Elternbrief zu Fotos, Videos und Audio bei Schulveranstaltungen

Liebe Eltern, liebe Sorgeberechtigte,

im Folgenden finden Sie die ausführlichere Version mit den Hintergründen zu unseren Regeln rund um Fotos, Videos und Audio bei Schulveranstaltungen.

Gerade bei Aufführungen (z. B. in der Projektwoche) entstehen sehr schnell Gruppenaufnahmen, auf denen viele Kinder klar erkennbar sind. Damit steigt das Risiko von Verletzungen der Privatsphäre. Besonders kritisch ist professionelles Material (hohe Auflösung, Nahaufnahmen, gute Tonqualität): Es macht Kinder häufig eindeutig identifizierbar und erhöht das Risiko, dass Aufnahmen später von Unternehmen oder Behörden verknüpft oder sogar biometrisch ausgewertet werden können. Biometrische Merkmale sind Erkennungsmerkmale, die einer Person eindeutig zugeordnet werden können.

Hinzu kommt ein praktischer Effekt: Viele an Veranstaltungen beteiligte Personen bedeuten oft auch viele Geräte, viele Fotos und Videos. Damit wächst automatisch die Zahl von Speichern, Kopieren, Weiterleiten und möglichen Freigaben an Apps und Dienste – und es wird immer schwieriger nachzuvollziehen, wo Medien am Ende liegen und welche Personen und Unternehmen Zugriff haben.

Warum sind biometrische Daten bei Kindern besonders sensibel?

Aus Fotos, Videos und Audioaufnahmen können biometrische Daten entstehen, etwa:

- Gesicht (Gesichtserkennung, Gesichtsmerkmale)
- Stimme (Stimmerkennung, Stimmprofil)

Biometrische Daten gelten als besonders sensibel, weil sie eine Person (und damit auch Kinder) über Situationen hinweg wiedererkennbar machen können.

Konkrete Risiken, wenn Bilder/Audio weitergegeben werden

- **Wiedererkennung & Überwachung**: Kinder können über Gesicht oder Stimme in anderen Medien wiedererkannt und über Zeit „getrackt“ und überwacht werden.
- **Profilbildung & Verknüpfung**: Biometrische Merkmale können mit Informationen wie Name, Schule, Hobbys, Kontakten oder Standortdaten verbunden werden – daraus können detaillierte Profile von Personen in den Händen von Unternehmen entstehen, die z.B. für Werbung verwendet werden.
- **Missbrauch (Deepfakes/Imitation):** Aus Bild- oder Audiomaterial lassen sich in kurzer Zeit täuschend echte Fälschungen (Deepfakes) oder Stimm-Imitationen erzeugen, die für Mobbing, sexualisierte Gewalt, Täuschung oder Betrug missbraucht werden können.

Weitergabe an private Firmen (Apps, Cloud-Dienste, soziale Netzwerke)

Sobald Fotos, Videos oder Audios geteilt oder in Apps/Clouds hochgeladen werden (z. B. Messenger, soziale Netzwerke, Foto-Clouds, KI-Funktionen, Backup-Dienste), werden sie oft an private Unternehmen übermittelt und dort verarbeitet – teils auch außerhalb des EU-Rechtsraums.

Wichtige Punkte dabei:

- **Nutzungsbedingungen/Verträge: Den Vertrag mit der App/Plattform schließen Sie mit dem anbietenden Unternehmen ab – nicht die anderen Familien**. Sind andere Kinder erkennbar, werden deren Daten in ein System gegeben, dessen Geschäftsbedingungen diese Familien nicht akzeptiert haben (oder bewusst ablehnen).

- **Kontrollverlust**: In Apps/Clouds ist oft schwer nachzuvollziehen, wo Medien gespeichert sind, wer Zugriff erhält und wie lange Daten vorgehalten werden (z. B. automatische Backups, Synchronisation, Weiterleitungen).
- **Biometrische Informationen**: Geräte- und Plattformanbieter können aus Fotos/Audios Gesichts- oder Stimmmerkmale ableiten. Das erhöht das Risiko späterer Wiedererkennung, Überwachung oder Verknüpfung.

Was sagen gesetzliche Vorgaben und Rechte?

Die Regeln orientieren sich an grundlegenden Rechten und Gesetzen, u. a.:

- **Grundgesetz** (Art. 1 Abs. 1; Art. 2 Abs. 1 GG): Menschenwürde und freie Entfaltung der Persönlichkeit, inklusive informationeller Selbstbestimmung.
- **UN-Kinderrechtskonvention** (Art. 16): Recht des Kindes auf Privatsphäre und Schutz vor rechtswidrigen Eingriffen.
- **Charta der UN-Menschenrechte** (Art. 12): Schutz vor willkürlichen Eingriffen in das Privatleben.
- **DSGVO** (u. a. Art. 4, Art. 9, Art. 4 Nr. 14): Das Weitergeben/Teilen von Bildern/Videos ist regelmäßig eine Datenverarbeitung; wenn Kinder erkennbar sind, braucht es besondere Sorgfalt. Biometrische Daten sind besonders sensibel; Kinder gelten als besonders schutzbedürftige Gruppe.
- **Recht am eigenen Bild** (§ 22 KunstUrhG): Erkennbare Bilder dürfen grundsätzlich nur mit Einwilligung verbreitet oder öffentlich gezeigt werden; bei Kindern entscheiden die Sorgeberechtigten.

Warum ist das in der Praxis so schwer?

Wir wissen: Die digitale Welt ist komplex. Viele Smartphones und Apps …

- speichern Medien automatisch oder standardmäßig in **Clouds/Backups**,
- verlangen weitreichende **Berechtigungen** auf die Mediathek,
- **analysieren** Medien (z. B. nach **Gesichtern/Stimmen**),
- verarbeiten **Metadaten** wie Ort, Zeit, soziale Kontakte,
- und es ist oft **nicht transparent**, was im Hintergrund passiert oder was die langen **Geschäfts- und Nutzungsbedingungen** konkret bedeuten.

Genau deshalb braucht es als Schulgemeinschaft klare, einfache Regeln, an die sich alle halten können.

Weiteres Basis-Wissen und Hilfestellungen finden Sie beim Bundesbeauftragten für Datenschutz und Informationsfreiheit:
https://www.bfdi.bund.de/DE/Buerger/Basiswissen/KinderundJugendliche/KinderundJugendliche-node.html

Vielen Dank, dass Sie mithelfen, die Privatsphäre und das Recht auf informationelle Selbstbestimmung aller Kinder und Familien zu schützen.

Mit freundlichen Grüßen