SPIELRAUM. Digital

PRAXISLEITFADEN FÜR TRÄGER DER KINDER- UND JUGENDHILFE

Sensible Daten im Jugendhilfealltag

Messenger, private Endgeräte, Formulare und Cloudspeicher sicher einordnen

SPIELRAUM.Digital
Ein Angebot der SPIELRAUM Jugendhilfe GmbH
spielraum-digital.de

Stand: Juli 2026

01 Warum dieses Thema zählt

Träger der Kinder- und Jugendhilfe verarbeiten Angaben, die weit über Namen und Kontaktdaten hinausgehen. Vieles davon betrifft Kinder und Jugendliche in ohnehin verletzlichen Lebenslagen — und bleibt jahrelang aktenrelevant.

Was im Alltag tatsächlich verarbeitet wird

- Gesundheitsinformationen und Diagnosen
- Angaben zu Medikation
- Hilfepläne und Zielvereinbarungen
- Krisenverläufe und Vorfallsdokumentation
- familiäre Situationen und Beziehungskonstellationen
- Gewalt- und Missbrauchserfahrungen
- Schulische Verläufe und Behördenkorrespondenz
- Angaben zu Sorgeberechtigten
- Personal- und Qualifikationsunterlagen
- Führungszeugnisse und Nachweise

> **Ein erheblicher Teil dieser Angaben fällt unter Art. 9 DSGVO — besondere Kategorien personenbezogener Daten. Für sie gilt ein grundsätzliches Verarbeitungsverbot mit eng gefassten Ausnahmen.**

Was daraus folgt

Die Datenschutz-Grundverordnung verlangt in Art. 5, dass Daten rechtmäßig, zweckgebunden, datenminimiert sowie integer und vertraulich verarbeitet werden — und dass der Verantwortliche das nachweisen kann. Art. 24, 25 und 32 DSGVO konkretisieren das zu einer Pflicht, technische und organisatorische Maßnahmen am Risiko auszurichten, sie datenschutzfreundlich voreinzustellen und regelmäßig zu überprüfen.

Für die Jugendhilfe kommt eine Besonderheit hinzu: Nimmt ein öffentlicher Träger Einrichtungen und Dienste freier Träger in Anspruch, ist nach § 61 Abs. 3 SGB VIII sicherzustellen, dass der Schutz personenbezogener Daten dort in entsprechender Weise gewährleistet ist. § 64 SGB VIII bindet die Verwendung an den Zweck der Erhebung, § 65 SGB VIII schützt anvertraute Daten in der persönlichen und erzieherischen Hilfe besonders.

Der Maßstab ist der Schutzbedarf, nicht die Betriebsgröße

Die Anforderungen richten sich nach dem Risiko für die betroffenen Personen — nicht danach, wie viele Mitarbeitende ein Träger hat. Ein Team von acht Personen, das Krisenverläufe dokumentiert, verarbeitet ebenso schutzbedürftige Daten wie eine große Einrichtung. Der Aufwand darf angemessen sein; das Schutzniveau nicht beliebig.

02 Wie informelle Strukturen entstehen

Kaum ein Träger hat sich bewusst für unklare Zuständigkeiten entschieden. Die meisten Wege sind gewachsen, weil sie in dem Moment funktioniert haben, in dem sie gebraucht wurden.

Tempo schlägt Struktur
Übergaben, Krisen und Rückfragen entstehen abends, am Wochenende und unterwegs. Ein Chat ist in Sekunden geöffnet, ein Antrag auf ein neues System dauert Wochen.

Die Arbeit ist mobil
Ein großer Teil der Tätigkeit findet nicht am Schreibtisch statt. Werkzeuge, die auf dem Smartphone sofort funktionieren, setzen sich durch.

Keine eigene IT
Gerade kleinere und neu gegründete Träger haben keine IT-Abteilung, die Alternativen prüft, einrichtet und erklärt.

Einzellösungen wachsen mit
Was mit drei Personen gut funktioniert hat, wird bei dreißig unübersichtlich — meist ohne dass jemand den Übergang bemerkt.

Kosten und Aufwand
Fachsoftware ist häufig auf große Einrichtungen zugeschnitten, teuer und schwerfällig. Kostenlose Werkzeuge sind sofort verfügbar.

Datenschutz kommt später
Strukturen entstehen oft erst, wenn der Betrieb bereits läuft — und müssen dann nachträglich auf gewachsene Wege angewendet werden.

> **Pragmatisch gestartet bedeutet nicht automatisch dauerhaft geeignet.**

Dieser Leitfaden bewertet keine Person und kein Team. Er beschreibt, an welchen Stellen die Kontrolle über sensible Daten typischerweise verloren geht — und was nötig ist, um sie zurückzugewinnen, ohne die tägliche Arbeit zu erschweren.

Das Problem ist nicht die Digitalisierung

Digitale Werkzeuge haben die Dokumentation in der Jugendhilfe spürbar erleichtert. Kritisch wird es dort, wo Digitalisierung unkontrolliert geschieht: ohne geklärte Verantwortlichkeit, ohne persönliche Konten, ohne Übersicht darüber, wo Daten liegen und wer sie sehen kann.

03 Fünf typische Alltagssituationen

Jede dieser Situationen hat einen nachvollziehbaren Grund. Entscheidend ist die dritte Spalte: Wo genau entsteht das Risiko — und ist es beherrschbar?

SITUATION	WARUM PRAKTISCH	WO DAS RISIKO ENTSTEHT
Private WhatsApp-Gruppe fürs Team	Alle sind ohnehin erreichbar, Nachrichten kommen sofort an, niemand muss geschult werden.	Fallinformationen liegen auf privaten Geräten und in privaten Konten. Wer ausscheidet, behält Verläufe und Medien. Adressbuchzugriff, automatische Medienspeicherung und private Backups lassen sich nicht zentral steuern.
Tagesbericht über ein Online-formular	Schnell erstellt, von überall ausfüllbar, Ergebnisse landen automatisch in einer Tabelle.	Häufig ungeklärt: unter welchem Konto das Formular läuft, wo die Antworten gespeichert werden, wer Zugriff hat, ob ein Auftragsverarbeitungsvertrag besteht und wie gelöscht wird.
Hilfeplan im persönlichen Cloudordner	Sofort geteilt, gemeinsam bearbeitbar, immer die aktuelle Fassung.	Freigabelinks lassen sich weiterleiten, Berechtigungen wachsen unbemerkt, Downloads erzeugen lokale Kopien. Beim Ausscheiden bleibt der Ordner im privaten Konto der Person.
Klientenfoto auf dem privaten Smartphone	Dokumentation von Verletzungen, Sachschäden oder Belegen ohne zusätzliches Gerät.	Bilder wandern automatisch in private Foto-Backups und Galerien, werden dort dauerhaft gespeichert und lassen sich nicht gezielt löschen.
Gemeinsames Benutzerkonto	Ein Passwort für alle, kein Verwaltungsaufwand, jeder kommt rein.	Zugriffe sind keiner Person zuzuordnen. Beim Ausscheiden müsste das Passwort für alle geändert werden — was in der Praxis selten geschieht.

Die Aufsichtsbehörden äußern sich zum dienstlichen Messenger-Einsatz differenziert. Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz weist darauf hin, dass im dienstlichen Kontext dienstliche Endgeräte eingesetzt werden sollten und die Nutzung privater Geräte allenfalls ausnahmsweise und mit tragfähigen technischen Lösungen in Betracht kommt.

04 Was konkret passieren kann

Keine Schreckensszenarien — sondern Vorfälle, die in der Praxis regelmäßig vorkommen und selten aus Nachlässigkeit entstehen.

Ein Smartphone geht verloren
Auf dem Gerät liegen Chatverläufe mit Klarnamen, Fotos und Berichten. Ohne Geräteverwaltung lässt sich der Zugriff nicht aus der Ferne beenden.

Jemand bleibt in der Gruppe
Nach dem Ausscheiden vergisst niemand böswillig etwas — es fällt schlicht nicht auf. Der Verlauf bleibt lesbar, neue Nachrichten kommen weiter an.

Ein Freigabelink wird weitergeleitet
Gut gemeint an eine Kollegin geschickt, von dort weiter. Der Link funktioniert für jeden, der ihn hat — unbegrenzt.

Dateien sichern sich selbst
Dienstliche Fotos und Dokumente werden automatisch in ein privates Cloud-Backup übernommen, oft unbemerkt und dauerhaft.

Ein Bericht erreicht den Falschen
Eine Autovervollständigung im Mailprogramm genügt. Bei unverschlüsselten Anhängen ist der Inhalt unmittelbar lesbar.

Ein Passwort altert
Das gemeinsame Kennwort wurde bei der Einrichtung vergeben und nie geändert. Wer es einmal kannte, kennt es weiterhin.

Niemand kennt die Kopien
Berichte wurden auf private Rechner heruntergeladen, um zu Hause weiterzuarbeiten. Wo diese Dateien liegen, weiß der Träger nicht.

Ein Konto bleibt aktiv
Der Zugang einer ausgeschiedenen Person wird nicht gesperrt, weil unklar ist, wer dafür zuständig ist.

Der gemeinsame Nenner

In keinem dieser Fälle hat jemand fahrlässig gehandelt. Was fehlt, ist jeweils dasselbe: die Möglichkeit des Trägers, den Zugriff zu erkennen, zu begrenzen und zu beenden.

05 Mögliche Konsequenzen

Die folgenden Stufen bauen aufeinander auf. Sie treten nicht automatisch ein und schon gar nicht alle gemeinsam — welche greift, hängt vom Einzelfall ab.

1 **Organisationsmangel**
Schutz-, Nachweis- und Organisationspflichten können verletzt sein, wenn sensible Daten unkontrolliert über private Geräte, private Konten oder ungeeignete Wege verarbeitet werden (Art. 5 Abs. 2, Art. 24, 32 DSGVO).

2 **Datenschutzverletzung**
Werden Daten unbefugt zugänglich, geht ein Gerät verloren, bleibt eine ausgeschiedene Person in einer Gruppe oder wird eine Datei falsch freigegeben, kann eine Verletzung des Schutzes personenbezogener Daten vorliegen.

3 **Melde- und Informationspflichten**
Nach Art. 33 DSGVO ist unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden an die Aufsichtsbehörde zu melden — außer die Verletzung führt voraussichtlich nicht zu einem Risiko. Bei voraussichtlich hohem Risiko sind zusätzlich die betroffenen Personen zu benachrichtigen (Art. 34 DSGVO).

4 **Aufsichtsrechtliche Maßnahmen**
Die Datenschutzaufsicht kann Nachbesserungen verlangen, Verarbeitungen beschränken, Löschungen anordnen oder eine bestimmte Verarbeitung untersagen.

5 **Schadensersatz und Geldbußen**
Betroffene Personen können materiellen und immateriellen Schaden geltend machen (Art. 82 DSGVO). Geldbußen richten sich nach Art. 83 DSGVO; dort sind auch die Zumessungskriterien geregelt.

6 **Nachfragen von Auftraggebern und Aufsicht**
Bei erheblichen oder wiederholten Organisationsmängeln können Jugendämter, Datenschutzbeauftragte oder zuständige Stellen Nachweise und Veränderungen verlangen.

7 **Strafrechtliche Prüfung**
Strafbarkeit ist kein Automatismus. § 42 BDSG erfasst nur qualifizierte Vorsatztaten — etwa das wissentliche Zugänglichmachen von Daten einer großen Zahl von Personen in Gewinnabsicht. § 203 StGB betrifft das unbefugte Offenbaren durch bestimmte Berufsgruppen, darunter staatlich anerkannte Sozialarbeiterinnen und Sozialpädagogen sowie anerkannte Erziehungs- und Jugendberatungsstellen.

Wovon die Bewertung tatsächlich abhängt

- Sensibilität der betroffenen Daten
- Anzahl der betroffenen Personen
- ob Unbefugte tatsächlich Zugriff hatten
- Dauer des Vorfalls bis zur Entdeckung
- vorhandene Schutzmaßnahmen
- Grad des Verschuldens
- Reaktion und Zusammenarbeit des Trägers
- frühere gleichartige Vorfälle

Wichtig zur Einordnung: Ein Datenschutzmangel führt nicht dazu, dass eine Betriebserlaubnis nach § 45 SGB VIII entzogen wird. Die Vorschrift enthält keine ausdrückliche Datenschutzanforderung; sie verlangt in Absatz 3 unter anderem eine Konzeption zur Qualitätssicherung sowie eine ordnungsgemäße Buch- und Aktenführung. Datenschutz und Betriebserlaubnis sind getrennte Verfahren mit unterschiedlichen Zuständigkeiten.

06 Was nicht automatisch unzulässig ist

Dieser Abschnitt ist bewusst gesetzt. Wer aus Sorge pauschal alles verbietet, verliert die Mitarbeitenden — und bekommt Schattenlösungen statt Sicherheit.

Cloudsysteme
Nicht pauschal unzulässig. Es kommt auf Verantwortlichkeit, Verträge, Verarbeitungsorte, Rechteverwaltung und die tatsächliche Konfiguration an.

Digitale Formulare
Nicht pauschal unzulässig. Entscheidend sind das Konto, unter dem sie betrieben werden, der Speicherort der Antworten und ein geregelter Löschprozess.

Mobiles Arbeiten
Nicht pauschal unzulässig — und in der Jugendhilfe ohnehin unverzichtbar. Es braucht abgesicherte Geräte und klare Regeln.

Private Endgeräte
Können unter einem tragfähigen Konzept eingebunden werden, das dienstliche und private Daten trennt und dem Träger Zugriff auf die dienstliche Seite belässt.

Unternehmenslösungen bekannter Anbieter
Können bei passenden Verträgen, geprüfter Konfiguration und dokumentierten Maßnahmen geeignet sein — das unterscheidet sie von privat angelegten Konten.

Messenger im Dienst
Der Unterschied liegt nicht allein im Produktnamen, sondern darin, ob der Träger Konten, Geräte, Berechtigungen und Löschung steuern kann.

> **Der Unterschied liegt selten im Produkt. Er liegt darin, ob der Träger die Verarbeitung kontrolliert — oder ob sie in privaten Konten und auf privaten Geräten stattfindet.**

Neun Fragen, die den Ausschlag geben

01 Wer ist verantwortlich, wer verarbeitet im Auftrag?
02 Bestehen die erforderlichen Verträge nach Art. 28 DSGVO?
03 Wo werden die Daten verarbeitet, welche Unterauftragnehmer wirken mit?
04 Arbeiten alle Beteiligten mit persönlichen, dienstlich verwalteten Konten?
05 Sind Berechtigungen nach Rollen vergeben und dokumentiert?
06 Ist die Übertragung verschlüsselt, sind die Geräte abgesichert?
07 Lassen sich Zugriffe beenden und Daten gezielt löschen?
08 Sind Sicherungen und Wiederherstellung geregelt und erprobt?
09 Ist die tatsächliche Konfiguration dokumentiert — nicht nur die geplante?

07 Mindestanforderungen an eine geeignete Struktur

Diese Punkte sind kein Maximalprogramm, sondern die Grundlage, auf der sich alles Weitere aufbauen lässt. Sie entsprechen den Anforderungen aus Art. 5, 24, 25, 28 und 32 DSGVO.

Zugänge und Berechtigungen

- Persönliche Benutzerkonten für jede Person — keine gemeinsam genutzten Zugänge
- Keine geteilten Passwörter; Zugangsdaten werden nicht per Chat weitergegeben
- Rollenbasierte Zugriffsrechte, die dem tatsächlichen Aufgabenzuschnitt entsprechen
- Zwei-Faktor-Authentifizierung, insbesondere für administrative Zugänge
- Zeitnahe Sperrung beim Ausscheiden, mit klar benannter Zuständigkeit
- Nachvollziehbare Administration: dokumentiert, wer welche Rechte vergeben hat

Kommunikation und Geräte

- Dienstlich kontrollierte Kommunikationswege für Fallinformationen
- Geregelte Geräteverwaltung mit Bildschirmsperre, Verschlüsselung und Fernsperrung
- Trennung von dienstlichen und privaten Daten, auch auf mobilen Geräten
- Keine sensiblen Angaben über öffentliche Kontaktformulare

Betrieb und Nachweis

- Geregelte Sicherungen mit festgelegtem Rhythmus
- Wiederherstellungskonzept, das mindestens einmal tatsächlich erprobt wurde
- Vertrag zur Auftragsverarbeitung, wo erforderlich, mit transparenter Unterauftragnehmerliste
- Dokumentierte technische und organisatorische Maßnahmen
- Klare Aufbewahrungs- und Löschfristen je Datenart
- Verzeichnis der Verarbeitungstätigkeiten, das den realen Betrieb abbildet

Menschen

- Einführung neuer Mitarbeitender in die geltenden Regeln, nicht nur in die Technik
- Regelmäßige, kurze Auffrischung statt einmaliger Grundschulung
- Geregeltes und angstfreies Vorgehen bei möglichen Datenschutzvorfällen

Als methodische Grundlage für die Ausgestaltung technischer und organisatorischer Maßnahmen bietet sich das Standard-Datenschutzmodell der Datenschutzkonferenz an; es übersetzt die Anforderungen der DSGVO in prüfbare Gewährleistungsziele.

08 Schneller Selbstcheck

Zwölf Fragen als Grundlage für ein Gespräch im Leitungsteam — keine Prüfung, keine Punktzahl.

Besitzt jede Person einen eigenen dienstlichen Zugang?	Ja ☐	Nein ☐
Können wir Zugriffe beim Ausscheiden zeitnah beenden?	Ja ☐	Nein ☐
Wissen wir, auf welchen Geräten Klientendaten liegen?	Ja ☐	Nein ☐
Ist ausgeschlossen, dass dienstliche Daten in private Backups wandern?	Ja ☐	Nein ☐
Bestehen mit allen relevanten Dienstleistern die erforderlichen Verträge?	Ja ☐	Nein ☐
Können wir nachvollziehen, wer auf welche Klientendaten zugreift?	Ja ☐	Nein ☐
Sind Sicherungen und Wiederherstellung tatsächlich getestet?	Ja ☐	Nein ☐
Sind private Messenger für Fallinformationen organisatorisch ausgeschlossen?	Ja ☐	Nein ☐
Gibt es einen geregelten Ablauf für verlorene Geräte?	Ja ☐	Nein ☐
Wissen Mitarbeitende, wie sie einen möglichen Datenschutzvorfall melden?	Ja ☐	Nein ☐
Sind Aufbewahrungs- und Löschfristen festgelegt?	Ja ☐	Nein ☐
Werden sensible Angaben von öffentlichen Kontaktformularen ferngehalten?	Ja ☐	Nein ☐

Wie Sie das Ergebnis lesen

Überwiegend Ja
Gute Grundlage. Sinnvoll ist, den Stand schriftlich festzuhalten und in festen Abständen zu überprüfen — besonders nach Personalwechseln.

Mehrere Nein
Konkrete Handlungsfelder benennen und nach Dringlichkeit ordnen. Beginnen Sie dort, wo die sensibelsten Daten fließen.

Viele Nein
Die Struktur sollte systematisch neu geordnet werden. Das ist kein Grund zur Panik, aber einer, es nicht weiter aufzuschieben.

Ein Hinweis zur Ehrlichkeit

Der Check nützt nur, wenn er ehrlich beantwortet wird. „Eigentlich schon" ist in der Praxis meistens ein Nein. Der Wert liegt im offenen Blick auf die eigenen Abläufe, nicht in der Zahl der Häkchen.

09 Ein realistischer Weg

Der häufigste Grund, warum nichts passiert, ist die Vorstellung, alles auf einmal ändern zu müssen. Das ist weder nötig noch sinnvoll.

SCHRITT 01

Erfassen

Welche Werkzeuge sind tatsächlich im Einsatz — auch die, die nie offiziell eingeführt wurden? Welche Daten fließen wohin, wer hat Zugriff?

SCHRITT 02

Ordnen

Risiken und Zuständigkeiten benennen und nach Dringlichkeit sortieren. Nicht alles ist gleich kritisch.

SCHRITT 03

Überführen

Kommunikation, Dateien und Dokumentation schrittweise in kontrollierte Umgebungen bringen — beginnend dort, wo die sensibelsten Daten liegen.

SCHRITT 04

Verankern

Mitarbeitende einführen, Abläufe verbindlich festlegen, Entscheidungen dokumentieren.

> **Nicht alles muss an einem Tag ersetzt werden. Entscheidend ist ein nachvollziehbarer Weg aus gewachsenen Einzellösungen in eine kontrollierte Struktur.**

Was sich erfahrungsgemäß bewährt

- **Mit der Kommunikation beginnen.** Dort entstehen die meisten unkontrollierten Kopien, und die Umstellung ist für das Team am schnellsten spürbar.
- **Alternativen anbieten, bevor etwas untersagt wird.** Ein Verbot ohne Ersatz führt zuverlässig zu Umgehungen.
- **Eine verantwortliche Person benennen.** Nicht zwingend eine Fachkraft für Datenschutz, aber jemand, bei dem die Fäden zusammenlaufen.
- **Den Stand schriftlich festhalten.** Auch ein unvollständiger, aber dokumentierter Stand ist besser als ein guter, den niemand belegen kann.
- **Nach jedem Personalwechsel prüfen.** Das ist der Moment, in dem Zugriffe erfahrungsgemäß offen bleiben.

10 Wie SPIELRAUM.Digital unterstützt

Wir sind selbst Träger der Kinder- und Jugendhilfe. Was wir anbieten, haben wir zuerst für den eigenen Betrieb gebaut — und stellen es seither auch anderen zur Verfügung.

Website
Die öffentliche Seite des Trägers: Leistungsdarstellung, Freiplatz- kommunikation, Karriere und datensparsame Anfrageformu-lare.

Mitarbeiterportal
Dienste, Einsätze, Berichte, Nachweise und Onboarding an einem Ort — mit persönlichen Konten und rollenbasierten Rechten.

Cloud und Kommunikation
Dateien, Teamchat, Videokonferenzen, Kalender, Aufgaben und Boards in einer vom Träger kontrollierten Umgebung.

Benutzer- und Rechtekonzepte
Unterstützung dabei, Rollen sinnvoll zuzuschneiden und Berechtigungen nachvollziehbar zu dokumentieren.

Einrichtung und Migration
Übernahme bestehender Daten und Ablösung gewachsener Einzellösungen — schrittweise und ohne Betriebsunterbrechung.

Betrieb in Deutschland
Auf Wunsch vollständig betreut, mit Hosting in deutschen Rechenzentren — alternativ Installation in Ihrer eigenen IT.

Updates und Sicherungen
Aktualisierungen, Sicherungen und Überwachung laufen geregelt, mit festem Ansprechpartner.

Einführung und Begleitung
Technische Dokumentation, Einführung des Teams und persönliche Begleitung über die Einrichtung hinaus.

Wo unsere Rolle endet

Wir stellen die technische Infrastruktur und helfen dabei, digitale Arbeitsabläufe kontrollierbar und nachvollziehbar aufzubauen. Rechtliche Einzelfallprüfungen bleiben Aufgabe des Trägers und seiner Datenschutzberatung. Wir sind weder Datenschutzberatung noch externe Datenschutzbeauftragte — arbeiten aber gern mit den Personen zusammen, die diese Rolle bei Ihnen ausfüllen.

11 Kontakt und Quellen

Digitale Struktur unverbindlich besprechen

Ein Gespräch, in dem wir uns ansehen, womit Sie heute arbeiten und was sich mit vertretbarem Aufwand verbessern lässt. Ohne Verkaufsdruck und ohne Vorbereitung Ihrerseits.

SPIELRAUM.Digital
Ein Angebot der SPIELRAUM Jugendhilfe GmbH
24937 Flensburg
spielraum-digital.de · digital@spielraum-jh.de

spielraum-digital.de/kontakt

Verwendete Quellen

Ausschließlich Gesetzestexte sowie Veröffentlichungen von Aufsichtsbehörden und öffentlichen Stellen. Alle Quellen abgerufen am 31. Juli 2026.

EUR-LEX
Verordnung (EU) 2016/679 (DSGVO), konsolidierte deutsche Fassung
https://eur-lex.europa.eu/eli/reg/2016/679/oj/deu

BUNDESMINISTERIUM DER JUSTIZ
§ 61 SGB VIII — Anwendungsbereich
https://www.gesetze-im-internet.de/sgb_8/__61.html

BUNDESMINISTERIUM DER JUSTIZ
§ 62 SGB VIII — Datenerhebung
https://www.gesetze-im-internet.de/sgb_8/__62.html

BUNDESMINISTERIUM DER JUSTIZ
§ 64 SGB VIII — Datenübermittlung und -nutzung
https://www.gesetze-im-internet.de/sgb_8/__64.html

BUNDESMINISTERIUM DER JUSTIZ
§ 65 SGB VIII — Besonderer Vertrauensschutz
https://www.gesetze-im-internet.de/sgb_8/__65.html

BUNDESMINISTERIUM DER JUSTIZ
§ 42 BDSG — Strafvorschriften
https://www.gesetze-im-internet.de/bdsg_2018/__42.html

BUNDESMINISTERIUM DER JUSTIZ
§ 203 StGB — Verletzung von Privatgeheimnissen
https://www.gesetze-im-internet.de/stgb/__203.html

DATENSCHUTZKONFERENZ
Standard-Datenschutzmodell (SDM), Version 3.1
https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V31.pdf

DATENSCHUTZKONFERENZ
Kurzpapier Nr. 14 — Beschäftigtendatenschutz
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_14.pdf

DATENSCHUTZKONFERENZ
Kurzpapier Nr. 17 — Besondere Kategorien personenbezogener Daten
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_17.pdf

EUROPÄISCHER DATENSCHUTZAUSSCHUSS
Leitlinien 9/2022 zur Meldung von Datenschutzverletzungen
https://www.edpb.europa.eu/documents/guideline/guidelines-92022-on-personal-data-breach-notification-under-gdpr_de

LFDI RHEINLAND-PFALZ
Themenseite WhatsApp — dienstlicher Einsatz und private Endgeräte
https://www.datenschutz.rlp.de/themen/whatsapp

HESSISCHER BEAUFTRAGTER FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT
Handreichung zum datenschutzkonformen mobilen Arbeiten (2023)
https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2024-01/handreichung_zum_mobilen_arbeiten_231221.pdf

BAYERISCHER LANDESBEAUFTRAGTER FÜR DEN DATENSCHUTZ
Der Sozialdatenschutz unter der Datenschutz-Grundverordnung
https://www.datenschutz-bayern.de/datenschutzreform2018/SGB.pdf

BAYERISCHES LANDESJUGENDAMT (ZBFS)
Schutz der personenbezogenen Daten
https://www.blja.bayern.de/steuerung-planung-organisation/schutz-personenbezogene-daten/

BFDI
Informationen zu Meldungen von Datenschutzverstößen
https://www.bfdi.bund.de/DE/Service/Kontakt/Meldung-Datenschutzversto%C3%9F/Info_MeldungDSVerstoss.html