

(EU-)DSGVO: Was ist neu im Datenschutz?

Ein Überblick für Fachkräfte der Kinder- und Jugendhilfe

DSGVO-Ausnahmen

Die DSGVO gilt nicht:

für „**Privates**“ – für natürliche Personen, die personenbezogene Daten zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten verarbeiten – beispielsweise privater Schriftverkehr, Adressbücher oder die Nutzung Sozialer Netzwerke und Online-Tätigkeiten im Rahmen persönlicher oder familiärer Zwecke;

bei der **nicht automatisierten Verarbeitung** personenbezogener Daten, die nicht in einem Dateisystem gespeichert sind oder gespeichert werden sollen – bspw. Akten und Aktensammlungen, die nicht nach bestimmten Kriterien geordnet sind;

für die die **nationale Sicherheit** betreffende Tätigkeiten;

für die Datenverarbeitung zum Zwecke der **Strafverfolgung und Gefahrenabwehr** durch die zuständigen Behörden; hier gilt die zeitgleich mit der Datenschutz-Grundverordnung verabschiedete Richtlinie (EU) 2016/680.

Die Bedeutung des Datenschutzes nimmt zu und macht auch vor den in der Kinder- und Jugendhilfe tätigen Akteur/-innen nicht halt.

Seit dem 25.5.2018, nach zweijähriger Übergangsfrist, gilt nun in allen EU-Mitgliedsländern die neue Datenschutz-Grundverordnung (DSGVO). Sie soll die Gesetze zum Datenschutz in Europa harmonisieren und ein einheitliches Datenschutzniveau innerhalb der EU gewährleisten. Die DSGVO löst die europäische Datenschutz-Richtlinie von 1995 und das Bundesdatenschutzgesetz (BDSG) ab. Sie ist eine Reaktion auf die gestiegenen Schutzbedürfnisse der Verbraucher in Zeiten der Digitalisierung.

Die DSGVO soll daher vor allem die Rechte der Verbraucher/-innen stärken und ihnen mehr Transparenz, Information und Schutz ihrer personenbezogenen Daten bieten. Sie führt die bisherigen Grundsätze der Datenverarbeitung, etwa die Zweckbindung, Erforderlichkeit und Datensparsamkeit, unverändert fort, und bringt einige Neuerungen mit sich.

Für wen gilt die DSGVO?

Eigentlich für alle. Die Datenschutz-Grundverordnung gilt mit wenigen Ausnahmen für jede/n, die/er personenbezogene Daten verarbeitet. Dazu gehören zum Beispiel Behörden und Schulen, aber auch Einrichtungen der Kinder- und Jugendhilfe, Vereine, Online-Shops und Anbieter von Social Media-Diensten.

Was sind personenbezogene Daten?

Personenbezogene Daten sind solche, die einer Person bestimmbar zugeordnet werden können. Dazu gehören der Name, die Adresse und das Geburtsdatum, zudem das Geschlecht, die Religionszugehörigkeit und Informationen über die körperliche und geistige Gesundheit. Die DSGVO schließt erstmalig auch genetische und biometrische Daten ein.

Wann ist eine Verarbeitung rechtmäßig?

Wie bisher bedarf jegliche Verarbeitung personenbezogener Daten einer legitimierenden Rechtsgrundlage. Eine Verarbeitung personenbezogener Daten ist nur rechtmäßig

- mit der Einwilligung der betroffenen Person oder
- wenn die Verarbeitung erforderlich ist

- für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen,
- zum Schutz lebenswichtiger Interessen der betroffenen (z. B. Kindeswohl) oder einer anderen natürlichen Person,
- zur Wahrung berechtigter Interessen der/s Verantwortlichen oder Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen,
- zur Erfüllung einer rechtlichen Verpflichtung der/s Verantwortlichen oder
- für die Wahrnehmung einer im öffentlichen Interesse liegenden oder in Ausübung hoheitlicher Gewalt erfolgenden Aufgabe der/s Verantwortlichen (sog. Öffnungsklausel für die nationalen Gesetzgeber – vgl. Regelungen zum Sozialdatenschutz SGB X).

Neu ist der ausdifferenzierte Zweckbindungsgrundsatz, welcher Kriterien für eine zulässige weitere Verarbeitung von Daten benennt. Sind der ursprüngliche Zweck der Erhebung und der Zweck der Weiterverarbeitung durch die gleiche verantwortliche Stelle kompatibel, dürfen die Daten auf Basis der ursprünglichen Rechtsgrundlage weiterverarbeitet werden.

Ab welchem Alter können Kinder- und Jugendliche wirksam Einwilligungen erteilen?

In Art. 8 Abs. 1 DSGVO ist nun verbindlich festgelegt worden, dass Kinder und Jugendliche bei Angeboten von Diensten der Informationsgesellschaft (WhatsApp, Instagram, etc.) selbst erst ab 16 Jahren wirksam eine Einwilligung zur Verwendung ihrer personenbezogenen Daten erteilen können. Bei Unter-16-Jährigen müssen grundsätzlich die Eltern ihr Einverständnis zur Datenerhebung und -verarbeitung geben. Denn Kinder können meist nicht die Folgen und Risiken einer Datenverarbeitung abschätzen, die bspw. zu Werbezwecken erfolgt oder um Nutzerprofile zu erstellen und bedürfen daher eines besonderen Schutzes.

Unternehmen wie WhatsApp sollen sich mit „angemessenen Anstrengungen unter Berücksichtigung der verfügbaren Technik“ vergewissern, dass wirklich die Eltern oder andere Erziehungsberechtigte ihre Einwilligung gegeben haben. Genaue Umsetzungsvorgaben für Anbieter wie Instagram o. WhatsApp oder gibt es aber nicht.

!! Praxistipp!!

Aktualisierung der Einverständniserklärungen

Für die in der Kinder- und Jugendhilfe tätigen Akteur/-innen dürfte dies in der praktischen Arbeit insbesondere für die Nutzung von Kommunikationswegen mit Unter-16-Jährigen (z. B. via WhatsApp) relevant sein. Hierfür sollten nun Einverständniserklärungen vorliegen. Auch für die Verwendung von Daten und Bildern von Kindern und Jugendlichen unter 16 Jahren – etwa für die Vereinshomepage oder Email-Verkehr – wird nun eine Einwilligung der Erziehungsberechtigten benötigt.

Sind bisherige Einwilligungen gültig?

Laut [Länder-Beschluss der Aufsichtsbehörden](#) gelten bisher erteilte Einwilligungen fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, S. 3 DSGVO). Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen. Die (neuen) Informationspflichten nach Art. 13 DSGVO müssen dafür nicht erfüllt sein, da sie für bisherige Einwilligungen nicht vorausgesetzt wurden.

Einwilligungen, bei denen das Freiwilligkeitselement fehlt oder die von Kinder- und Jugendlichen unter 16 Jahren abgegeben worden sind, gelten hingegen nicht fort (→ Einholen der Einverständniserklärung der Eltern erforderlich).

Quelle: [bfdi.bund.de](https://www.bfdi.bund.de) – Dok. „Fortgeltung Bisher Erteilter Einwilligungen“

!! Praxistipp !!

Häufig ist unklar, ob die bisher genutzten Daten – z. B. Mail-Adressen für ein Newsletter-Mailing – in Gänze mit Einwilligung der Betroffenen verwendet werden. Deshalb ist es empfehlenswert, das Einverständnis der Betroffenen noch einmal explizit mit der konkreten Information, wofür die Daten verwendet werden, und dem Hinweis des Bestehens eines jederzeitigen Widerrufsrechts einzuholen. Dies ist seit Jahresbeginn auch der Grund für viele Mails, mit der Bitte um Zustimmung zur weiteren Verwendung der Mail-Adresse.

Wozu dienen die Transparenz- und Informationspflichten?

Verbraucher/-innen können nur dann auch tatsächlich überblicken, welche Konsequenzen ihre Dateneingabe bei einem Unternehmen hat, wenn sie genau wissen, wofür und in welchem Umfang die Daten eigentlich verwendet werden. Deshalb sind in der DSGVO dezidierte Transparenz- und Informati-

onspflichten für Datenverarbeitende nach Art. 13, 14 DSGVO installiert worden.

Die DSGVO weitet nicht nur den Umfang, sondern auch die Art (verständlich, keine Verklausulierungen) und den Anlass der Information aus.

Die betroffenen Personen sollten nicht nur aktiv bei der erstmaligen Erhebung, sondern grundsätzlich bei jeder beabsichtigten Weiterverarbeitung für andere Zwecke über die aufgeführten Aspekte unterrichtet werden. Die Informationen hat der/die Verantwortliche eigeninitiativ in verständlicher Form, d. h. ohne einen Antrag der betroffenen Person, zur Verfügung zu stellen. Das gilt insbesondere für Angebote, die sich speziell an Kinder und Jugendliche richten (Art. 12 Abs. 1 DSGVO).

Welche Rechte gelten für Betroffene?

Nutzer/-innen hatten schon nach der alten Gesetzeslage Auskunftsrechte: Sie konnten Unternehmen fragen, welche Daten über sie gespeichert sind, an wen sie weitergegeben werden und zu welchem Zweck.

Mit der DSGVO sind diese Rechte nun erweitert worden. Gestärkt wird das sogenannte „Recht auf Vergessenwerden“: Verbraucher/-innen können verlangen, dass ihre Daten gelöscht werden – sofern es keine rechtlichen Gründe gibt, sie weiter zu speichern. So sollen theoretisch „Online-Ausrutscher“ verschwinden.

Auch das Recht auf Datenmitnahme ist neu: Damit sollen Nutzer/-innen ihre gespeicherten Daten in einem technisch gängigen und kompatiblen Format von einem Dienstleister zum anderen mitnehmen können, zum Beispiel von E-Mail-Anbietern oder Musikstreaming-Diensten. Dies soll unter anderem den Wettbewerb fördern und den Anbieterwechsel vereinfachen.

Welche Pflichten haben die datenverarbeitenden Stellen?

Viele Verarbeitungspflichten sind konzeptionell mit der bisherigen Rechtslage vergleichbar, erfordern aber dennoch Anpassungen – z. B. **das Erstellen/Anpassen der Datenschutzerklärung für die eigene Homepage** – in der behördlichen und betrieblichen Praxis:

- Gewährleistung geeigneter technischer und organisatorischer Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit, Artikel 24, 25 und 32
- Anforderungen an die Auftragsverarbeitung,

Artikel 28

- Führen eines Verzeichnisses der Verarbeitungstätigkeiten, Artikel 30
- Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und Benachrichtigung der betroffenen Personen, Artikel 33, 34
- Durchführung einer Datenschutz-Folgenabschätzung, vorherige Konsultation der Aufsichtsbehörden, Artikel 35 und 36
- Benennung und Mitteilung eines Datenschutzbeauftragten, Artikel 37 bis 39
Hinweis: Ein(e) Datenschutzbeauftragte(r) ist wie bisher bei Vereinen und ehrenamtlichen Institutionen in der Regel nur dann zu bestellen, wenn „mindestens zehn Personen verwaltungsmäßig ständig mit der automatisierten Verarbeitung personenbezogener Daten“ beschäftigt sind (§ 38 Abs 1 S.1 BDSG 2018 neu).

Grauzone Facebook-Fanpages

Der EUGH hat am 5.6.2018 entschieden, dass Betreiber von Facebook-Fanpages und Facebook gemeinsame für den Datenschutz verantwortlich sind. Ein Verweis allein auf die Verantwortung von Facebook reiche nicht aus. Die Betreiber müssten selbst – etwa durch Vereinbarungen – gewährleisten, dass Facebook ihnen die notwendigen Informationen zur Erfüllung der datenschutzrechtlichen Anforderungen zur Verfügung stellt (entschieden nach alter Rechtslage vor DSGVO EuGH, Urte. v. 5.6.2018 – C-210/16). Das ist derzeit für niemanden umsetzbar, da Fanpage-Betreiber keinen Einfluss auf die Vorgänge nehmen, noch mit Facebook etwas aushandeln können.

Welche Handlungsmöglichkeiten bestehen?

- **Abschalten.**
Wer jedes rechtliche Risiko scheut, sollte die Fanpage deaktivieren.
- **Abwarten. Datenschutzerklärung und Impressum anpassen.** Urteil bezog sich auf die alten EU-Datenschutzrichtlinien – das Bundesverwaltungsgericht muss den Fall noch zu Ende führen und hat auch einen eigenen Beurteilungsspielraum.

Hinweise des LDI NRW zu dem Urteil:

https://www.lidi.nrw.de/mainmenu_Aktuelles/Inhalt/Facebook-Fanpage-Urteil-des-EuGH--Was-Fanpage-Betreiber-jetzt-tun-muessen/Facebook-Fanpage-Urteil-des-EuGH--Was-Fanpage-Betreiber-jetzt-tun-muessen.html

Wie sollen Vereine, kleinere Institutionen und ehrenamtliche Organisationen die DSGVO umsetzen?

Sie sollten die möglichen Risiken adäquat bewerten: Je sensibler die Daten sind, desto besser müssen sie geschützt werden. Je wahrscheinlicher oder schwerer das von der Datenverarbeitung ausgehende Risiko ist, desto umfangreicher und höher sind die Pflichten der/s Verantwortlichen.

Empfehlung des Bundesinnenministeriums

„Für die technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit gilt: Nicht jede Datenverarbeitung erfordert gleich hohe Sicherheitsstandards. Es ist ein dem Risiko angemessenes Schutzniveau unter Berücksichtigung der Implementierungskosten erforderlich.“

Im Rahmen der üblichen Vereins- oder ehrenamtlichen Tätigkeit dürften im Regelfall bereits Standardmaßnahmen, wie die Lagerung personenbezogener Daten in abschließbaren Vorrichtungen, aktuelle Betriebssysteme mit Passwortschutz, Zugriffsrechten und aktuellem Virenschutz, den Anforderungen genügen.“

www.bmi.bund.de/SharedDocs/faqs/DE/themen/it-digitalpolitik/datenschutz/datenschutzgrundvo-liste.html

Wer kontrolliert die Einhaltung der Datenschutz-Grundverordnung?

Zuständig für die Kontrolle sind die Datenschutzbehörden der Länder sowie die Bundesdatenschutzbeauftragte Andrea Voßhoff. In Nordrhein-Westfalen ist der Landesbeauftragte für Datenschutz und Informationsfreiheit NRW die zuständige Aufsichtsbehörde (www.ldi.nrw.de).

Was ist mit Rechtsverstößen?

Nutzer/-innen können sich bei Nichteinhaltung der DSGVO im ersten Schritt direkt an das jeweilige Unternehmen wenden. Hilft dieses nicht weiter, unterstützen Verbraucherzentralen und Datenschutzbehörden.

Erlangt eine Aufsichtsbehörde durch eine Beschwerde oder eine anlasslose Kontrolle Kenntnis von einem Verstoß gegen die Datenschutz-Grundverordnung oder eine nationale Datenschutzvorschrift, kann sie die/den Verantwortliche/n verwarnen oder Anweisungen, Anordnungen oder Verarbeitungsverbote aussprechen (Artikel 58 Absatz 2 Datenschutz-Grundverordnung).

Es bestehen aber keine gesetzlichen Meldepflichten, die anordnen, dass quasi „jedermann“ etwaige Verstöße gegen die DSGVO melden muss.

Zusätzlich oder anstelle der Abhilfebefugnisse kann die Aufsichtsbehörde nach Artikel 83 DSGVO Geldbußen von bis zu 20 Millionen EUR oder 4 Prozent des weltweiten Jahresumsatzes verhängen. Dem Gebot der Wirksamkeit, aber auch der Verhältnismäßigkeit, ist hierbei in jedem Einzelfall Rechnung zu tragen.

Was heißt das für Akteure der Kinder- und Jugendhilfe?

Dies bedeutet, dass die in der Kinder- und Jugendhilfe tätigen Akteur/-innen nicht in Panik verfallen müssen. Die hohen Summen sollen finanzkräftige, kommerzielle Unternehmen abschrecken und sie zur Einhaltung der DSGVO bewegen und nicht nicht-kommerzielle Akteur/-innen verunsichern, die keine unlauteren Absichten haben. Dies verdeutlicht insbesondere der Erwägungsgrund 38 der DSGVO.

Erwägungsgrund 38

Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind....

Die Einwilligung des Trägers der elterlichen Verantwortung sollte im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein.

Link-Tipps

Bei allen Unsicherheiten in Umsetzungsfragen der DSGVO steht das LDI NRW als Ansprechpartner zur Verfügung. Gute praxisgerechte Umsetzungstipps finden sich auch hier:

- ✓ [Erste Hilfe Koffer für den 25.05.2018 vom Landessportbund NRW](http://www.vibss.de/vereinsmanagement/recht/datenschutz/)
- ✓ www.vibss.de/vereinsmanagement/recht/datenschutz/
- ✓ www.ldi.nrw.de
- ✓ [Handreichung des Bayerischen Landesamtes für Datenschutzaufsicht](http://www.la.bayern.de/de/kleinunternehmen.html)
- ✓ www.la.bayern.de/de/kleinunternehmen.html
- ✓ www.bfdi.bund.de