur Verfügung zu stellen.

Unter Berücksichtigung der besonderen Gegebenheiten im Arbeitsfeld der Offenen Jugendarbeit (Niederschwelligkeit, Freiwilligeit und Unverbindlichkeit) ist neben der Aushändigung einer schiftlichen Informationsblattes auch ein Aushang in den Räunlichkeiten der betreffenden Einrichtung vorstellbar. Sinnvollerweise kann dies auch in Kombination bei allenfalls bestehenden Hausregeln erfolgen[6].

Eine vergleichbare Informationspflicht würde nach Artikel 14 DSGVO auch dann bestehen, wenn künftig Daten bei Dritten erhoben werden (z.B. indem von Systempartner*innen Daten von Jugendlichen an die Einrichtung übermittelt werden). Eine **Ausnahme** von dieser Informationspflicht besteht allerdings dann, wenn die betreffenden Informationen einem Berufsgeheimnis unterliegen und daher vertraulich behandelt werden müssen. Im Fall der

[6] Diese Variante stellt einen Kompromiss zwischen dem Handlungsfeld der Offenen Jugendarbeit und den strengen Formalitäten des Datenschutzrechtes dar. Die Entscheidungspraxis der Datenschutzbehörde wird zeigen ob diese Variante ausreichend ist.

Offenen Jugendarbeit ist diese Ausnahme verwirklicht (vgl. die im § 2 Tiroler Jugendförderungs- und Jugendschutzgesetz normierte Verschwiegenheitspflicht[7]).

5.9 Transparenz

Betreffend die Datenverarbeitungen auf der Website der Einrichtung (z.B. Kontaktaufnahme über ein Kontaktformular oder die bekannt gegebene E-Mail-Adresse) kann die Information nach Artikel 13 DSGVO in Form einer „Datenschutzerklärung" erfolgen.
Dabei sind die Betroffenen (Besucher*innen der Website) über ihre Rechte aufzuklären. Im Einzelnen handelt es sich um:

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch

Die Datenschutzerklärung sollte nicht in das Impressum eingebettet, sondern als eigener Punkt (z.B. „Datenschutz") dargestellt werden.

Sind Träger in sozialen Netzwerken (social media) vertreten, empfehlen wir dort zumindest auf die Datenschutzerklärung der Website zu verlinken. Es ist derzeit unklar ob in sozialen Netzwerken eine eigene Datenschutzerkärung zu verankern ist.

HINWEIS: Für die Datenschutzerklärung bietet die Website der Österreichischen Wirtschaftskammer die wichtigsten Textbausteine. Link zur WKO-Website.

5.10 Interne Datenschutzstrategien

Als Verantwortliche unterliegen die Rechtsträger der Einrichtung der Rechenschaftspflicht nach Artikel 5 Absatz 2 DSGVO und müssen nachweisen, dass sie die allgemeinen Grundsätze für die Datenverarbeitung einhalten (siehe Kapitel 5.1 Einhaltung der Grundsätze der Datenverarbeitung).

Weiters hat der Verantwortliche nach Artikel 24 Absatz 2 DSGVO im Wege von internen Datenschutzstrategien die Umsetzung geeigneter TOMs nachzuweisen (siehe Kaptiel 5.3 Technische und organisatorische Maßnahmen).

[7] Dass eine solche Verschwiegenheitspflicht in anderen Bundesländern – mangels gesetzlicher Regelungen – fehlt, dürfte in der Praxis keine großen Auswirkungen haben, da im Regelfall der Jugendliche auf den/die Jugendarbeiter*in zukommen wird und ihn mit seinen Problemen konfrontiert (Art. 13 DSGVO).

EMPFEHLUNG: Aus Zweckmäßigkeitsgründen sollten nicht nur die Einhaltung der allgemeinen Grundsätze für die Datenverarbeitung und die Umsetzung geeigneter TOMs, sondern auch weitere getroffene Maßnahmen im Zuge der Umsetzung der DSGVO schriftlich dokumentiert werden:

- Verzeichnis der Verarbeitungstätigkeiten nach Artikel 30 DSGVO
- Einhaltung der Grundsätze nach Artikel 5 DSGVO
- TOMs nach Artikel 24 DSGVO
- Datensicherheitsmaßnahmen nach Artikel 32 DSGVO
- Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO (wenn erforderlich)

6 Arbeitshilfen

6.1 Checkliste

6.1.1 Dringende Maßnahmen

- ☐ Wurde das Verzeichnis aller Verarbeitungstätigkeiten erstellt?
- ☐ Wurde geprüft, in welchen Fällen die (ausdrückliche) Einwilligungserklärung von Jugendlichen einzuholen ist?
- ☐ Werden die Grundsätze für jede Datenverarbeitung eingehalten?
- ☐ Werden betroffene Personen über die Verarbeitung ihrer personenbezogenen Daten informiert?
- ☐ Wurde eine Datenschutzerklärung auf der Website der Einrichtung veröffentlicht?
- ☐ Wurden Dienstnehmer*innen schriftlich zum Datengeheimnis verpflichtet?
- ☐ Werden für jede Verarbeitung von Fotos Einwilligungserklärungen der betroffenen Personen eingeholt?
- ☐ Wurden mit externen Dienstleistern (Auftragsverarbeitern) Verträge über die Auftragsverarbeitung abgeschlossen?

6.1.2 Weiterführende Maßnahmen

- ☐ Wurden geeignete „TOMs“ ausgewählt und implementiert?
- ☐ Wurden die Datensicherheitsmaßnahmen überprüft und gegebenenfalls angepasst?
- ☐ Wurde eine Datenschutz-Folgenabschätzung für die Beratung und Begleitung in der Mobilen Jugendarbeit durchgeführt?
- ☐ Wurden die internen Datenschutzstrategien ausgearbeitet?[8]

[8] Es wird empfohlen, die internen Datenschutzstrategien zu strukturieren und sich dabei an den Punkten der Checkliste zu orientieren.

6.2 Vorlagen und Muster

HINWEIS: Die nachfolgenden Vorlagen werden trotz sorgfältiger Bearbeitung ohne Gewähr zur Verfügung gestellt. Sie sollen eine erste Orientierung ermöglichen. Die einzelfall-bezogene und detaillierte Auseinandersetzung auf Grundlage des Einrichtungskonzepts und der tatsächlichen Tätigkeiten bleibt unerlässlich.

- Vorlage Verarbeitungsverzeichnis (Personalverwaltung, Tagesdokumentation, Erstberatung, Beratung und Begleitung)
- Mustervertrag über die Auftragsverarbeitung
- Musterverschwiegenheitserklärung für Mitarbeiter*innen (Datengeheimnis)[9]
- Mustereinwilligung bezüglich Fotos
- Mustereinwilligung bezüglich Datenverarbeitung
- Musterinformation gemäß Artikel 13 DSGVO

Diese Vorlagen stehen als offene Dokumente (excel oder word) zur Verfügung.

[9] Neben Mitarbeiter*innen wird empfohlen, auch andere Personenkreise, die typischerweise Zugriff auf personenbezogene Daten haben können, eine Verschwiegenheitserklärung unterfertigen zu lassen. In der Praxis betrifft dies insbesondere ehrenamtliche Mitarbeiter*innen sowie externe Honorarkräfte (z.B. Coaches oder Trainer) und beigezogene Reinigungskräfte.