Datenschutz für die digitale Schülerverwaltung

Univ.-Prof. (SFU) Dr. Konrad Lachmayer

Dr. Thomas Menzel

Handreichung des Bundesministeriums für Bildung, Wissenschaft und Forschung

Stand: 7. Mai 2018

Inhaltsverzeichnis

Einleitung

I. Allgemeine datenschutzrechtliche Grundlagen für die Schülerverwaltung

Management Summary

1. Datenschutz als gesetzliche Rahmenbedingung der Schülerverwaltung
- A. Überblick
- B. Zentrale datenschutzrechtliche Begriffe
- C. Datenschutzrechtliche Prinzipien
- D. Datenschutzrechtliche Regeln
- E. Schulrechtliche Regeln zum Datenschutz

2. Datenschutz als Grundrecht
- A. Überblick
- B. Die Rechte von Schülerinnen und Schülern
- C. Die Schulleitung als Grundrechtsverpflichteter
- D. Der Rechtsschutz von Schülerinnen und Schülern

II. Besondere datenschutzrechtliche Fragestellungen in der Schülerverwaltung

Management Summary

1. Überblick
2. Neue digitale Schülerverwaltung
3. Schnittstellen zwischen Schulleitung und LSR / BMUKK
4. Schulwechsel
5. Elektronisches Klassenbuch
6. Edu.card
7. Weitere Fragestellungen
- A. Dienstleistungsvereinbarung
- B. Umgang mit Gesundheitsdaten/SV-Nr.
- C. Videoüberwachung
- D. Schutz des persönlichen Bildnisses
- E. Internet-Policy für Schulen

III. Anhang

1. **Glossar**
2. **Abkürzungsverzeichnis**
3. **Literaturverzeichnis**
4. **Vorlagen**
5. **Checkliste**
6. **Rechtstexte**

Einleitung

Mit der zunehmenden **Informationalisierung** des Alltags, dem Potenzial elektronischer Medien zur Vereinfachung von Verwaltungsabläufen und zur didaktischen Unterstützung des Unterrichts spielen Informationstechnologien in der Schule eine wichtige Rolle. Der Einsatz von IT & Internet bedeutet aber auch die zunehmende Verarbeitung von personenbezogenen Daten, vor allem von Schülerinnen und Schülern. **Die Verarbeitung dieser Daten unterliegt rechtlichen Regeln,** die im Schulbereich im Besonderen zu berücksichtigen sind, da Schülerinnen und Schüler als Minderjährige besonders schützenswert sind. Für die Schulleitung bzw. Administration ebenso wie für die IT-Beauftragten und generell für alle Lehrerinnen und Lehrer stellen sich zahlreiche, immer komplexer werdende Fragen der Verarbeitung personenbezogener Daten in der Schule.

Diesem Bedarf nach Antworten bzw. Richtlinien **für datenschutzkonforme Verarbeitung personenbezogener Daten in der Schülerverwaltung** möchte diese Handreichung nachkommen. Ziel ist die Aufarbeitung zentraler datenschutzrechtlicher Fragestellungen für die Schülerverwaltung. Es sollen rechtswissenschaftliche Grundlagen des Datenschutzes praxisrelevant präsentiert werden, um der Schülerverwaltung das notwendige Basiswissen für den Schulalltag zur Verfügung zu stellen. Die vorliegende Handreichung versteht sich als erste Grundlage, die aufgrund technischer und rechtlicher Entwicklungen sowie praktischer Erfahrungen weiter vertieft werden kann.

Die neue Regelung des Datenschutzes auf europäischer Ebene durch die **Datenschutz-Grundverordnung (DSGVO)**[1] sowie die damit verbundene Anpassung des Datenschutzgesetzes auf nationaler Ebene schaffen neue rechtliche Rahmenbedingungen für den Datenschutz in Europa, der mit 25. Mai 2018 in Kraft tritt. Die vorliegende Handreichung bezieht sich auf diese Rechtsgrundlagen.

[1]

Die vorgelegte Unterlage ist in **drei** große **Teile** untergliedert:

Im ersten Teil „**Allgemeine datenschutzrechtliche Grundlagen für die Schülerverwaltung**“ werden gesetzliche Rahmenbedingungen für die Schülerverwaltung sowie die notwendigen verfassungsrechtlichen Grundlagen (Grundrecht auf Datenschutz) dargestellt. Im Mittelpunkt stehen die datenschutzrechtlichen Begriffe, Prinzipien und Regeln in Hinblick auf ihre Relevanz für die Schülerverwaltung (etwa Schulleiterinnen und Schulleiter als datenschutzrechtliche Verantwortliche, Zweckbindung des Datenschutzrechts, besondere Kategorien von Daten, BilDokG etc).

Über diese allgemeinen Grundlagen hinaus werden im zweiten Teil **spezielle datenschutzrechtliche Fragestellungen** aus dem **schulischen Alltag** behandelt. Insbesondere wird auf die neue digitale Schülerverwaltung sowie datenschutzrechtliche Fragen des Schulwechsels, des elektronischen Klassenbuches, der Dienstleistungsvereinbarung, des Umgangs mit Gesundheitsdaten, der Videoüberwachung, des Schutzes des persönlichen Bildnisses sowie der Internet-Policy für Schulen eingegangen.

Im dritten Teil („**Anhang**“) werden in einem Glossar die wesentlichen (datenschutz)rechtlichen Begriffe zusammengefasst. Darüber hinaus befinden sich darin ein Abkürzungs- und Literaturverzeichnis sowie ausgewählte Vorlagen für den Gebrauch in der Schülerverwaltung. Überdies werden eine Checkliste für die Verarbeitung personenbezogener Daten sowie Auszüge aus Gesetzen und Verordnungen zur Verfügung gestellt.

Abschließend ist festzuhalten, dass **jede Art der Vervielfältigung oder Veröffentlichung für Bildungszwecke in Österreich unter Einhaltung der allgemeinen Zitierregeln ausdrücklich erwünscht ist.**

I. Allgemeine datenschutzrechtliche Grundlagen für die Schülerverwaltung

Management Summary

Datenschutz als gesetzliche Rahmenbedingung der Schülerverwaltung

- Die europäische Datenschutz-Grundverordnung (DSGVO) regelt die zentralen Begriffe und die wichtigsten Prinzipien des Datenschutzrechts sowie die Rechte des Betroffenen; es sieht Datensicherheitsmaßnahmen, Dokumentations- und Informationsvorschriften ebenso wie eine Datenschutz-Folgeabschätzung und die verpflichtende Einrichtung eines Datenschutzbeauftragten vor. Das österreichische Datenschutzgesetz (**DSG)** idf BGBl I 120/2017 regelt neben dem **Grundrecht auf Datenschutz** die Konkretisierung des Rechtsschutzes. Gem. § 3 BilDokG ist die **Schulleitung datenschutzrechtlich Verantwortlicher im Sinne des Datenschutzrechts.**

- Die **zentralen datenschutzrechtlichen Begriffe** sind „personenbezogene Daten“, „besondere Kategorien von Daten“, „Verantwortlicher“, „betroffene Person“, „Auftragsverarbeiter“ sowie die „Verarbeitung“ von Daten und die „Einwilligung“.

- Die wichtigsten datenschutzrechtlichen **Prinzipien** sind „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“, die „Zweckbindung“ und die „Datenminimierung“.

- Neben den Bestimmungen der DSGVO und des DSG sind vor allem das Bildungsdokumentationsgesetz (**BilDokG)** und das Schulunterrichtsgesetz (**SchUG)** als Grundlage für das Verwenden personenbezogener Daten relevant. Beide Gesetze schaffen konkrete gesetzliche Grundlagen, wie sie das DSG für das Verwenden personenbezogener Daten fordert.

- **Die Rechtmäßigkeit der Datenverarbeitung** liegt gem. Art. 6 DSGVO vor, wenn, wenn **eine ausdrückliche gesetzliche Ermächtigung besteht**, der **Betroffene** der Datenverarbeitung **zugestimmt** hat, oder **lebenswichtige Interessen des Betroffenen** die Verarbeitung erfordern oder die Verarbeitung für die Wahrnehmung einer Aufgabe im öffentlichen Interesse erforderlich ist.

- Auch wenn keine explizite gesetzliche Ermächtigung zur Verarbeitung personenbezogener Daten besteht, so dürfen diese **Daten** von der Schulleitung **verwendet werden**, **wenn** diese eine **wesentliche Voraussetzung für die Wahrnehmung einer** der Schulleitung **gesetzlich übertragenen Aufgabe** (etwa im Rahmen des SchUG) bilden.

- Die **Einwilligung** ist eine wichtige Möglichkeit der datenschutzrechtlich zulässigen Verarbeitung personenbezogener Daten. Dabei ist zu beachten, dass die Einwilligung von jedem/jeder einzelnen Schüler bzw. Schülerin einzuholen ist, dass die Einwilligung freiwillig erfolgt und wer die Einwilligung zu geben hat (Erziehungsberechtigte oder Schüler/Schülerin).

- Bestehen **lebenswichtige Interessen des Betroffenen** so dürfen die Daten der betroffenen Person verwendet werden. Damit sind primär **akute medizinische Notfälle** angesprochen.

- Die **Regeln des DSG** beziehen sich sonst etwa auf externe Informationpflichten (Art 12ff DSGVO), interne Dokumentationspflichten (Art 30 DSGVO), Maßnahmen zur Datensicherheit (Art 32 DSGVO), die Meldung von Datenmissbrauch (*Data Breach Notification*) im Sinne des Art 33f DSGVO, die Datenschutz-Folgeabschätzung (Art 35f DSGVO) sowie die verpflichtende Einrichtung eines Datenschutzbeauftragten (Art 37ff DSGVO).

Grundrecht auf Datenschutz

- Die **österreichische Verfassung** gewährt ebenso wie die europäische Grundrechtecharta Betroffenen ein **Grundrecht auf Datenschutz**. Dies bedeutet, dass die Verarbeitung personenbezogener Daten nur unter bestimmten Voraussetzungen möglich ist. Liegen die Voraussetzungen nicht vor, bedeutet dies eine Verletzung des Grundrechts auf Datenschutz.

- Die Verarbeitung personenbezogener Daten muss **verhältnismäßig** erfolgen. Dies bedeutet, dass die Datenverarbeitung zur Erfüllung der Aufgaben notwendig sein muss.

- Die Schulleitung ist verpflichtet, das Grundrecht auf Datenschutz zu gewährleisten. Die aus dem Grundrecht auf Datenschutz erfließenden Rechte der betroffenen Schülerinnen

und Schüler bzw. Lehrerinnen und Lehrer sind insbesondere das Recht auf **Auskunft** sowie die Rechte auf **Berichtigung** und **Löschung**.

- Die Betroffenen können ihre Rechte, wenn ihnen diese nicht durch die Schulleitung gewährt werden, mittels **Beschwerde** bei der unabhängigen **Datenschutzbehörde** geltend machen.

CHECKLISTE

Wenn in der Schülerverwaltung personenbezogene Daten verwendet werden sind folgende Fragen zu beantworten:

✓ Wer ist datenschutzrechtlich Verantwortlicher?

☐ Schulleitung ☐ BMBWF ☐ Anderer: _____

✓ Wer sind die betroffenen Personen?

☐ Schülerinnen und Schüler ☐ Lehrerinnen und Lehrer

☐ Erziehungsberechtigte ☐ Andere: _____

✓ Welche personenbezogenen Daten werden verwendet?

☐ Namen ☐ Adresse ☐ Bildnis

☐ Andere: _____

_____

_____

✓ Werden besonderen Kategorien personenbezogenen Daten verwendet?

☐ Nein ☐ Ja

Wenn ja, welche?

☐ ethnische/rassische Herkunft

☐ religiöse/philosophische Überzeugung

☐ Gesundheit/Sexualleben

☐ Andere (politische Meinung, Gewerkschaftszugehörigkeit)

✓ Zu welchem Zweck werden die personenbezogenen Daten verwendet?

☐ Aufnahme in die Schule ☐ Prüfung

☐ HU ☐ Widerspruch

☐ Schulveranstaltung ☐ Anderer: _____

✓ Wie werden die personenbezogenen Daten verwendet?

☐ Erfassen von neuen Daten ☐ Verändern

☐ Abfragen/Benützen ☐ Verknüpfen

☐ Löschen/Vernichten ☐ Speichern

☐ Anders: _____

✓ Werden die personenbezogenen Daten weitergegeben?

☐ Nein ☐ Ja

Wenn ja, an wen?

☐ Übermittlung an Dritte: _____

Wenn Dritte, auf welcher Grundlage?

_____

☐ Überlassung an Auftragsverarbeiter:

_____

Wenn Auftragsverarbeiter, wurde eine Dienstleistungsvereinbaung abgeschlossen?

☐ Ja ☐ Nein

✓ Ist die Verarbeitung erforderlich bzw. verhältnismäßig? Wieso ist die Verarbeitung das gelindeste Mittel?

☐ Begründung: _____

_____

✓ Auf welcher rechtlichen Grundlage werden die personenbezogenen Daten verwendet?

☐ Explizite gesetzliche Grundlage:

☐ BilDokG ☐ SchUG ☐ Andere

Konkrete Bestimmung nennen: _____

☐ Implizite gesetzliche Grundlage (, da Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt); welche gesetzlich vorgesehene Aufgabe?

☐ SchUG ☐ Andere

Konkrete Bestimmung nennen: _____

☐ Einwilligung:

Schriftliche Einwilligung der Betroffenen eingeholt? ☐ Ja ☐ Nein

☐ bis 14. Lbj. Erziehungsberechtigte

☐ ab Vollendung des 14. Lbj. Schülerinnen und Schüler

☐ Lebenswichtiges Interesse (Medizinischer Notfall)

☐ Andere rechtliche Grundlage: _____

1. Datenschutz als gesetzliche Rahmenbedingung der Schülerverwaltung

A. Überblick

Die **Datenschutz-Grundverordnung** setzt – abgesehen von den grundrechtlichen Rahmenbedingungen, die sich in § 1 DSG und Art 8 GRC finden – **zentrale Vorgaben** für das Verwenden personenbezogener Daten für die Schülerverwaltung. Ausgangspunkt sind die durch die DSGVO vorgesehenen Begriffe gem Art 4 DSGVO (siehe sogleich unter B.). Ausgehend von der datenschutzrechtlichen **Begrifflichkeit** sind die datenschutzrechtlichen **Prinzipien** die oberste Ebene des einfachgesetzlichen Datenschutzverständnisses (C.). Festgelegt werden die Prinzipien in konkreten datenschutzrechtlichen **Regelungen** (D.), die neben den allgemeinen Bestimmungen zur Datenverarbeitung etwa auch die Einwilligung, die Informationspflichten, die Dokumentationspflichten, die Datensicherheit, das Verfahren zur Datenschutz-Folgeabschätzung, die sog. Data Breach Notification oder die verpflichtende Einrichtung des Datenschutzbeauftragten betreffen.

Über die Bestimmungen der DSGVO und das DSG hinaus finden sich aber auch in den schulrechtlichen Regelungen Anknüpfungspunkte an das Datenschutzrecht (E.). Diesbezüglich sind vor allem das BilDokG und das SchUG zu nennen.

Die hier vorgenommene schulrechtliche Analyse des Datenschutzrechts muss im Kontext der **Entwicklungen auf europäischer Ebene** gesehen werden. Mit der **europäischen Datenschutz-Grundverordnung** hat die Union ein **neues Datenschutzrecht geschaffen**, das mit 25. Mai 2018 in Kraft trat. Das österreichische DSG ist damit nur noch in bestimmten spezifischen Fragen, wie etwa dem Verfahren vor der Datenschutzbehörde, den Datenschutzbeauftragten im öffentlichen Bereich oder der Bildaufnahmen von Relevanz.[2]
Die Inhalte der DSGVO sind dager auch im Schulrecht anzuwenden.

[2] Eine besondere Relevanz kommt der Festlegung des Mindestalters für eine datenschutzrechtliche Einwilligung gem § 4 Abs 4 DSG (Vollendung des 14. Lbj.); siehe dazu unter xxx.

B. Zentrale datenschutzrechtliche Begriffe

Art 4 DSGVO definiert die wichtigsten Begriffe des Datenschutzrechts. Die Begriffsbestimmungen sind zum Teil kompliziert ausgefallen. Dennoch ist es wichtig, die zentralen Bestimmungen zu kennen.

Ausgangspunkt ist der Begriff der personenbezogenen Daten:

- **Personenbezogene Daten** sind Informationen über **betroffene natürliche Personen**, die identifiziert oder identifizierbar sind; „identifizierbar" sind Daten, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Eine besondere Definition gibt es für besonders schutzwürdige Daten (bisher sog. „sensible Daten"), die als besonderer Kategorien personenbezogener Daten bezeichnet werden und an deren Verarbeitung Art 9 DSGVO höhere Anforderungen knüpft:

- **Besondere Kategorien von Daten** (früher als sensible Daten bezeichnet) sind personenbezogene Daten aus denen die **rassische und ethnische Herkunft**, **politische Meinungen**, **religiöse** oder weltanschauliche **Überzeugungen** hervorgehen, sowie die Verarbeitung von **genetischen Daten**, **biometrischen Daten** zur eindeutigen Identifizierung einer natürlichen Person, **Gesundheitsdaten** oder Daten zum **Sexualleben** oder der **sexuellen Orientierung**.

Die zwei zentralen **Rollen** im Datenschutz sind die **betroffene Person** und der datenschutzrechtlich **Verantwortliche:**

- **Betroffene Person** ist jede vom **Verantwortlichen** verschiedene natürliche Person, deren Daten verarbeitet werden (Schülerinnen und Schüler, Lehrerinnen und Lehrer).

- **Verantwortlicher** ist eine natürliche oder juristische **Person** oder eine **Behörde, Einrichtung oder andere Stelle**, die alleine oder gemeinsam mit anderen die **Entscheidung getroffen** haben, personenbezogene **Daten zu verwenden**

(**Schulleiter/Schulleiterin,** § 3 BilDokG), unabhängig davon, ob sie die Daten selbst verwenden oder damit einen Auftragsverarbeiter damit beauftragen.

An dieser Stelle kommt der sog. **Auftragsverarbeiter** als weitere Rolle ins Spiel. Es handelt sich um eine Person oder ein Unternehmen, das von der Schulleitung herangezogen wird, um Daten für diesen zu verarbeiten (z.B. externe Datenbanken, Wartung der EDV, Essensabrechnung, Herstellung von edu.cards oder sonstigen Schülerausweisen, Fotografen).

- **Auftragsverarbeiter** ist jede natürliche oder juristische Person, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (etwa Bundesrechenzentrum).

Neben den im Datenschutzrecht bestehenden Rollen werden auch die Handlungen definiert. **Überbegriff** ist das **Verarbeiten von Daten**. Darunter wird jeder mit oder ohne (!) Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten verstanden. Darunter fällt

- das **Erheben**,
- das Erfassen,
- die Organisation,
- das Ordnen,
- die **Speicherung**,
- die Anpassung oder Veränderung,
- das Auslesen,
- das Abfragen,
- die **Verwendung**,
- die Offenlegung durch Übermittlung,
- **Verbreitung** oder eine andere Form der Bereitstellung,
- den Abgleich oder die **Verknüpfung**,
- die Einschränkung,
- das **Löschen** oder die **Vernichtung**

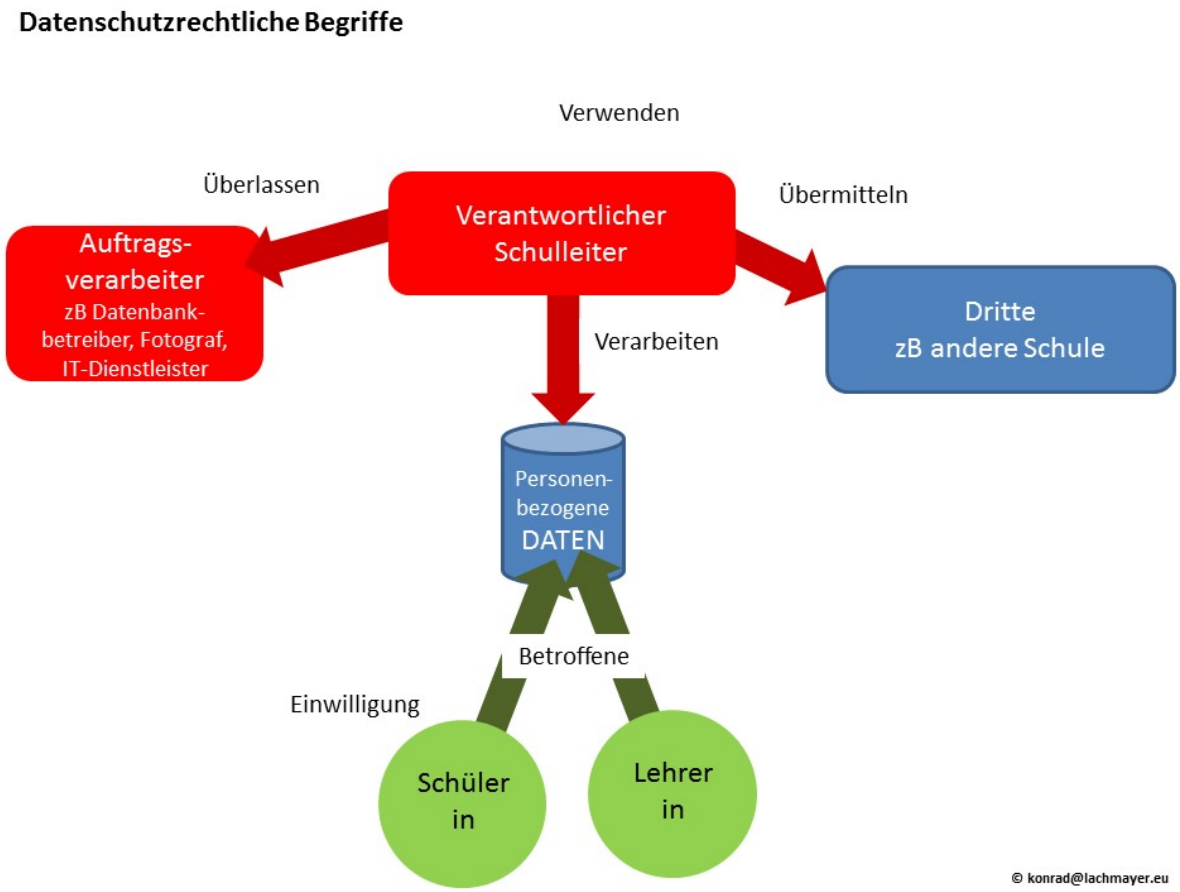
von personenbezogenen Daten.

Als zentraler Begriff des Datenschutzrechts wird schließlich auch die **Einwilligung** definiert:

- **Einwilligung** ist jede **freiwillig** für den bestimmten Fall, in **informierter** Weise und unmissverständlich abgegebene **Willensbekundung** in Form einer Erklärung oder einer sonstigen **eindeutigen bestätigenden Handlung**, mit der die betroffene Person zu

verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Abb. 1:



C. Datenschutzrechtliche Grundsätze

Die **wichtigsten** datenschutzrechtlichen **Grundsätze** sind:

- **Rechtmäßigkeit,** Verarbeitung nach Treu und Glauben**, Transparenz**
- **Zweckbindung**
- **Datenminimierung** und **Speicherbegrenzung („Verhältnismäßigkeit“)**
- Richtigkeit
- **Integrität und Vertraulichkeit**
- Rechenschaftspflicht

Ausgangspunkt ist immer die **Rechtmäßigkeit** der Datenverarbeitung (siehe dazu sogleich näher). Nur wenn ein legitimer Grund für eine Datenverarbeitung vorliegt (siehe Art. 6 DSGVO), darf diese erfolgen.

Treu und Glaube bezieht sich neben der allgemeinen Vorgabe, personenbezogene Daten nur rechtmäßig zu verwenden, vor allem darauf, dass der/die Betroffene, also die Schülerin bzw. der Schüler, in Hinblick auf die Datenverarbeitung oder aber das Bestehen und die Durchsetzbarkeit ihrer bzw. seiner Rechte, nicht irregeführt oder im Unklaren gelassen wird. Treu und Glaube wird durch die Umsetzung von Informations- und Dokumentationspflichten ebenso wie durch geeignete technische und organisatorische Maßnahmen erfüllt.

Die neue DSGVO betont auch die **Transparenz als wichtigen Grundsatz** des Datenschutzrechts. Die betroffenen Personen müssen in diesem Sinne etwa von den Verantwortlichen über die Verarbeitung und deren Zwecke informiert werden (Art 12 ff DSGVO).

Zweckbindung ist ein fundamentaler Grundsatz des Datenschutzrechts. Dieser besagt, dass personenbezogene Daten nur „für festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden“ dürfen (Art 5 Abs 1 Z 2 DSGVO). Es ist also unzulässig, die für einen Zweck verwendeten Daten für einen anderen Zweck zu verwenden, nur weil sie bereits gespeichert sind. Für den anderen Zweck muss die Voraussetzung für die Datenverarbeitung eigenständig vorliegen. Mit der Zweckbindung geht auch die Begrenzung des Datenumfangs, die Richtigkeit und Aktualität der Daten sowie die zeitliche Begrenzung in Hinblick auf die Zweckerfüllung einher.

- **Datenminimierung** und **Speicherbegrenzung („Verhältnismäßigkeit“)**

Das Datenschutzrecht basiert auf den **Grundsatz der Datenminimierung**. Personenbezogene Daten soll nur dann erhoben, verarbeitet oder weitergegeben werden, wenn dies für den **Zweck** der Datenverarbeitung **notwendig** ist, also das **gelindeste Mittel** darstellt. Die Datenminimierung bringt auch die **Speicherbegrenzung**, allerdings in zeitlicher Hinsicht zum Ausdruck. Daten dürfen nur **solange** gespeichert werden, wie dies für die Zwecke, für die sie verarbeitet werden, **erforderlich** ist.

Die Datenminimierung und die Speicherbegrenzung bringen die grundrechtliche **Verhältnismäßigkeitsprüfung** zum Ausdruck, die verlangt, dass die Datenverarbeitung für den damit verfolgten Zweck geeignet und erforderlich ist. Die **Eignung** bezieht sich darauf, dass die Datenverarbeitung zur Erreichung des Zwecks der Datenverarbeitung beitragen können muss.

Ist die Datenverarbeitung nicht geeignet, so ist sie auch nicht verhältnismäßig. Zentrales Kriterium ist die **Erforderlichkeit**. Ist die Datenverarbeitung tatsächlich notwendig, um den Zweck der Datenverarbeitung zu erreichen oder könnte dasselbe Ziel auch ohne die Verarbeitung personenbezogener Daten erreicht werden. Ist die Datenverarbeitung nicht erforderlich, so ist sie nicht verhältnismäßig. Das Prinzip der Verhältnismäßigkeit wird auch durch den Grundsatz der Datenminimierung zum Ausdruck gebracht. Dieser besagt, dass die Datenverarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss. Die Erforderlichkeit ist auch zeitlich zu interpretieren; dies bedeutet: wie lange ist die Datenverarbeitung erforderlich und ab wann ist sie nicht mehr erforderlich.

Schließlich hängt die Verhältnismäßigkeit von der **Abwägung** zwischen der Wichtigkeit des mit der Datenverarbeitung verfolgten Zwecks einerseits und der Intensität des Eingriffs in die Rechte der Betroffenen andererseits ab. So ist die Verarbeitung besonderer Kategorien von Daten (etwa Gesundheitsdaten) ein besonders starker Eingriff in die Rechte der Schülerinnen und Schüler. Einem solchen Eingriff muss ein besonders guter Grund gegenüber stehen.

Das **Prinzip der Richtigkeit** besagt, dass die personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein müssen; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Datenschutz bedeutet auch **Datensicherheit**. So müssen die personenbezogenen Daten in einer Weise verarbeitet werden, die eine angemessene **IT-Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (**Integrität und Vertraulichkeit**).

Als abschließendes Prinzip sieht die **Rechenschaftspflicht** vor, dass der Verantwortliche die Einhaltung all dieser Prinzipien nachweisen können muss. Kann er dies nicht, so ist er dafür auch verantwortlich.

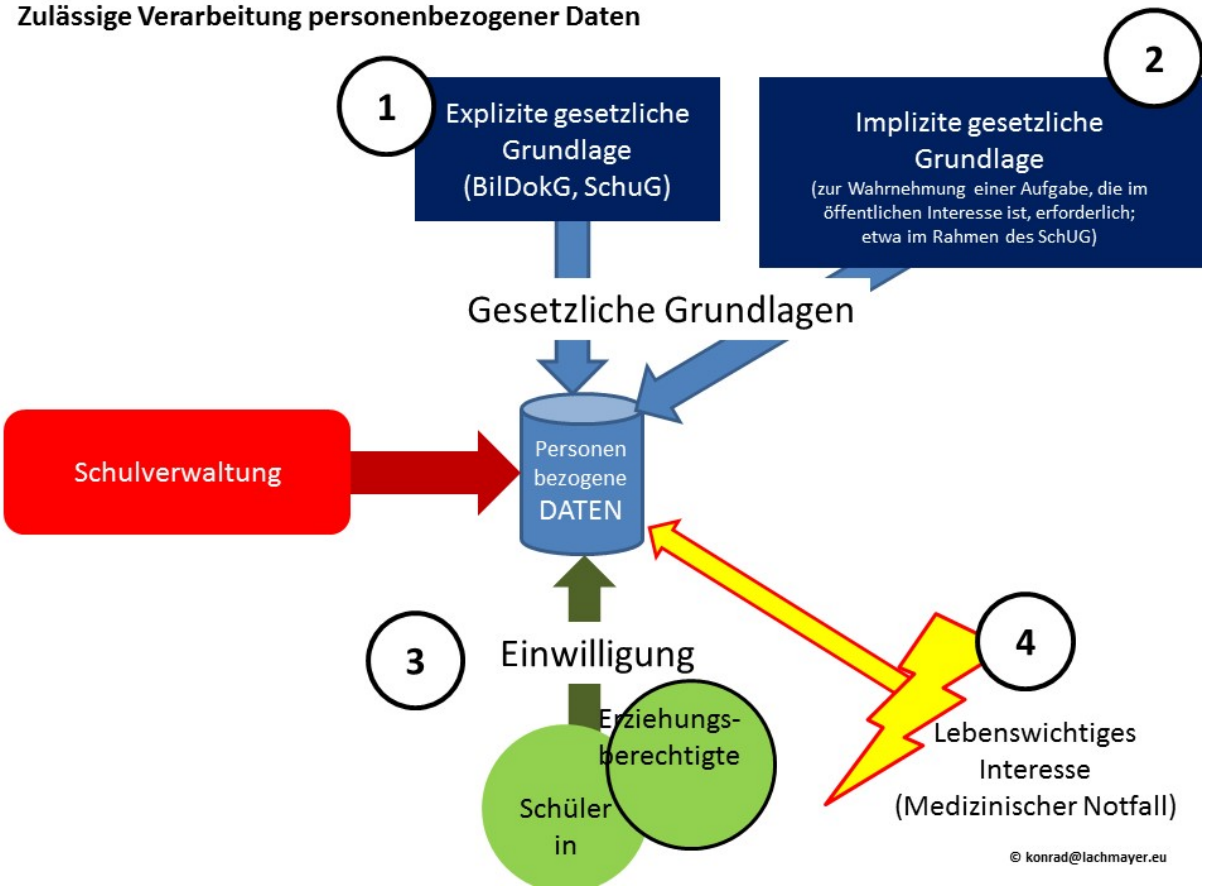
D. Datenschutzrechtliche Regeln

a. Die Rechtmäßigkeit der Datenverarbeitung

Die DSGVO stellt in Art. 6 unterschiedliche Möglichkeiten für die Rechtmäßigkeit der Datenverarbeitung zur Verfügung. (Reihung nach praktischer Bedeutung für die Schulverwaltung)

- Lit. e: die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- Lit. a: Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- Lit. b: die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- Lit. c: die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- Lit. d: die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

Abb. 2



Schutzwürdige Geheimhaltungsinteressen bei **Verarbeitung nicht-sensibler Daten** werden nicht verletzt, wenn

- eine **ausdrückliche gesetzliche Ermächtigung** zur Verarbeitung der Daten besteht oder
- die Verarbeitung zur Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.
- der **Betroffene** der Verarbeitung seiner Daten **zugestimmt** hat, wobei ein **Widerruf jederzeit möglich** ist und die Unzulässigkeit der weiteren Verarbeitung der Daten bewirkt, oder
- **lebenswichtige Interessen** des **Betroffenen** die Verarbeitung erfordern (akuter medizinische Notfall) oder
- **überwiegende berechtigte Interessen des Verantwortlichen** (also des Schulleiters / der Schulleiterin) die Verarbeitung erfordern.

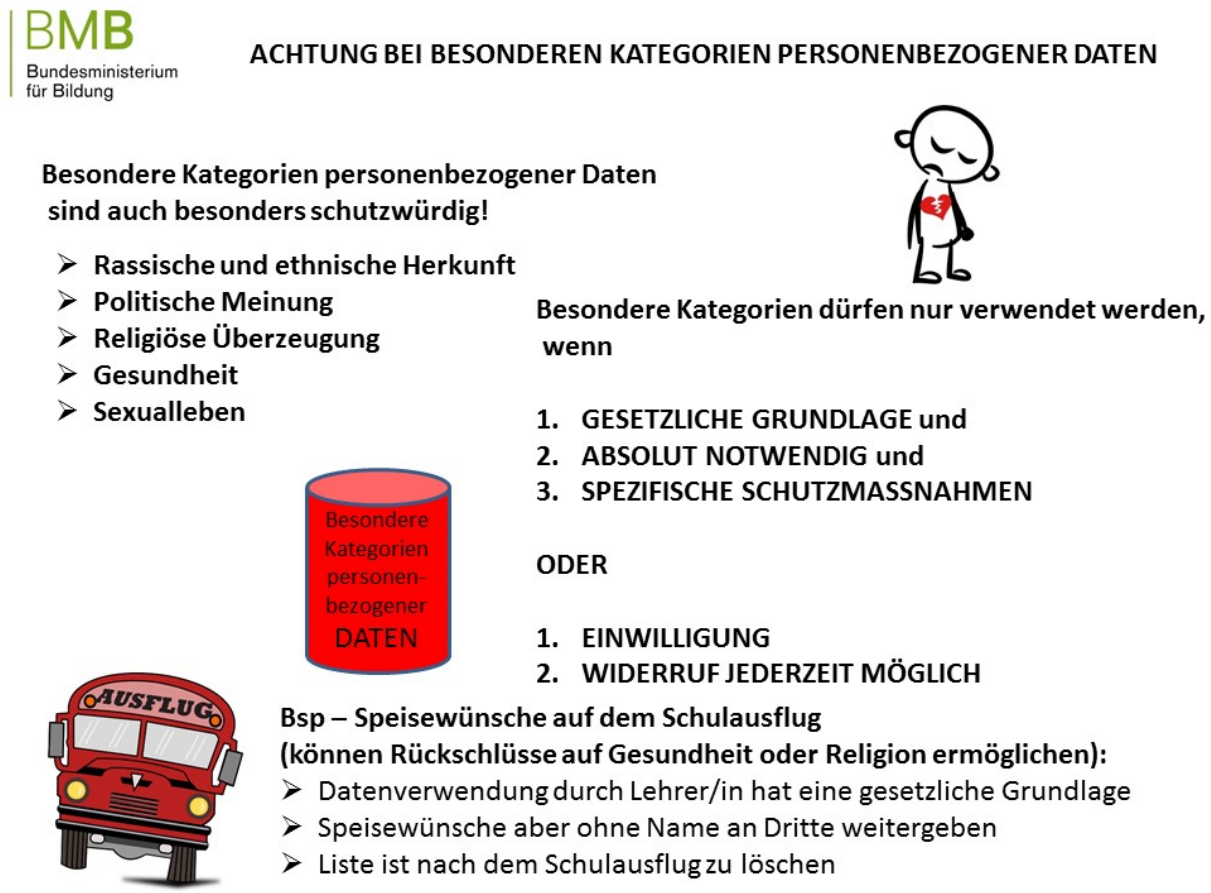
Überwiegende berechtigte Interessen der Schulleitung liegen im Sinne des § 8 Abs 3 DSG vor, wenn die Datenverarbeitung für die Schulleitung **eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe** ist.

FRAGE: Wann ist die Datenverarbeitung eine „wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe“?

Dies bedeutet, dass etwa das **SchUG** herangezogen werden kann, um zu argumentieren, inwieweit eine Datenverarbeitung im Rahmen der Schülerverwaltung erfolgen muss. Das **Verhältnismäßigkeitsprinzip** (Eignung, Erforderlichkeit, Abwägung) ist diesbezüglich von großer Bedeutung.

Besondere Bedeutung kommt dabei den Bestimmungen gem §§ 56 iVm 77 und 77a SchUG zu. § 56 SchUG normiert, dass normiert, dass der Schulleiter bzw. die Schulleiterin zur Besorgung aller Angelegenheiten des SchuG zuständig ist, sofern das SchuG nichts anderes vorsieht. Gem § 56 Abs 4 SchuG hat der Schulleiter bzw. die Schulleiterin für die Führung der Amtsschriften zu sorgen. §§ 77 und 77a SchuG sieht als solche Amtsschriften insbesondere Schülerstammblätter, Gesundheitsblätter, Klassenbücher und Prüfungsprotokolle vor. Die Datenverwendug in der Schülerverwaltung ist regelmäßig eine wesentliche Voraussetzung der Führung der Amtsschriften, die eine der Schulleitung gesetzlich übertragene Aufgabe darstellt.

Abb. 3:



Bei **besonderen Kategorien von Daten** (politische Meinung, Religion, Gesundheit) sind die Vorgaben zur Rechtmäßgkeit der Verarbeitung zwar ähnlich den allgemeinen Vorgaben in Art 6 DSGVO, im Detail aber **noch strenger**. Diese dürfen nur verwendet werden, wenn:

- der Betroffene die Daten offenkundig selbst öffentlich gemacht hat oder
- die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich, oder
- sich die **Ermächtigung oder Verpflichtung zur Verarbeitung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen,** oder

- der **Betroffene** seine **Einwilligung** zur Verarbeitung der Daten **ausdrücklich erteilt** hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verarbeitung der Daten bewirkt, oder
- die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,
- die Verarbeitung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist.

c. Die Einwilligung

Die **Einwilligung** ist auch aus Sicht der Schülerverwaltung ein **unverzichtbarer Teil** des Umgangs mit Datenschutz. Besteht **keine gesetzliche Grundlage** (DSGVO, SchUG, BilDokG), so können die personenbezogenen Daten nur mit Einwilligung verwendet werden. Mit Einwilligung ist auch die Verarbeitung besonderer Kategorien von Daten möglich.

ACHTUNG: In Hinblick auf die Einwilligung sind allerdings wichtige Aspekte zu beachten:

1. Es bedarf einer **Einwilligung jedes einzelnen** Schülers bzw. jeder einzelnen Schülerin. Eine Einwilligung etwa des SGA reicht nicht! Stimmt eine Schülerin bzw. ein Schüler nicht zu, so dürfen diese personenbezogenen Daten auch nicht verwendet werden, sondern nur die Daten jener Schülerinnen und Schüler, die zugestimmt haben. Einwilligung kann daher nur für Systeme verwendet werden, bei denen nicht zwingend alle Schülerinnen und Schüler erfasst werden.

2. Die **Einwilligung** muss in **verständlicher und leicht zugänglicher Form** in einer klaren und einfachen Sprache **erfolgen**. Die datenschutzrechtliche Einwilligung muss von anderen Zustimmungserklärungen getrennt erfolgen. Eine **Einwilligung** muss solange die Daten verarbeitet oder gespeichert werden **nachgewiesen werden können**.

3. Die **Einwilligung** kann **jederzeit ohne Angabe von Gründen widerrufen** werden. Die Schulleitung muss überdies auf die Möglichkeit des Widerrufs hinweisen. Im Falle des Widerrufs müssen die personenbezogenen Daten gelöscht werden. Ohne Einwilligung fehlt es sodann an der Zulässigkeit der Datenverarbeitung. Eine Weiterverarbeitung ist nicht mehr möglich. Bei der Einwilligung ist also zu beachten, dass selbst wenn anfänglich etwa alle Schülerinnen und Schüler einer Klasse eine Einwilligung zur Verarbeitung der Daten geben, durch Widerruf die Einwilligung aller wieder verloren gehen kann

4. Die Einwilligung muss **freiwillig** und für den **konkreten Fall** erfolgen. Da die Schulleitung hoheitlich tätig wird, ja zum Teil sogar mit Schulpflicht verbunden ist, ist die von der DSGVO geforderte Freiwilligkeit der betroffenen Schülerinnen und Schüler entscheidend. Es darf kein Druck bezüglich Abgabe oder Nichtabgabe der Einwilligung ausgeübt werden. Überdies kann eine Einwilligung nicht pauschal erfolgen, also etwa für alle in der Schule vorgesehenen Datenverarbeitungen. Es muss eine Einwilligung in Kenntnis der Sachlage für den konkreten Fall der Datenverarbeitung sein. Der Zweck und die Form der Datenverarbeitung muss daher auch offengelegt werden.

Zusammenfassend ist daher festzuhalten, dass eine **Einwilligungslösung oft nicht optimal** ist, vor allem dann, wenn möglichst alle Schülerinnen und Schüler beteiligt werden sollen. Die Einwilligung jedes einzelnen Schülers zu erhalten, stellt schon einen beachtlichen Aufwand dar. Dabei ist es ganz wichtig, dass die Freiwilligkeit der Einwilligung gewahrt wird und keinesfalls Druck auf den Schüler/die Schülerin bzw. die Erziehungsberechtigten ausgeübt wird. Schließlich sind die Betroffenen auf die Möglichkeit eines Widerrufs hinzuweisen, der die gegebenen Einwilligungen rasch wieder reduzieren kann. Umgekehrt ist zu betonen, dass bei fehlender gesetzlicher Grundlage bzw. wenn nicht argumentiert werden kann, dass es sich bei dieser Datenverarbeitung um eine notwendige Voraussetzung für die Wahrnehmung einer der Schulleitung gesetzlich übertragenen Aufgabe handelt, die Schulleitung auf das Einwilligungsmodell angewiesen ist.

FRAGE: Wer erteilt die datenschutzrechtliche Einwilligung? Die Erziehungsberechtigten oder die Schülerinnen und Schüler?

§ 4 Abs 4 DSG legt fest, dass ein Kind mit Vollendung des vierzehnten Lebensjahres rechtmäßig eine Einwilligung in die Verarbeitung der eigenen personenbezogenen Daten geben kann.[3]

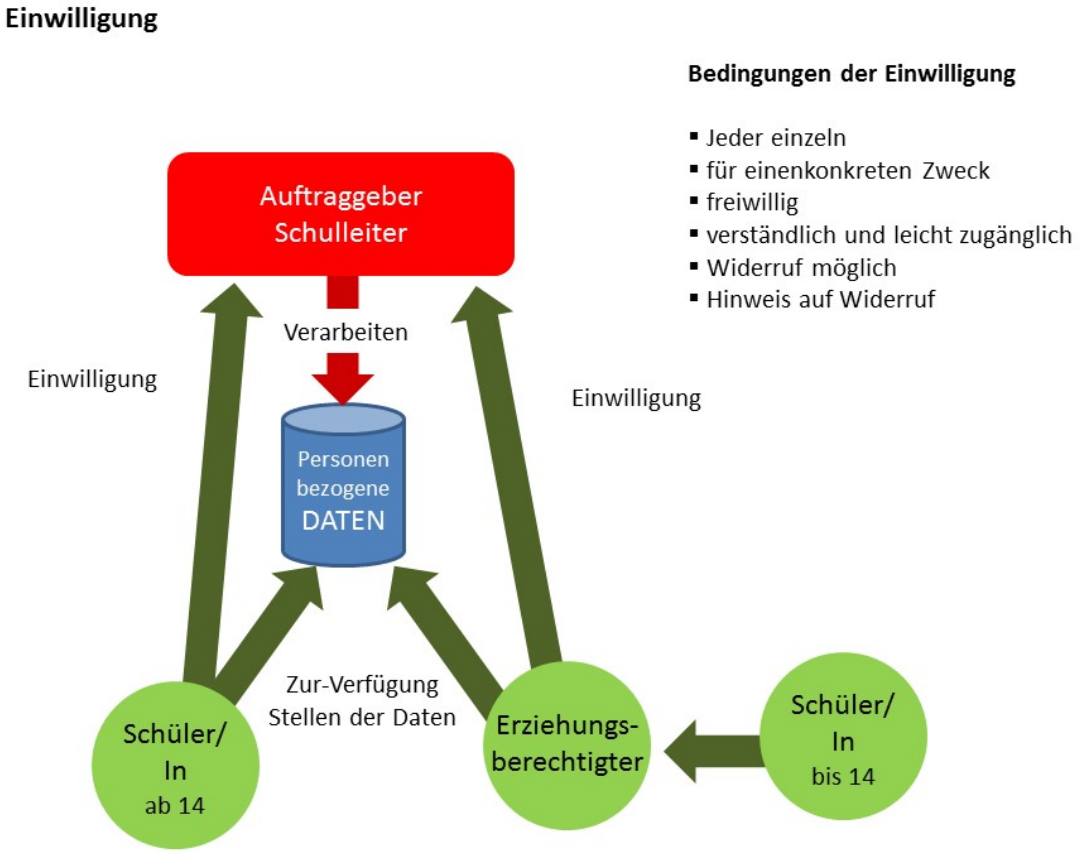
1. Eine datenschutzrechtliche Einwilligung bei Minderjährigen **unter 14 Jahren** ist im Rahmen der Schülerverwaltung jedenfalls durch die **Erziehungsberechtigten** zu geben.

2. Ab dem 14. Lbj. ist die Einwilligungserklärung durch die Schülerinnen und Schüler selbst zu geben, sodass die Eltern diese Erklärung nicht für ihre Kinder abgeben dürfen, da es sich

[3] Die genannte Bestimmung des § 4 Abs. 4 DSG bezieht sich auf „Angebote von Diensten der Informationsgesellschaft, die bei einem Kind direkt gemacht wird“. Diese Formulierung bezieht sich auf Art. 8 Abs. 1 DSGVO. Die Bestimmung ist nicht einschränkend zu verstehen und kommt daher auch im Bereich des Schulrechts zur Anwendung.

beim Datenschutzrecht um ein höchstpersönliches Recht handelt. Es empfiehlt sich jedenfalls, die Erziehungsberechtigten über die datenschutzrechtliche Einwilligung zu informieren.

Abb. 4:



d. Datensicherheit

Datenschutzrecht bedeutet auch, dass die Daten technisch und organisatorisch geschützt werden. In diesem Zusammenhang spricht man von **Datensicherheit**. Datensicherheit ist damit eine Grundvoraussetzung für Datenschutz. Die neue digitale Schülerverwaltung soll daher die Schulen vom Serverbetrieb entlasten und die Datensicherheit erhöhen. Für die Datensicherheit sind folgende Prinzipien entscheidend:

- **Vertraulichkeit**: Daten dürfen nur von autorisierten Benutzern gelesen bzw. modifiziert werden
- **Integrität**: Daten dürfen nicht unbemerkt verändert werden

Die DSGVO verlangt ein dem Risiko der Datenverwendung **angemessenes Schutzniveau**, wobei bei der Beurteilung des Schutzniveaus insbesondere die Risiken durch — ob

unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw unbefugten Zugang zu personenbezogenen Daten zu berücksichtigen sind.

Für die **Datensicherheit** sind insbesondere **folgende Maßnahmen** einzubeziehen:

- ⇨ die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;
- ⇨ die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme** und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- ⇨ die **Fähigkeit**, die Verfügbarkeit der personenbezogenen **Daten** und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall **rasch wiederherzustellen**;
- ⇨ ein **Verfahren zur** regelmäßigen **Überprüfung**, Bewertung und Evaluierung der Wirksamkeit der Systeme

In Schulen sind Grundregeln der Datensicherheit von besonderer Bedeutung. **Datensicherheit** bezieht sich **nicht nur** auf **technische Sicherheit** der Computer, **sondern** vor allem **auch** auf **organisatorische Maßnahmen**, die den Zugriff auf Daten regeln und damit den Missbrauch von Daten verhindern. Hervorgehoben werden soll die Pflicht, Protokolle zu führen und die gesetzten Maßnahmen zu dokumentieren.

FRAGE: Welche Maßnahmen der Datensicherheit sind zu ergreifen?

- ➢ die **Aufgabenverteilung** ist bei der Datenverarbeitung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen;
- ➢ die Verarbeitung von Daten ist an das Vorliegen **gültiger Aufträge** der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden;
- ➢ jeder **Mitarbeiter** muss über seine nach DSGVO und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten **belehrt werden;**
- ➢ die Zutrittsberechtigung zu den Räumlichkeiten des Verantwortlichen oder Auftragsverarbeiter ist zu regeln;
- ➢ die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verarbeitung durch Unbefugte ist zu regeln;
- ➢ die **Berechtigung** zum Betrieb der Datenverarbeitungsgeräte ist festzulegen und jedes (!) Gerät muss durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abgesichert werden;
- ➢ es sind **Protokolle** zu führen, damit tatsächlich durchgeführte Verarbeitungsvorgänge, wie insbesondere Änderungen, Abfragen und

Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können;

- außerdem ist eine **Dokumentation** über die getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

e. Datenschutz durch technische Ausgestaltung und Voreinstellungen

Die DSGVO verpflichtet die Verantwortlichen, also auch die Schulleiterinnen und Schulleiter, **geeignete technische und organisatorische Maßnahmen** (TOM) umzusetzen, um den Datenschutz im Sinne der DSGVO zu gewährleisten (Art. 24 DSGVO). Die Verantwortlichen haben einen **Nachweis** zu erbringen, dass diese Maßnahmen gesetzt wurden.

Zu diesen Maßnahmen zählen auch Datenschutz durch **Technikgestaltung** und die Wahl datenschutzfreundlicher Voreinstellungen im Sinne des Art. 25 DSGVO. So trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. **Pseudonymisierung** —, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. Dies gilt ebenso für die Wahl von **datenschutzfreundlichen Voreinstellungen**.

FRAGE: Was bedeutet und welche Rolle spielt Pseudonymisierung?

Pseudonymisierung bedeutet die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden (Art 4 Z 5 DSGVO). Diese liegt etwa vor, wenn der Name des Schülers bzw. der Schülerin durch eine Kennzahl ersetzt wird und diese Zahl nicht den Personen zugänglich ist, die die Daten verarbeiten. Die Einschränkung der Zugänglichkeit dieser Informationen kann etwa in Form eines Berechtigungssystems erreicht werden.

f. Verzeichnis der Verarbeitungstätigkeiten

Das bisher bestehende **Datenverarbeitungsregister** bei der Datenschutzbehörde wurde mit der Einführung der DSGVO abgeschafft und durch ein (internes) sog. **Verzeichnis der Verarbeitungstätigkeiten** ersetzt (Art 30 DSGVO). Geführt wird das Verzeichnis durch den jeweiligen datenschutzrechtlich Verantwortlichen. Das Bundesministerium für Bildung, Wissenschaft und Forschung führt das Verzeichnis der Verarbeitungstätigkeiten für die zentralen vom Ministerium zur Verfügung gestellten Datenverarbeitungen.
Im Wege der Datenschutzbeauftragten der LSR/SSR Wien wird den weiterführenden höheren Schulen im Zuge der Schulung ein Formular für Verzeichnismeldungen zur Verfügung gestellt. Die daraus resultierenden Meldungen werden durch den LSR/SSR Wien gesammelt und evident gehalten.

FRAGE: Muss jeder Schulleiter / jede Schulleiterin eine Verzeichnis der Verarbeitungstätigkeiten führen?

Nur so weit über die zentralen Datenverarbeitungen des Ministeriums hinaus von der Schule selbst personenbezogene Daten in anderen Zusammenhängen bzw. für andere Zwecke verarbeitet werden, ist ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Dies wird aber nicht von der Schule selbst geführt, sondern soweit es sich um Anwendungen die aus dem Vollzug eines Bundesgetzes resultieren meldet der jeweilige Schulleiter dem Datenschutzbeauftragtem im LSR/SSR Wien seine individuelle Anwendung zur Aufnahme in das DataReg im jeweiligen LSR/SSR Wien

Im Verzeichnis der Verarbeitungstätigkeiten führen, sind darin insbesondere folgende Informationen in Hinblick auf jede Datenverarbeitung anzuführen:

- ⇨ den Namen und die Kontaktdaten des Verantwortlichen sowie des 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 werden, gegebenenfalls Übermittlungen von Daten an ein Drittland
- ⇨ die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

⇨ eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen in Hinblick auf die Datensicherheit

g. Data Breach Notification

Die DSGVO enthält auch eine Bestimmung zur sog. „Data Breach Notification", also zur **Informationspflicht bei Datenmissbrauch** normiert.

Recht im Originaltext:

Art 33 Abs 1 DSGVO: Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der […] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Im Bereich der Schülerverwaltung kann etwa ein Hackerangriff von Schülern bzw SchülerInnen oder dritter Seite auf die Datenbanken der Schule erfolgen und damit für den Schulleiter bzw. die Schulleiterin die Verpflichtung der Information ausgelöst werden. Im Fall eines Datenmissbrauches soll jedenfalls zuerst die zuständige Abteilung des BMBWF (zentraleinformatik@bmbwf.gv.at) sowie der Datenschutzbeauftragte des LSR/SSR Wien kontaktiert werden. In eingeschränkten Fällen, insbesondere bei hohen Risiko für die Rechte und Freiheiten der betroffenen Personen, kann auch eine Pflicht zur Information der betroffenen Personen entstehen. Ist diese Pflicht mit einem unverhältnismäßigen Aufwand verbunden sein, so kann auch eine öffentliche Bekanntmachung erfolgen. Dies ist jedenfalls vor im Dienstweg mit den Datenschutzbeauftragten im LSR/SSR Wien und dem BMBWF abzuklären.

h. Datenschutzrechtliche Folgen-Abschätzung

Bei der Erfassung von Datenanwendungen im Verzeichnis der Verarbeitungstätigkeiten ist auch eine **Risikoabschätzung** vorzunehmen. Im Falle eines **hohen Risikos für die Rechte und Freiheiten natürlicher Personen** kann eine sog **Datenschutz- Folgeabschätzung** gem. Art 35 DSGVO erforderlich werden. Eine solche Situation liegt etwa bei systematischer umfangreiche Überwachung öffentlich zugänglicher Bereiche vor oder wenn eine umfangreiche Verarbeitung

besonderer Kategorien vom personenbezogener Daten (etwa Gesundheitsdaten) folgt. In einem solchen Fall hat der datenschutzrechtlich Verantwortliche eine **Abschätzung der Folgen** der vorher gesehenen Verarbeitungsvorgänge für den Schutz der personenbezogenen Daten durchzuführen und dabei nicht nur geplanten **Verarbeitungsvorgänge** zu **beschreiben** und das damit verbundene **Risiko** zu **bewerten**, sondern insbesondere auch **geplante Abhilfemaßnahmen** zur Bewältigung der Risiken vorzusehen. Damit sind insbesondere Garantien, Sicherheitsvorkehrungen und Verfahren angesprochen. Es kann in diesem Zusammenhang die Notwendigkeit entstehen Datenschutzbehörde vorab zu konsultieren.
Derzeit wird durch eine Arbeitsgruppe, der Vertreter der Zentralstelle, der LSR/SSR Wien sowie Schulen angehören, eine Datenschutzfolgeabschätzung erstellt, die weitgehend alle schulischen Anwendungen abdecken soll, sodass hier voraussichtlich kein eigener Handlungsbedarf für Schulen besteht. Sollten Sie der Auffassung sein, dass Sie für eine besondere Anwendung an Ihrem Schulstandort eine eigene Datenschutzfolgeabschätzung benötigen, kontaktieren Sie bitte den Datenschutzbeauftragten an Ihrem LSR/SSR Wien bzw. in der Zentralstelle.

i. Einrichtung eines Datenschutzbeauftragten

Die **DSGVO verpflichtet** alle Behörden und ö**ffentlichen Stellen zur Einrichtung eines Datenschutzbeauftragten**. Es kann aber auch mehrere Behörden und öffentliche Stellen unter Berücksichtigung der Organisationsstruktur **einen gemeinsamen Datenschutzbeauftragten** benennen. Im Bildungsbereich wurde in diesem Sinne ein Datenschutzbeauftragte auf **ministerielle Ebene** eingerichtet sowie weitere Datenschutzbeauftragte auf **Ebene der Stadt- und Landesschulräte**. Diese Datenschutzbeauftragten übernehmen auch die Funktion für die jeweiligen Schulen.

Die Datenschutzbeauftragten sind unabhängig eingerichtet haben insbesondere folgende Aufgaben:

- ⇨ Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten
- ⇨ Überwachung der Einhaltung der Datenschutzvorschriften
- ⇨ Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter
- ⇨ Beratung — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschätzung
- ⇨ Zusammenarbeit mit der Aufsichtsbehörde und Anlaufstelle für die Aufsichtsbehörde

Derzeit wurden in der Zentralstelle sowie in allen LSR/SSR Wien Datenschutzbeauftrage eingerichtet. Die Namen der jeweiligen Personen werden auf der Webseite des BMBWF zur

Verfügung gestellt. Generell sind die Datenschutzbeauftragten unter folgenden Mail-Adressen erreichbar:
datenschutz@bmbwf.gv.at
datenschutz@lsr-bgld.gv.at
datenschutz@lsr-ktn.gv.at
datenschutz@lsr-noe.gv.at
datenschutz@lsr-ooe.gv.at
datenschutz@lsr-sbg.gv.at
datenschutz@lsr-stmk.gv.at
datenschutz@lsr-t.gv.at
datenschutz@lsr-vgb.gv.at
datenschutz@ssr-wien.gv.at

E. Schulrechtliche Regeln zum Datenschutz

a. Das Bildungsdokumentationsgesetz

Das **Bildungsdokumentationsgesetz** (BilDokG) ist eine zentrale gesetzliche Grundlage zur datenschutzrechtlichen Ermächtigung der Schulleitung. § 2 Abs 3 BilDokG stellt klar, dass der Schulleiter/die Schulleiterin als datenschutzrechtlicher Verantwortlicher anzusehen ist. Werden aber Mittel zur Verarbeitung durch die Schulleitung gemeinsam mit dem BMBWF festgelegt, so sind der Schulleiter/die Schulleiterin und das BMBWF gemeinsam Verantwortliche (§ 2 Abs 4 BilDokG). Für diese Fälle sind die jeweiligen Verpflichtungen der gemeinsam Verantwortlichen in transparenter Form in einer Vereinbarung festzulegen, wobei in den Fällen von Verarbeitungen nach gesetzlichen Vorgaben oder nach Vorgaben des BMBWF jedenfalls vom BMBWF das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO zu führen ist und eine allfällige Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO durchzuführen ist.

§ 3 BilDokG verweist in Hinblick auf den **Zweck der automationsunterstützten Verarbeitung personenbezogener Daten** auf die **Vollziehung des SchUG** und legt sodann die Schülerdaten fest, die im Rahmen dieses Gesetzes erfasst werden dürfen. **§ 3 Abs 1 und 2 BilDokG** sehen vor, dass der Schulleiter/die Schulleiterin für die Vollziehung des SchUG sowie der sonstigen schulrechtlichen Vorschriften folgende schülerbezogene Daten nach Maßgabe der technischen Möglichkeiten automationsunterstützt zu verarbeiten hat:

- Namen

- Geburtsdatum
- SV-Nummer
- Geschlecht
- Staatsangehörigkeit
- Anschrift am Heimatort, gemäß Angaben des Erziehungsberechtigten bzw. der Schülerinnen und Schüler
- Beginn- und Beendigungsdatum, Beendigungsform der jeweiligen Ausbildung
- Religionsbekenntnis gemäß Angaben des Erziehungsberechtigten bzw. der Schülerinnen und Schüler
- das allfällige bildungseinrichtungsspezifische Personenkennzeichen (zB Matrikelnummer).
- Erstes Jahr der allgemeinen Schulpflicht
- Festgestellter sonderpädagogischer Förderbedarf
- Eigenschaft als o. oder ao. Schüler
- Schulkennzahl, Schulformkennzahl
- mit dem Schulbesuch zusammenhängende Daten über die Verletzung der Schulpflicht, die Teilnahme an Unterrichts- und Betreuungsangeboten, den Schulerfolg, die Schul- bzw. Unterrichtsorganisation, den Bildungsverlauf sowie die Inanspruchnahme von Transferleistungen aus dem Familienlastenausgleich nach Maßgabe der Anlage 1
- andere für Vollzugsaufgaben an der Schule notwendige Daten gemäß Anlage 1a (Daten im Zusammenhang mit der Aufnahme der Schülerinnen und Schüler sowie in Zusammenhang mit der Durchführung von Aufnahms- und Eignungsprüfungen; für die Ausgestaltung der Unterrichtsordnung (etwa Klassenbildung, Stundenplan, Befreiungen, Anmeldung zum Betreuungsteil) erforderliche Daten; für die Ausstellung von Zeugnissen, Schulnachrichten und Schulbesuchsbestätigungen erforderliche Daten; Daten zur Beurteilung für Aufsteigen und Wiederholen von Schulstufen, Abschluss von Modulen sowie zur Feststellung der zulässigen Dauer des Schulbesuchs; zur Durchführung von abschließenden Prüfungen und Externistenprüfungen erforderliche Daten; Kontaktdaten der Erziehungsberechtigten; Kontaktdaten der Schüler- und Elternvertreter.)

§ 6 BilDokG sieht überdies die Zusammenführung ausgewählter Daten der Schülerinnen und Schüler in einer **Gesamtevidenz** der Schüler und Schülerinnen der Bildungseinrichtungen vor.

Schließlich regelt § 7c BilDokG einen **Datenverbund der Schulen** in Hinblick auf die **Aufnahme von Schülerinnen und Schüler**. Der Datenverbund der Schulen dient dem Zweck der

Vollständigkeit und der Richtigkeit der bei einem Schulwechsel in den lokalen Evidenzen zu verarbeitenden Schülerdaten. Jede Schule hat im Fall der Beendigung der Schülereigenschaft durch einen Schüler oder eine Schülerin oder auf Anfrage des Schulleiters oder der Schulleiterin einer den betreffenden Schüler oder die betreffende Schülerin aufnehmenden Schule schülerbezogene Daten zu übermitteln. In diesem Fall sind der Schulleiter/die Schulleiterin und das BMBWF gemeinsam Verantwortliche gem Art. 26 DSGVO. Das BRZ wird als Auftragsverarbeiter tätig. Abfrageberechtigt sind die Schulleiterinnen/Schulleiter hinsichtlich der an der betreffenden Schule aufgenommenen Schülerinnen und Schüler. Mit der erfolgten Abfrage des Schülerdatensatzes ist dieser aus dem Datenverbund der Schulen zu löschen.

b. Das Schulunterrichtsgesetz

Ausgangspunkt der Verpflichtungen des Schulleiters/der Schulleiterin als datenschutzrechtlicher Verantwortlicher ist **§ 56 SchUG**, also die allgemeine Regelung über den Schulleiter/die Schulleiterin. § 56 SchUG sieht vor, dass

- der Schulleiter/die Schulleiterin zur Besorgung aller Angelegenheiten nach dem SchUG zuständig ist, sofern dieses Gesetz nicht andere Zuständigkeiten vorsieht
- der Schulleiter/die Schulleiterin der unmittelbare Vorgesetzte aller an der Schule tätigen Lehrerinnen und Lehrer ist. Seine Aufgaben umfassen insbesondere Schulleitung und -management, Qualitätsmanagement, Schul- und Unterrichtsentwicklung, Führung und Personalentwicklung sowie Außenbeziehungen und Öffnung der Schule.
- der Schulleiter/die Schulleiterin für die Einhaltung aller Rechtsvorschriften und schulbehördlichen Weisungen sowie für die **Führung der Amtsschriften** der Schule und die Ordnung in der Schule zu sorgen hat.

Auch wenn das SchUG nicht an die datenschutzrechtliche Terminologie angepasst wurde, beinhaltet es doch unterschiedliche gesetzliche Grundlagen, die für die Verarbeitung personenbezogener Daten im Rahmen der Schülerverwaltung herangezogen werden können. Ausgangspunkt ist die Führung von Aufzeichnungen (Amtsschriften) gem. **§§ 77 und 77a SchUG**, für die gem. § 56 Abs 4 SchUG letztlich der Schulleiter/die Schulleiterin verantwortlich ist. Zur konkreten Führung der Amtsschriften sind die jeweiligen Klassenvorstände gem. § 54 Abs 2 SchUG berufen. Die §§ 77 und 77a SchUG heben folgende Aufzeichnungen an Schulen hervor:

- **Klassenbücher** sind gem **§ 77 SchuG** für jede Klasse zu **Dokumentationszwecken** verpflichtend vorgesehen. Sie enthalten insbesondere Schule, Schulart, Schulstandort, Schuljahr, Klasse bzw. Jahrgang, Schulformkennzahl, Namen der Schülerinnen und Schüler, Unterrichtsgegenstände (Stundenplan), Namen der unterrichtenden Lehrerinnen und Lehrer,

Termine für Schularbeiten und Tests, Anmerkungen zu den einzelnen Unterrichtsstunden: Beginn und Ende der Unterrichtsstunde, behandelter Lehrstoff, durchgeführte Prüfungen, besondere Vorkommnisse wie zB Abweichungen vom Stundenplan (Stundentausch, Supplierung, Entfall, Schulveranstaltungen ua.), Anmerkungen zu den einzelnen Schülerinnen oder Schülern: Fernbleiben, Aufgaben und Funktionen, besondere Vorkommnisse. **Besondere Kategorien personenbezogener Daten** (Art. 9 Abs. 1 DSGVO) dürfen nur dann im Klassenbuch vermerkt werden, wenn deren Dokumentation ein erhebliches öffentliches Interesse darstellt. Klassenbücher können **elektronisch geführt** werden und sind unter Beachtung der Zugriffsbeschränkungen und Datensicherheitsmaßnahmen **drei Jahre** ab dem Ende des letzten Schuljahres der betreffenden Klasse oder des betreffenden Jahrganges an der Schule **aufzubewahren.**

- **Prüfungsprotokolle** über die Durchführung von Einstufungsprüfungen (§ 3 Abs. 6, 7 und 7a), Aufnahms- und Eignungsprüfungen (§§ 6 bis 8), Feststellungsprüfungen (§ 20 Abs. 2), Nachtragsprüfungen (§ 20 Abs. 3), Prüfungen über Kenntnisse und Fertigkeiten des praktischen Unterrichtes (§ 20 Abs. 4), Wiederholungsprüfungen (§ 23), Reifeprüfungen, Semesterprüfungen (§ 23a), Semesterprüfungen über noch nicht besuchte Unterrichtsgegenstände (§ 23b), Einstufungsprüfungen (§ 26a Abs 1 und 3), Einstufungsprüfungen (§ 26a Abs. 1 und 2), Aufnahmsprüfungen (§ 29); Externistenprüfungen (§ 42) und Prüfungen in Widerspruchs- und Beschwerdeverfahren (§ 71 Abs. 4 und 5). In den Prüfungsprotokollen sind die Prüfungskommission (der bzw. die Prüfer/Prüferin), die Daten des Prüfungskandidaten/der Prüfungskandidatin, die Aufgabenstellungen, die Beschreibung der Leistungen und ihre Beurteilung, die Prüfungsergebnisse und die bei der Prüfung oder auf Grund der Prüfungsergebnisse getroffenen Entscheidungen und Verfügungen zu verzeichnen.

Zum Nachweis der Ordnungs- und Rechtmäßigkeit schulinterner Vorgänge sind **Besprechungsprotokolle gem § 77a Abs 3 SchUG** sowie Aufzeichnungen von Konferenzen und von Sitzungen schulpartnerschaftlicher Gremien zu dokumentieren. Sie haben insbesondere zu enthalten: Datum, Zeit, Ort, Namen der Anwesenden; Tagesordnungspunkte; Anträge; Aufzeichnung des Sitzungsverlaufs; gefasste Beschlüsse und Abstimmungsergebnisse sowie Namen und Unterschrift der Protokollführerin oder des Protokollführers.

Protokolle und Aufzeichnungen sind unter Beachtung der **Zugriffsbeschränkungen und Datensicherheitsmaßnahmen gemäß § 77 Abs. 3 drei Jahre** ab dem Jahr, in dem das Protokoll geführt oder die Aufzeichnung stattgefunden hat, aufzubewahren.

In Hinblick auf die **Schülerzeugnisse** konkretisiert **§ 22 SchUG** die zu verwendenden Daten. Diese beinhalten etwa:

- die Bezeichnung, Form bzw. Fachrichtung der Schulart und den Standort der Schule;
- die Personalien des Schülers;
- die besuchte Schulstufe und die Bezeichnung der Klasse (des Jahrganges);
- die Unterrichtsgegenstände der betreffenden Schulstufe und die Beurteilung der darin erbrachten Leistungen (§ 20), sofern der Unterricht in Leistungsgruppen erfolgt, auch die Angabe der Leistungsgruppe;
- die Beurteilung des Verhaltens des Schülers/der Schülerin in der Schule

Gem **§ 61 Abs 3 SchUG** haben die **Erziehungsberechtigten** „die für die Führung der Amtsschriften der Schule erforderlichen Dokumente vorzulegen und Auskünfte zu geben sowie erhebliche Änderungen dieser Angaben unverzüglich der Schule mitzuteilen“.

2. Datenschutz als Grundrecht

A. Überblick

Die Relevanz des Datenschutzes für die Schülerverwaltung ergibt sich aus seiner rechtlichen Bedeutung. Das Datenschutzrecht ist nicht nur eine gesetzliche Vorgabe. **Datenschutz ist** ein verfassungsgesetzlich gewährleistetes Recht, und damit ein **Grundrecht der österreichischen Verfassung (§ 1 Datenschutzgesetz – DSG)**.[4] Als grundrechtliche Vorgabe muss sich der Gesetzgeber (auch im Schulrecht) wie auch die (Schul)Verwaltung an das Datenschutzrecht halten. Das Grundrecht auf Datenschutz schützt die Geheimhaltung personenbezogener Daten.

FRAGE: Was ist mit „personenbezogenen Daten" gemeint?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen (siehe näher unter I.2.B.)

Recht im Originaltext:

§ 1 Abs. 1 DSG: „**Jedermann hat**, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, **Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten**, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind."

FRAGE: Wann unterliegen personenbezogene Daten nicht dem Datenschutz?

Wenn diese allgemeine verfügbar sind (etwa im Internet, nicht aber auf eingeschränkt zugänglichen Foren oder schulinternen Seiten[5]) oder wenn es keinen Bezug mehr zwischen den Daten und der Person gibt (etwa wenn diese in einer Form anonymisiert sind, dass kein Rückschluss auf die Person mehr möglich ist, oder etwa wenn diese in Statistiken aggregiert sind).

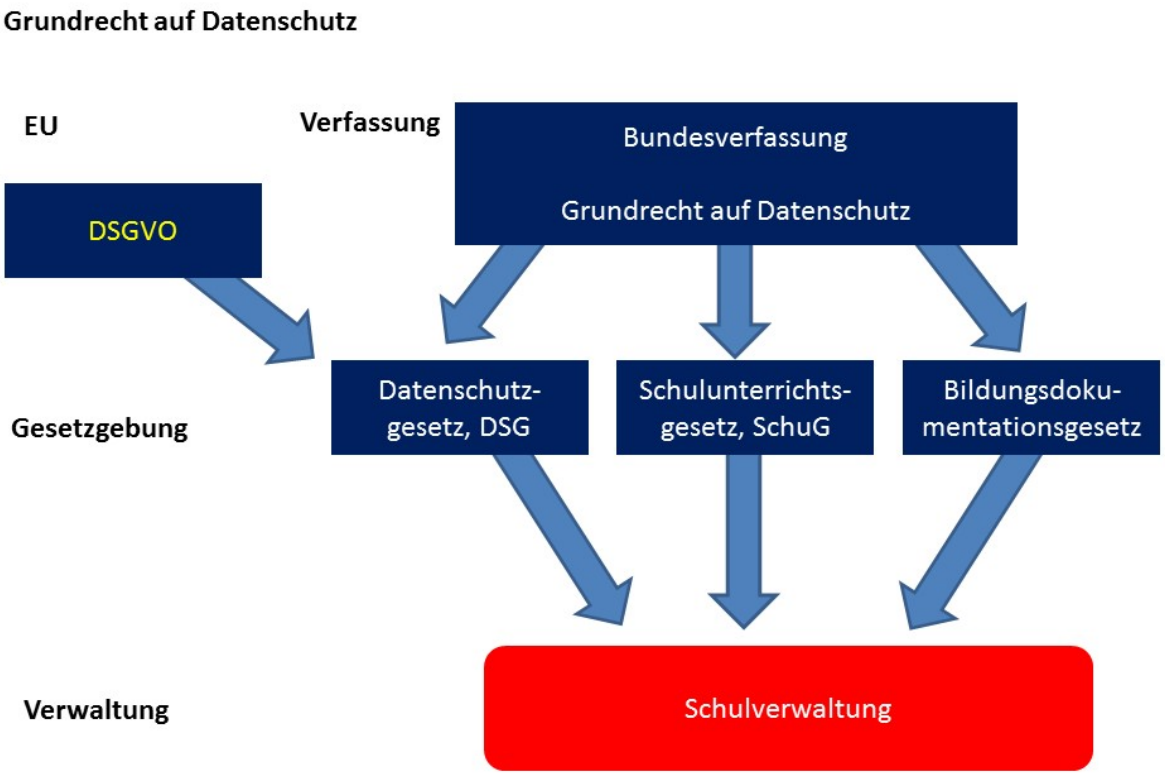
[4] § 1 DSG ist eine Verfassungsbestimmung. Auch wenn das Grundrecht auf Datenschutz in einem einfachen Bundesgesetz verankert ist, handelt es sich um eine Bestimmung des Verfassungsrechts.

[5] Die allgemeine Verfügbarkeit setzt auch eine Veröffentlichung voraus, die zulässiger Weise im Internet stattgefunden hat. Stellt also ein Schüler/eine Schülerin personenbezogene Daten eines anderen Schülers/einer anderen Schülerin ohne dessen/deren Zustimmung auf eine allgemein zugängliche Webseite ins Internet, so liegt keine „allgemeine Verfügbarkeit" im Sinne des DSG vor. Nur wenn die Zustimmung des Schüler vorliegt oder dieser selbst seine Daten im Internet veröffentlicht, liegt „allgemeine Verfügbarkeit" vor und die personenbezogenen Daten unterliegen nicht dem Grundrecht auf Datenschutz.

Rechtliche Konsequenzen aus dem Grundrecht auf Datenschutz für die Schulleitung:

- Die Schulleitung muss das Grundrecht auf Datenschutz einhalten!
- Die Schulleitung darf nur unter Beachtung des Grundrechts personenbezogene Daten verwenden.
- Für das Verwenden personenbezogener Daten bedarf es entweder einer gesetzlichen Grundlage (in der DSGVO, im DSG, im SchUG oder in anderen Gesetzen, etwa dem BilDokG) oder einer Einwilligung der Schülerinnen und Schüler bzw. der Erziehungsberechtigten.
- Überdies muss das Verwenden personenbezogener Daten verhältnismäßig sein. Die Verarbeitung darf also nur dann erfolgen, wenn sie geeignet ist, das damit verbundene Ziel zu erreichen, wenn sie unbedingt notwendig ist und nicht übermäßig in die Rechte des Einzelnen eingreift.
- Schülerinnen und Schüler, Lehrerinnen und Lehrer können ihre Rechte auf Geheimhaltung der personenbezogenen Daten rechtlich geltend machen, wenn diese durch die Schulleitung verletzt werden.
- Die Schulleitung kann in Hinblick auf die betroffenen Personen im Einzelfall eine Auskunftspflicht, eine Richtigstellungspflicht und eine Löschungspflicht treffen.

Abb. 5:



Das **Datenschutzrecht** ist auch **auf europäischer Ebene** grundrechtlich stark **verankert**:

- Art. 8 EU-Grundrechtecharta (GRC, Abs. 1: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.“)
- Art. 16 Vertrag über die Arbeitsweise der EU (AEUV, Abs. 1: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.“)
- Art. 8 Europäische Menschenrechtskonvention (EMRK, Recht auf Achtung des Privat- und Familienlebens)[6]

Die **Schulleitung** ist **auch** den **europäischen Grundrechten verpflichtet**. Sie muss sich daher nicht nur aufgrund der innerstaatlichen Verfassung, sondern aufgrund europäischer Vorgaben an das Datenschutzrecht halten.

B. Die Rechte von Schülerinnen und Schülern

a. Recht auf Geheimhaltung personenbezogener Daten

[6] Art. 8 EMRK ist allgemeiner gefasst. Die Rechtsprechung (Rsp) des Europäischen Gerichtshofs für Menschenrechte (EGMR) in Straßburg umfasst aber auch ein Grundrecht auf Datenschutz.

Das Grundrecht auf Datenschutz bietet zuallererst den **Betroffenen** das **Recht auf Geheimhaltung** ihrer Daten, also den Schutz vor Übermittlung und Preisgabe ihrer Daten. Geschützt ist der Betroffene auch vor der zwangsweisen Verpflichtung zur Weitergabe oder Offenlegung der personenbezogenen Daten.[7].

Ausgangspunkt ist, dass der Betroffene überhaupt keine Daten zur Verfügung stellen muss. Das Recht auf Geheimhaltung bezieht sich nicht nur auf automationsunterstützte Datenanwendung, sondern auch auf manuelle Daten sowie alle anderen Formen der Datenverarbeitung.[8] § 6 DSG konkretisiert das Datengeheimnis und verpflichtet insbesondere auch Mitarbeiter personenbezogene Daten geheimzuhalten

FRAGE: Wer ist „Betroffener" des Grundrechts auf Datenschutz?

Betroffener ist eine natürliche Person, deren Daten verwendet werden. Im Kontext der Schülerverwaltung sind also primär die Schülerinnen und Schüler betroffen, da ihre Daten verarbeitet werden. Der Kreis der Betroffenen kann aber etwa auch die Eltern, schulfremde Personen etc. betreffen. Entscheidend ist, dass ihre personenbezogenen Daten von der Schule verarbeitet werden. (siehe näher unter I.2.B.)

Die Verarbeitung personenbezogener Daten, also ein Eingriff in das Recht auf Geheimhaltung, ist nur unter Hinzutreten bestimmter weiterer Kriterien zulässig:

Recht im Originaltext:

§ 1 Abs. 2 DSG: Soweit die Verwendung von personenbezogenen Daten nicht **im lebenswichtigen Interesse des Betroffenen** oder mit seiner **Zustimmung** erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar **bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen**, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. …

FRAGE: Was ist mit „Einwilligung" gemeint?

[7] *Jahnel*, Handbuch Datenschutzrecht (2010) Rz 2/15.
[8] *Jahnel*, Handbuch Datenschutzrecht (2010) Rz 2/14.

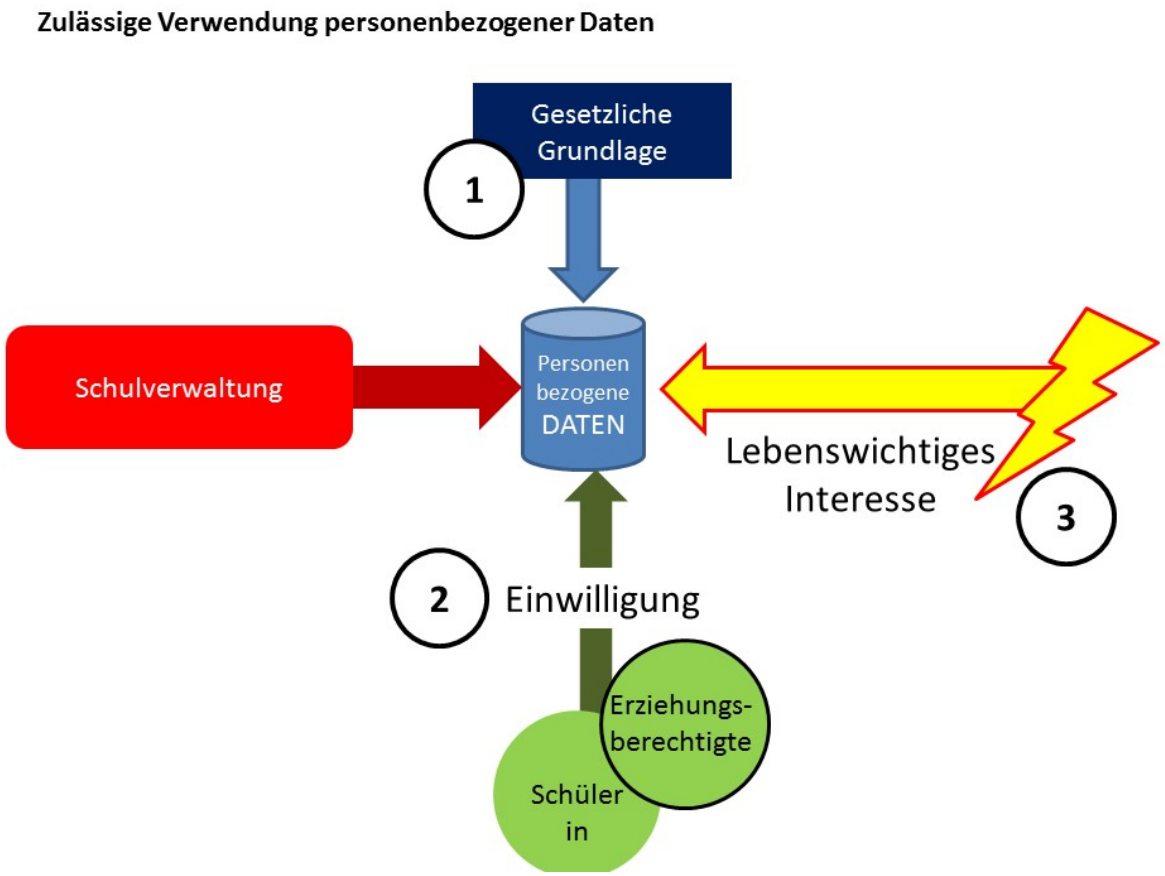
Einwilligung ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

In Hinblick auf die Schülerverwaltung bedeutet dies:

- Primär muss es eine **gesetzliche Grundlage** geben, die sich aus der DSGVO, dem DSG, dem SchUG, dem BilDokG oder anderen Gesetzen ergibt, um datenschutzrechtlich konform tätig werden zu können.
- Gibt es keine gesetzliche Grundlage so ist die **Einwilligung der Betroffenen** bzw. ihrer Erziehungsberechtigten einzuholen.
- Nur im **Ausnahmefall** kann eine Verarbeitung personenbezogener Daten im Kontext der Schülerverwaltung als „im **lebenswichtigen Interesse des Betroffenen**" angesehen werden. Es geht um Umstände, die „sich auf das Leben des Betroffenen im **medizinischen** [!] **Sinn** auswirken".[9] Primärer Zweck ist es, die Einwilligung des Betroffenen zu ersetzen, weil dieser aufgrund der Schwere des Falls nicht mehr in der Lage ist, selbst eine Einwilligung zu geben. Im Zusammenhang mit der Schülerverwaltung ermöglicht diese Bestimmung es der Schule (Direktion, Lehrpersonal), auch ohne die Einwilligung der Erziehungsberechtigten zur Weitergabe von personenbezogenen Daten bei schwerwiegenden Unfällen von Schülerinnen und Schülern rasch zu handeln, ohne Fragen des Datenschutzes klären zu müssen.

[9] *Jahnel*, Handbuch Datenschutzrecht (2010) Rz 2/35.

Abb. 6:



Geben die Schülerinnen und Schüler bzw. auch die Lehrerinnen und Lehrer ihre personenbezogenen Daten der Schulleitung bekannt und verwendet die Schulleitung diese Daten, so dürfen diese – ohne Vorliegen der genannten Voraussetzungen (gesetzliche Grundlage oder Einwilligung oder lebenswichtiges Interesse) – NICHT weitergegeben werden. Die Betroffenen haben ein Recht auf Geheimhaltung ihrer Daten. **Eine unzulässige Weitergabe verletzt das Grundrecht auf Datenschutz**.

b. Transparenz und Informationspflichten

Über das datenschutzrechtliche Grundrecht hinaus sieht die DSGVO zu allererst eine **Verpflichtung zur Transparenz für Verantwortliche** vor, damit betroffenen Personen über die Verarbeitung ihrer personenbezogene Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache informiert werden (Art 12 DSGVO). Insbesondere dann, wenn in der Schule personenbezogene Daten der Schülerinnen und Schüler verarbeitet werden, ist die Schulleitung gem. **Art. 13 DSGVO verpflichtet** mit dem Zeitpunkt der Erhebung insbesondere folgende **Informationen zur Verfügung zu stellen:**

- ⇨ den Namen und die Kontaktdaten des Verantwortlichen (also des Schulleiters oder der Schulleiterin)
- ⇨ die Kontaktdaten des Datenschutzbeauftragten im Landesschulrat (auf Webseite des BMBWF zentral für alle LSR veröffentlicht)
- ⇨ die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die **Rechtsgrundlage** für die Verarbeitung
- ⇨ gegebenenfalls die Empfänger der personenbezogenen Daten, wenn diese an Dritte weitergegeben werden sollen
- ⇨ die **Dauer**, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- ⇨ das Bestehen eines **Rechts auf Auskunft** seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung
- ⇨ das Bestehen eines **Beschwerderechts** bei einer Aufsichtsbehörde

Die **Information ist nicht zu erteilen**, **wenn** die S**chülerinnen und Schüler bereits informiert wurden**. Werden die personenbezogenen Daten nicht direkt bei der betroffenen Person erhoben, besteht nur in eingeschränkten Fällen eine Informationspflicht (Informationspflicht entfällt etwa bei unverhältnismäßigen Aufwand).
Seitens des BMBWF wird ein allgemeiner Text bezüglich der Informationsverpflichtung für bundesweite Schulanwendungen veröffentlicht werden.

c. Recht auf Auskunft, Richtigstellung und Löschung

Über das Recht auf Geheimhaltung hinaus sind drei weitere Rechte vom Grundrecht auf Datenschutz erfasst:

- ➢ Das Recht auf **Auskunft**
- ➢ Das Recht auf **Richtigstellung**
- ➢ Das Recht auf **Löschung**

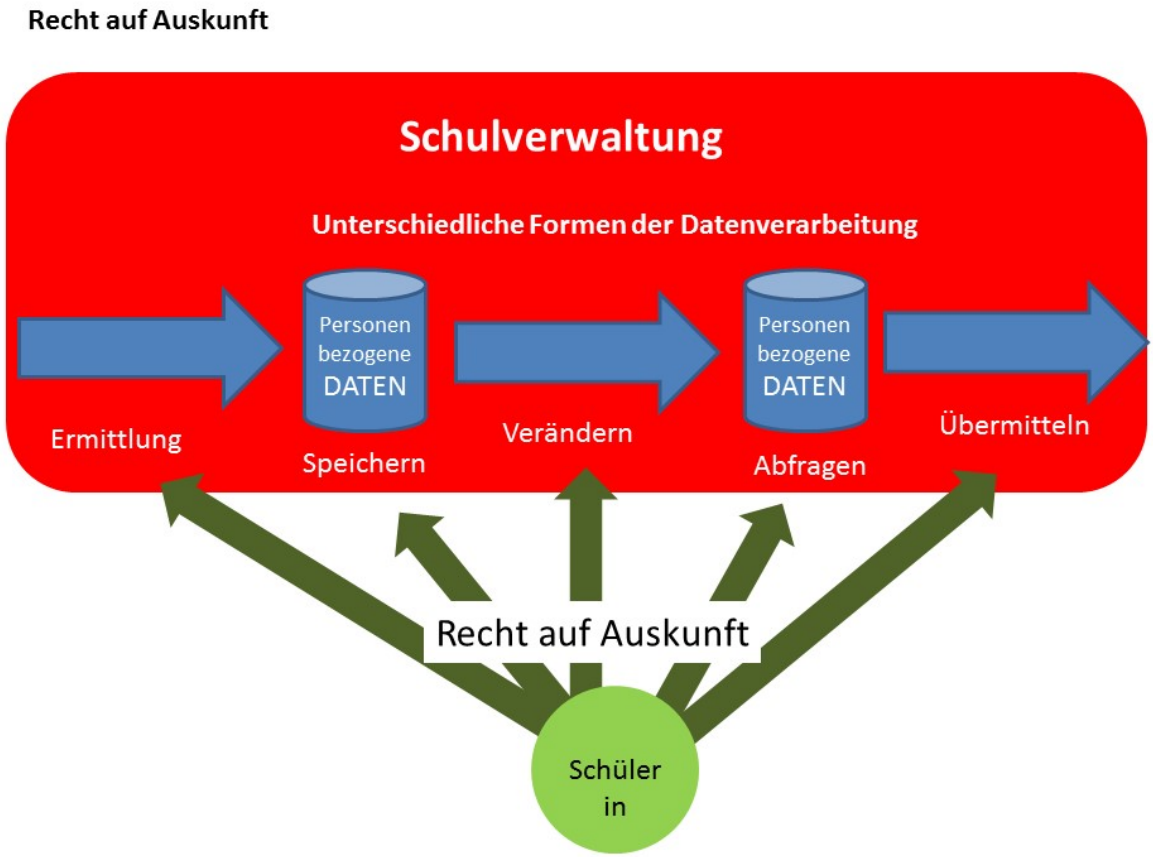
Recht im Originaltext: § 1 Abs. 3 DSG „Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

> 1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
> 2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten."

Recht auf Auskunft

Das **Recht auf Auskunft** bedeutet, dass sich sowohl die Schülerinnen und Schüler als auch die Lehrerinnen und Lehrer jederzeit an die Schulleitung wenden können, um zu **erfragen**, **welche** personenbezogenen **Daten gespeichert** werden. Die Schulleitung ist verpflichtet, entsprechende Auskunft zu geben. Darüber hinaus muss die Schule begründete Auskunft geben können, woher diese Daten stammen und wie und wozu sie verwendet werden. Schließlich ist auch offenzulegen, wem diese Daten weiter übermittelt werden. Die Offenlegung des gesamten Datenkreislaufs ist daher von der grundrechtlichen Verpflichtung umfasst. Die Details regelt nun Art 15 DSGVO.

Abb. 7:



FRAGE: Was ist bei der Auskunftserteilung zu beachten?

- Der **Schulleiter/die Schulleiterin** hat jeder Person oder Personengemeinschaft, die dies schriftlich verlangt und ihre Identität nachweist, **Auskunft** über die zu dieser Person verarbeiteten Daten zu **geben**. Mit Einwilligung des Schulleiters/der Schulleiterin kann das Auskunftsbegehren auch mündlich gestellt werden. Die Auskunft hat die verarbeiteten **Daten**, die Informationen über ihre **Herkunft**, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den **Zweck** der Datenverarbeitung sowie die Rechtsgrundlagen hierfür in allgemein verständlicher Form **anzuführen**.
- Mit Einwilligung des Auskunftswerbers kann anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.
- Wenn zur Person des Auskunftswerbers keine Daten vorhanden sind, genügt die Bekanntgabe dieses Umstandes (**Negativauskunft**).
- Der **Auskunftswerber** hat am Auskunftsverfahren über Befragung in dem ihm zumutbaren Ausmaß **mitzuwirken**, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Schulleiter/der Schulleiterin zu vermeiden.
- **Innerhalb von einem Monat nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen,** warum sie nicht oder nicht vollständig erteilt wird.
- Die Frist kann **um weitere zwei Monate verlängert** werden, wenn dies unter Berücksichtigung der **Komplexität** und der **Anzahl von Anträgen** erforderlich ist. Der Schulleiter bzw die Schulleiterin **unterrichtet** die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung.
- Die Auskunft ist unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und wenn der Auskunftswerber im laufenden Jahr noch kein Auskunftsersuchen an den Verantwortlichen zum selben Aufgabengebiet gestellt hat. In allen anderen Fällen kann ein pauschalierter Kostenersatz von 18,89 Euro verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.
- Von der Erteilung der Auskunft kann abgesehen werden, weil der Auskunftswerber am Verfahren nicht mitgewirkt oder weil er den Kostenersatz nicht geleistet hat.

Siehe Art 12, 15 DSGVO

<u>Das Recht auf Richtigstellung</u>

Das **Recht auf Richtigstellung** ist ein Folgerecht des Auskunftsrechts (Art 16 DSGVO). Wurden Daten falsch erfasst oder haben sich diese verändert, so haben sowohl die Schülerinnen und

Schüler als auch die Lehrerinnen und Lehrer ein Recht auf Richtigstellung (etwa eine Adressänderung), also auf **Änderung der gespeicherten Daten** in Hinblick auf den nun korrekten Inhalt der Daten. Unvollständige Daten sind in Hinblick auf den Zweck der Datenverarbeitung auf Richtigkeit zu prüfen.

Das Recht auf Löschung

Auch das **Recht auf Löschung** ist ein Folgerecht des Rechts auf Auskunft (Art 17 DSGVO). Stellt sich bei der Offenlegung der verwendeten personenbezogenen Daten heraus, dass bestimmte **Daten** etwa **unzulässiger Weise ermittelt oder gespeichert** wurden, so hat der Einzelne ein Recht auf Löschung dieser Daten. Die Unzulässigkeit kann sich auch durch Zeitablauf ergeben. So können Daten aus bestimmten Gründen für die Schulleitung erforderlich gewesen sein (etwa bestimmte Daten einer anderen Schule bei einem Schulwechsel). Fällt aber der Zweck der Datenverarbeitung (etwa erfolgreiche Aufnahme des Schülers) weg, so dürfen diese Daten nicht mehr gespeichert werden. Der Schüler bzw die Schülerin hat ein Recht, die Löschung dieser personenbezogenen Daten zu verlangen.

ACHTUNG: Generell hat der **Schulleiter/die Schulleiterin von sich aus unrichtige Daten richtig zu stellen** oder unzulässige Datenverarbeitungen zu löschen, wenn ihm/ihr diese bekannt werden. Wurden ihm/ihr richtiggestellte oder gelöschte Daten vor der Richtigstellung oder Löschung übermittelt, so hat der Schulleiter/die Schulleiterin die Empfänger dieser Daten hiervon in geeigneter Weise zu verständigen, sofern dies keinen unverhältnismäßigen Aufwand, insbesondere in Hinblick auf das Vorhandensein eines berechtigten Interesses an der Verständigung, bedeutet und die Empfänger noch feststellbar sind.

Der Beweis der Richtigkeit der Daten obliegt dem Schulleiter/der Schulleiterin, außer die Daten beruhen ausschließlich auf Informationen des/der Betroffenen. Eine Richtigstellung oder Löschung von Daten ist ausgeschlossen, soweit der Dokumentationszweck einer Datenanwendung nachträgliche Änderungen nicht zulässt. Die erforderlichen Richtigstellungen sind in diesem Fall durch Anmerkungen zu bewirken. Überdies gilt: Wenn die Löschung oder Richtigstellung von Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden kann, sind bis dahin die zu löschenden Daten für den Zugriff zu sperren und die zu berichtigenden Daten mit einer berichtigenden Anmerkung zu versehen.

FRAGE: Wie ist bei Richtigstellung oder Löschung vorzugehen?

- Der **Schulleiter/die Schulleiterin** hat von Amts wegen aber auch **auf Antrag von Betroffenen** vorzugehen.
- **Innerhalb von einem Monat** nach Einlangen eines Antrags auf Richtigstellung oder Löschung ist dem Antrag zu entsprechen und dem/der Betroffenen davon Mitteilung zu machen oder schriftlich zu begründen, warum die verlangte Löschung oder Richtigstellung nicht vorgenommen wird.
- Werden Daten verwendet, deren Richtigkeit der/die Betroffene bestreitet, und lässt sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen, so ist auf Verlangen des/der Betroffenen nur eine eingeschränkte Verarbeitung zulässig. Dies bedeutet dass die Verarbeitung dieser Daten nur mehr mit Einwilligung der betroffenen Person oder aus wichtigen öffentlichen Interessen zulässig ist. Die Einschränkung der Verarbeitung ist zu lange aufrecht zu halten, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen.

Siehe Art. 17 DSGVO

C. Die Schulleitung als Grundrechtsverpflichteter

Die **Schulleitung** ist organisatorisch Teil der **Bundesverwaltung** und somit ein **Organ einer Gebietskörperschaft**. Die Schulen sind unselbständige Anstalten des Bundes. Überdies wird die Schulleitung in Vollziehung der Gesetze und damit hoheitlich tätig. Die Vollziehung des Schulrechts fällt in den Bereich der Hoheitsverwaltung. Die Zuordnung der Schulleitung zum Bund ist für das Datenschutzrecht von erheblicher Bedeutung, da § 26 DSG zwischen Verantwortlichen des öffentlichen und dem privaten Bereich unterscheidet. Datenanwendungen sind dem öffentlichen Bereich im Sinne dieses Bundesgesetzes zuzurechnen, wenn sie für Zwecke eines „Verantwortlichen des öffentlichen Bereichs“ durchgeführt werden. Als „Verantwortlicher des öffentlichen Bereichs“ versteht § 26 DSG alle Verantwortlichen, die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, und soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.

Die **zentrale Anknüpfung** für die **datenschutzrechtliche Verantwortlichkeit** ist der Begriff des Verantwortlichen. **Verantwortlicher ist jede Person, die die Entscheidung trifft, die personenbezogenen Daten zu verwenden.**

Recht im Originaltext:

Art. 4 Z 7 DSGVO **Verantwortlicher**: die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser

> Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

§ 3 BilDokG verpflichtet den Schulleiter/die Schulleiterin zur Verarbeitung personenbezogener Daten in Erfüllung der Aufgaben des SchUG. Damit ist der **Schulleiter/die Schulleiterin** der **datenschutzrechtliche Verantwortliche** iSd Art. 4 DSGVO.[10] Den Schulleiter/die Schulleiterin als datenschutzrechtlichen Verantwortlichen vorzusehen entspricht der Funktion des Schulleiters/der Schulleiterin iSd § 56 SchUG. So ist der Schulleiter/die Schulleiterin grundsätzlich zur „Besorgung aller Angelegenheiten" des SchUG zuständig und überdies obliegt ihm/ihr gem. § 56 Abs. 4 SchUG die „Einhaltung aller Rechtsvorschriften". Der Schulleiter bzw. die Schulleiterin vereint Zuständigkeit und Verantwortlichkeit – dies auch im datenschutzrechtlichen Sinne – und ist damit konsequenter Weise datenschutzrechtlicher Verantwortlicher.[11]

Das BMBWF ist jedenfalls für das Führen des Verzeichnisses von Verarbeitungstätigkeiten gem. Art. 30 DSGVO und die Durchführung allfälliger Datenschutz-Folgenabschätzungen gem. Art. 35 DSGVO zuständig (§ 2 ABs 4 BilDokG).

An die Zuordnung des datenschutzrechtlichen Verantwortlichen knüpfen sich die **datenschutzrechtlichen Verpflichtungen**. So ist der **Schulleiter/die Schulleiterin** als Verantwortlicher zur Einhaltung des Grundrechts auf Datenschutz verpflichtet. Der Verantwortliche hat nicht nur für die Geheimhaltung der personenbezogenen Daten zu sorgen, sondern ist auch Adressat des Auskunftsrechts sowie des Rechts auf Richtigstellung bzw. Löschung.

D. Der Rechtsschutz von Schülerinnen und Schülern

Wenn Schülerinnen und Schüler bzw. Lehrerinnen und Lehrer ihre **Rechte** aus dem Grundrecht auf Datenschutz **geltend machen** wollen, so haben sie sich zu aller erst an die **Schulleitung** selbst zu wenden. Die Schulleitung hat sodann die entsprechenden Auskünfte in Hinblick auf den

[10] Siehe mwN *Jahnel*, Handbuch Datenschutzrecht (2010) Rz 3/37; DSK 11.3.2005, K120.991/0006-DSK/2005; DSK 20.06.2008, K600.055-001/0002-DVR/2008.
[11] Siehe *Wolkinger*, Datenschutz im Bildungswesen, in: Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) facultas.wuv 273 (282).

Betroffenen zu geben (siehe oben unter I.1.B.b.). Machen die Betroffenen bzw. ihre Erziehungsberechtigten weitere Rechte (Richtigstellung oder Löschung) geltend, so ist die Rechtmäßigkeit des Anliegens durch die Schulleitung zu prüfen. Kommt es zu keiner Einigung zwischen Schulleitung und Betroffenen, so steht den Betroffenen der **administrative und gerichtliche Rechtsweg** offen.

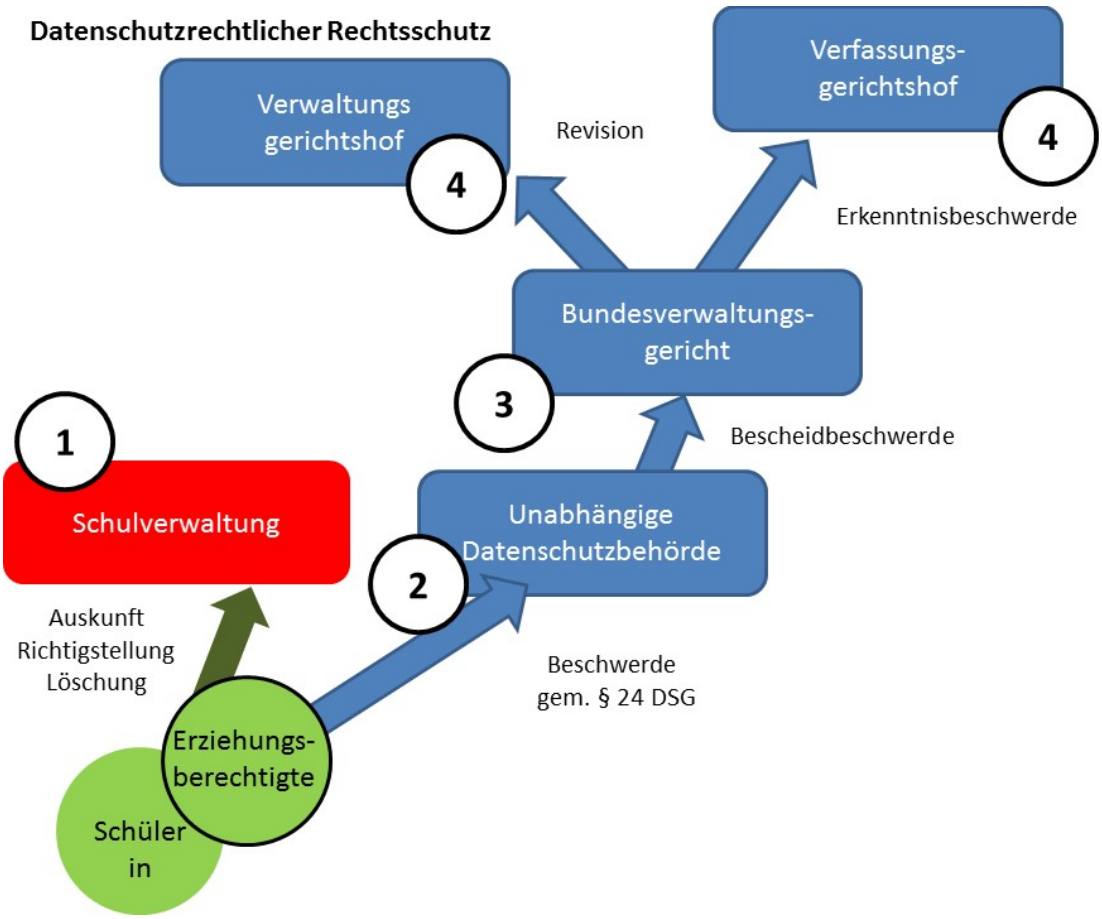
In Österreich besteht eine **unabhängige Datenschutzbehörde** mit einer Behördenleiterin an der Spitze. Betroffene Personen können sich über unzulässige Verarbeitungen ihrer personenbezogenen Daten bei der Datenschutzbehörde beschweren. Gegen den Bescheid der Datenschutzbehörde besteht die Möglichkeit einer Bescheidbeschwerde an das **Bundesverwaltungsgericht** (BVwG). Das BVwG ermöglicht einen gerichtlichen Rechtsschutz in Verwaltungsangelegenheiten und damit auch für das Datenschutzrecht. Es besteht vor dem BVwG keine Anwaltspflicht. Es kann sich nicht nur der Betroffene, sondern auch die Schulleitung an das BVwG wenden.[12] Das BVwG entscheidet in Form eines gerichtlichen Urteils, das als „Erkenntnis" bezeichnet wird. Gegen das Erkenntnis des BVwG besteht sodann gegebenenfalls die Möglichkeit, die Gerichtshöfe des öffentlichen Rechts anzurufen. Gem. Art. 144 B-VG kann eine **Erkenntnisbeschwerde** beim **Verfassungsgerichtshof (VfGH)** eingebracht werden, in der der Betroffene die Verletzung in seinem Grundrecht auf Datenschutz geltend machen kann.

[12] Amtsbeschwerde xxx.

Gem. Art. 133 B-VG kann auch eine Revision an den **Verwaltungsgerichtshof (VwGH)** erhoben werden. Die **Revision** ist aber nur zulässig, wenn

- sie von der Lösung einer Rechtsfrage abhängt, der grundsätzliche Bedeutung zukommt, insbesondere weil das Erkenntnis von der Rechtsprechung des Verwaltungsgerichtshofes abweicht,
- eine VwGH Rechtsprechung fehlt oder
- die zu lösende Rechtsfrage in der bisherigen Rechtsprechung des VwGH nicht einheitlich beantwortet wird.[13]

Abb. 8:



[13] Art 133 Abs. 4 B-VG idF BGBl I 2012/51.

II. Besondere datenschutzrechtliche Fragestellungen in der Schülerverwaltung

Management Summary

- Die **digitale Schülerverwaltung** führt zu einer neuen Systemarchitektur an den Schulen. Die datenschutzrechtlichen Verpflichtungen des Schulleiters/der Schulleiterin als Verantwortlicher bleiben bestehen. Die Datenerfassung beruht auf den expliziten datenschutzrechtlichen Bestimmungen des SchUG und des BilDokG sowie auf den schulrechtlichen Regelungen des SchUG, soweit die Datenverarbeitung eine wesentliche Voraussetzung für die Wahrnehmung einer der Schulleitung gesetzlich übertragenen Aufgabe darstellt. Darüber hinaus sieht die digitale Schülerverwaltung auch die Möglichkeit von bestimmten freiwilligen Angaben vor, die auf einer Einwilligung der Betroffenen beruht.

- Im Rahmen des **BilDokG** bestehen unterschiedliche **datenschutzrechtliche Schnittstellen** zwischen der Schulleitung und dem BMBWF bzw. den LSR. Hervorzuheben ist die Erstellung von Gesamtevidenzen, etwa auch der Schülerinnen und Schüler gem § 5 BilDokG. Hier werden nur pseudonymisierte Daten verarbeitet.

- Bei einem **Schulwechsel** besteht die Möglichkeit der Erfassung der personenbezogenen Daten der Schülerin bzw. des Schülers durch die neue Schule aufgrund der Vorlage der Daten durch die Schülerin bzw. den Schüler selbst. Darüber hinaus sieht § 7c BilDokG die Errichtung eines Datenverbunds der Schulen vor.

- Das **elektronische Klassenbuch** basiert auf den Bestimmung der §§ 77 SchUG. Weitere Aufzeichnungen (etwa Prüfungsprotokolle) finden ihre gesetzliche Grundlage in § 77a SchUG oder etwa Zeugnisse aufgrund der §§ 22, 22a SchUG.

- Die **edu.card** ist gesetzlich im § 57b SchUG geregelt Sie auf Verlangen des Schülers der Schülerin auszustellen und auch nicht eine wesentliche Voraussetzung für die Wahrnehmung einer der Schulleitung gesetzlich übertragenen Aufgabe. Insoweit bleibt die edu.card von der Einwilligung der betroffenen Schülerinnen und Schüler bzw. der Erziehungsberechtigten abhängig. Dabei ist vor allem die Zweckbindung (wofür werden welche Daten verwendet) und die Verhältnismäßigkeit von besonderer Bedeutung.

Jedenfalls muss es für Schülerinnen und Schüler die Möglichkeit geben, auch ohne edu.card regulär an den Schulaktivitäten teilzunehmen.

- **Weitere Fragestellungen** ergeben sich in Hinblick auf den Umgang mit Gesundheitsdaten und der SV-Nr., hinsichtlich der Videoüberwachung, einer allfälligen Dienstleistungsvereinbarung, dem Schutz des persönlichen Bildnisses und einer Internet-Policy für Schulen.

1. Überblick

Über die allgemeinen datenschutzrechtlichen Grundlagen in Hinblick auf die Schülerverwaltung hinaus ergeben sich zahlreiche **konkrete datenschutzrechtliche Fragestellungen im Schulalltag.** Die Frage- und Problemstellungen sind vielfältig und zum Teil sehr komplex. Schließlich sind mit Datenanwendungen oft vielfältige Prozesse der Verarbeitung personenbezogener Daten verbunden.

Im **Zentrum** der besonderen datenschutzrechtlichen Fragestellungen steht **die digitale Schülerverwaltung des Bundes**. Durch die Einführung einer einheitlichen IT-Systemarchitektur für Schulen werden die technischen Rahmenbedingungen für eine elektronische Schülerverwaltung neu strukturiert. Damit sind auch datenschutzrechtliche Klarstellungen erforderlich.

Über die digitale Schülerverwaltung hinaus sollen zentrale **datenschutzrechtliche Problembereiche aus dem Schulalltag** näher vorgestellt werden, die regelmäßig auftreten. Es wurden unterschiedliche Bereiche ausgewählt, die sich auf klassische schulrechtliche Themen beziehen, wie etwa den Schulwechsel oder den Umgang mit Gesundheitsdaten/SV-Nr. Ein Schwerpunkt liegt auf den technischen Neuerungen, wie etwa das Führen eines elektronischen Klassenbuchs oder der edu.card. Für die Schülerverwaltung von besonderer Relevanz sind ebenso der Schutz des persönlichen Bildnisses, die Verarbeitung von Videoüberwachung, die Vereinbarung mit Auftragsverarbeitern sowie die Internet-Policy für Schulen. Abschließend werden noch weitere Fragen kurz erläutert (Sponsoren, Facebook, Website, Handyblocker).

2. Digitale Schülerverwaltung

Die vor ein paar Jahren vorgenommene **Neustrukturierung der digitalen Schülerverwaltung** unter Zusammenführung der bisherigen unterschiedlichen Systeme unter ein einheitliches digitales System der Schülerverwaltung des Bundes schafft vielfältige Vorteile für die Schülerverwaltung:

- Entlastung der Bundesschulen von derzeit technisch aufwendiger Administration
- Einsatz modernster Technologie und zeitgemäßer Systemarchitektur
- Verfügbarkeit von Schnittstellen für wesentliche Verwaltungsaufgaben
- Vereinheitlichung der Organisation bei Ankauf und Adaptierung der Schülerverwaltungssoftware
- Senkung der Kosten für Betrieb und Wartung

Verantwortliche bleiben in der digitalen Schülerverwaltung weiterhin die **Schulleiter**/die **Schulleiterinnen**; dies aber nicht alleine! Werden Mittel zur Verarbeitung durch Schulleiterinnen bzw Schulleiter gemeinsam mit dem BMBWF festgelegt, so sind die Schulleiterinnen bzw Schulleiter und der zuständige Bundesminister gemeinsam Verantwortliche gemäß Art. 26 DSGVO. Für diese Fälle sind die jeweiligen Verpflichtungen der gemeinsam Verantwortlichen in transparenter Form in einer Vereinbarung festzulegen. Der BMBWF ist jedenfalls für das Führen des Verzeichnisses von Verarbeitungstätigkeiten gem. Art. 30 DSGVO und die Durchführung allfälliger Datenschutz-Folgenabschätzungen gem. Art. 35 DSGVO zuständig (§ 2 Abs 4 BilDokG).

Innerhalb der **einheitlichen Systemarchitektur** bestehen für die Schulen durch die vorgesehene Verwaltung der Zugriffsrechte eigene Bereiche (Mandantenfähigkeiten). Auf diese Bereiche der Schule können weder andere Schulleiter/Schulleiterinnen noch der LSR oder das BMBWF zugreifen. Es besteht kein Zugriff auf die Daten der anderen Schulleiter/Schulleiterinnen. Die rechtlichen Rahmenbedingungen haben sich insoweit nicht geändert.

Die neue Schülerverwaltung **unterscheidet** zwischen **personenbezogenen Daten,**

- die **aufgrund einer expliziten gesetzlichen Grundlage** (BilDokG, SchUG) oder einer wesentlichen Voraussetzung für die Wahrnehmung der dem Schulleiter/der Schulleiterin gesetzlich übertragenen Aufgaben (iSd SchUG) verarbeitet werden und
- die **nur mittels Einwilligung freiwillig** der Schulleitung zur Verfügung gestellt werden.

Je nach Bereich (gesetzliche Grundlage bzw. Aufgabe / Einwilligung) sind von Seiten der Schülerverwaltung die genannten rechtlichen Rahmenbedingungen zu berücksichtigen. Entscheidend ist in beiden Fällen, dass der Zweck der Datenverarbeitung klar ist und die Daten nur für diesen Zweck verwendet werden. Überdies ist bei der Datenverarbeitung immer auf die Verhältnismäßigkeit im Einzelfall verpflichtend Rücksicht zu nehmen.

ACHTUNG: Zum Teil werden durch die einheitliche, digitale Schülerverwaltung des Bundes auch **besondere Kategorien von Daten** (Religionsbekenntnis, Gesundheitsdaten) erfasst. Die vom System erfassten besonderen Kategorien von Daten sind möglichst zu beschränken.

Die **Datenerfassung beruht auf den expliziten datenschutzrechtlichen Bestimmungen des SchUG und des BilDokG** sowie auf den schulrechtlichen Regelungen des SchUG, soweit die Datenverarbeitung eine wesentliche Voraussetzung für die Wahrnehmung einer der Schulleitung gesetzlich übertragenen Aufgabe darstellt. Im Rahmen der digitalen Schülerverwaltung werden unterschiedliche **Datenkategorien** erfasst (siehe dazu den Anhang).

3. Schnittstellen zwischen Schulleitung und LSR / BMBWF

Im Rahmen des BilDokG ist vorgesehen, dass auch Daten der Schülerverwaltung an das BMBWF („den zuständigen Bundesminister“) übermittelt werden müssen. Es handelt sich dabei um explizite gesetzliche Grundlagen der Datenverarbeitung gem §§ 4, 5 BilDokG. Der dabei im Vordergrund stehende Zweck sind **Evidenzen**. Gem **§ 4 BilDokG** hat der zuständige Bundesminister „für die Zwecke der Planung, der Steuerung, der Wahrung der gesetzlichen Aufsichtspflichten, der Bundesstatistik und der Verwaltungsstatistik Evidenz über den Personal-, Betriebs- und Erhaltungsaufwand der Bildungseinrichtungen zu führen, bei denen dieser Aufwand zur Gänze oder zum Teil aus Bundesmitteln getragen wird.“ Dabei handelt es sich primär um **nicht personenbezogene oder pseudonymisierte Daten der Lehrerinnen und Lehrer**. Gem **§ 5 BilDokG** werden „Gesamtevidenzen der Schüler“ vorgesehen. Der BMBWF hat als datenschutzrechtlicher Verantwortlicher „für die Zwecke der Planung, der Steuerung, der Wahrung der gesetzlichen Aufsichtspflichten und der Bundesstatistik automationsunterstützt **Gesamtevidenzen der Schüler** einzurichten.“ Die Daten der Schülerinnen und Schüler werden in den Gesamtevidenzen aber nur **pseudonymisiert** gespeichert.

FRAGE: Was bedeutet Pseudonymisierung?

Pseudonymisierung“ bedeutet die **Verarbeitung personenbezogener Daten** in einer Weise, dass **die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen**

nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Siehe Art. 4 Z 5 DSGVO.

Das BMBWF kann gem. **§ 8 BilDokG** den **Schulbehörden des Bundes** (also etwa dem LSR), wenn es zum Zweck der Wahrnehmung der ihnen gesetzlich übertragenen Aufgaben (Planung, Steuerung und Wahrung der gesetzlichen Aufsichtspflichten) erforderlich ist, eine **Abfrageberechtigung** im Wege des Datenfernverkehrs auf die in den Gesamtevidenzen gemäß § 5 verarbeiteten Daten eröffnen, wobei ein Rückschluss auf Angaben über bestimmte Bildungsteilnehmer nicht möglich ist.

Recht im Originaltext:

§ 8. (1) Der Bundesminister für Bildung kann den Schulbehörden des Bundes, wenn es zum Zweck der Wahrnehmung der ihnen gesetzlich übertragenen Aufgaben (Planung, Steuerung und Wahrung der gesetzlichen Aufsichtspflichten) erforderlich ist, eine Abfrageberechtigung im Wege des Datenfernverkehrs auf die in den Gesamtevidenzen gemäß § 5 verarbeiteten Daten in der Weise eröffnen, dass statistische Auswertungen unter Wahrung des Statistikgeheimnisses … möglich und eine Ermittlung und Abspeicherung von Daten über einen bestimmten Bildungsteilnehmer bzw. ein Rückschluss auf Angaben über bestimmte Bildungsteilnehmer nicht möglich sind. …

Über diese Datenübermittlungen in Hinblick auf die Gesamtevidenzen hinaus, finden sich **weitere datenschutzrechtlich** relevante **Schnittstellen** zum BMBWF und zum LSR. Zu erwähnen ist etwa § 3 Abs 5 BilDokG: Absehen von Prüfungen gem. § 13 Abs. 3 Schulpflichtgesetz (SchPfG), Befreiung vom Besuch der Berufsschule gem. § 23 SchPfG, Befreiung vom Schulbesuch gem. § 15 SchPfG in Hinblick auf den LSR.

4. Schulwechsel

Mit dem **Übertritt eines Schülers bzw. einer Schülerin von einer Schule in eine andere** ist datenschutzrechtlich ein Wechsel des Verantwortlichen (von einer Schulleitung zur anderen)

verbunden. Die datenschutzrechtliche Fragestellung bezieht sich auf die Übernahme von personenbezogenen Daten von der alten Schule auf die neue.

Werden die Daten durch die neue Schule in das IT-System selbst übernommen, ist klarzustellen, wie die Schülerverwaltung diese Daten erhalten hat. Der typische Fall besteht dabei darin, dass die Schülerin bzw. der Schüler **freiwillig** seine Einwilligung erteilt, dass eine Schulde die Daten an die andere Schule übermittelt. Das Erfassen der Daten ist durch die §§ 3-8 SchUG, die sich mit der Aufnahme von Schülerinnen und Schülern befassen, im Rahmen des gesetzlichen Aufgabenbereichs der Schulleitung gedeckt.

Für die automatisierte Übermittlung der Daten wurde eine neue gesetzliche Grundlage in **§ 7c BilDokG** durch das Datenschutz-Anpassungsgesetz Bildung im Jahr 2018 geschaffen. § 7c BilDokG regelt nun einen **Datenverbund der Schulen** in Hinblick auf die **Aufnahme von Schülerinnen und Schüler**. Der Datenverbund der Schulen dient dem Zweck der Vollständigkeit und der Richtigkeit der bei einem Schulwechsel in den lokalen Evidenzen zu verarbeitenden Schülerdaten.

5. Elektronisches Klassenbuch

Klassenbücher sind sowohl **manuell als auch elektronisch** als Verarbeitung personenbezogener Daten zu verstehen. „Das Klassenbuch **dient** dazu, zur **Sicherstellung** und zum **Nachweis** der Ordnungsgemäßheit des **Unterrichts** Vorgänge zu dokumentieren, die im Zusammenhang mit der Organisation und der Durchführung von Unterricht stehen.“ Auch in Bezug auf diese besteht ein Recht auf Geheimhaltung, Auskunft, Richtigstellung und Löschung. Die Führung eines elektronischen Klassenbuchs kann sich auf die Bestimmung des **§ 77 Abs 3 SchUG** stützten. Klassenbücher erfassen folgende, zum Teil auch personenbezogene Daten:

- ✓ Schule, Schulart, Schulstandort, Schuljahr, Klasse bzw. Jahrgang, Schulformkennzahl,
- ✓ die Namen der Schülerinnen und Schüler der Klasse
- ✓ die Unterrichtsgegenstände (Stundenplan)
- ✓ den Namen der unterrichtenden Lehrerinnen und Lehrer,
- ✓ Termine für Schularbeiten und Tests,
- ✓ Anmerkungen zu den einzelnen Unterrichtsstunden: Beginn und Ende der Unterrichtsstunde, behandelter Lehrstoff, durchgeführte Prüfungen, besondere Vorkommnisse wie zB Abweichungen vom Stundenplan (Stundentausch, Supplierung, Entfall, Schulveranstaltungen ua.),

- ✓ Anmerkungen zu den einzelnen Schülerinnen oder Schülern: Fernbleiben, Aufgaben und Funktionen, besondere Vorkommnisse ua.

Besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO dürfen nur dann im Klassenbuch vermerkt werden, wenn deren Dokumentation ein erhebliches öffentliches Interesse darstellt.

Für die **Datensicherheit** der Klassenbücher wird vorgesehen, dass diese zu sichern sind und vor dem Zugriff anderer Personen als dem an der Schule tätigen Lehr- und Verwaltungspersonal geschützt zu verwahren sind. Es sind Datensicherheitsmaßnahmen gemäß Art. 32 DSGVO zu treffen und es sind die Bestimmungen über das Datengeheimnis anzuwenden.

FRAGE: Welche Datensicherheitsmaßnahmen sieht Art. 32 DSGVO vor?

Gem. Art. 32 Abs. 1 DSGVO haben datenschutzrechtlich Verantwortliche ebenso wie Auftragsverarbeiter insbesondere folgende technische und organisatorische Maßnahmen der Datensicherheit zu setzen:

- ⇨ Risikoanalyse hinsichtlich der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen und damit verbunden die Festlegung eines angemessenen Schutzniveaus
- ⇨ die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- ⇨ die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- ⇨ die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ⇨ ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Das Einräumen von Abfrageberechtigungen und das Schaffen von Einsichts- oder Zugriffsmöglichkeiten für andere Personen als dem an der Schule tätigen Lehr- und Verwaltungspersonal, Schülerinnen und Schüler sowie Erziehungsberechtigte ist nicht zulässig. Für Schülerinnen und Schüler sowie für Erziehungsberechtigte darf ein Personenbezug nur

hinsichtlich der eigenen Person bzw. des Kindes, auf das sich das Erziehungsrecht bezieht, hergestellt werden.

Klassenbücher sind unter Beachtung der Zugriffsbeschränkungen und Datensicherheitsmaßnahmen **drei Jahre ab dem Ende des letzten Schuljahres** der betreffenden Klasse oder **des betreffenden Jahrganges** an der Schule **aufzubewahren**. **Nach Ablauf der Aufbewahrungsfrist** sind physische Aufzeichnungen zu vernichten und elektronisch gespeicherte Aufzeichnungen zu **löschen**.

6. Edu.card

Die edu.card ist eine **Karte**, auf der ein elektronischer Chip angebracht sein kann, und die als Sichtfunktion für Schülerinnen und Schüler den **bisherigen Schülerausweis zwecks Authentifizierung gleichgestellt**. Damit wird auf den Vorwurf der leichten Fälschbarkeit des bisherigen papierbasierten Schülerausweises, den die Schülerinnen und Schüler selbst ausfüllen, reagiert.

Neben diesem grundsätzlichen Zweck der edu.card kann bzw. wird diese mit **unterschiedlichen anderen Funktionen** verbunden, etwa Zugangsmöglichkeiten zu Räumen wie der Bibliothek. Sie kann aber auch mit einer Kopierkarten- oder Geldbörsefunktion ausgestattet werden. Wird die edu.card über die Funktion als reiner Sichtausweis hinausgehend auch als **ServiceCard** eingesetzt und werden auf dem Chip der Vor- und Nachname des Schülers gespeichert, so handelt es sich um die Verarbeitung personenbezogener Daten. Diese werden sodann je nach Funktion mit weiteren Daten verknüpft. Dies können etwa Schuldaten (Bezeichnung der Schule, Schulkennzahl) und Schülerdaten (Lichtbild, Geburtsdatum, Ausweisnummer) sein. Durch weitere Funktionen werden weitere personenbezogene Daten gesammelt.

Datenschutzrechtlicher Verantwortlicher der edu.card ist der Schulleiter/die Schulleiterin. Die Einführung und der Einsatz der edu.card können jedenfalls auf Basis der **datenschutzrechtlichen Einwilligung** erfolgen. Die Einwilligung zur edu.card muss durch den einzelnen Schüler bzw. die einzelne Schülerin erfolgen. Dabei ist – wie oben dargestellt – in besonderer Weise auf die Einwilligung der Erziehungsberechtigten bzw. der Schüler sowie auf die damit verbundene Freiwilligkeit der Einwilligung zu achten. Dies bedeutet aber auch, dass es für Schülerinnen und Schüler, die keine Einwilligung geben, zu keinen strukturellen Nachteilen bei der Benützung der Schulinfrastruktur kommen kann (etwa bei dem Zugang zu Räumen).[14]

[14] Siehe *Wohlkinger*, Datenschutz im Bildungswesen, in: Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) facultas.wuv 273 (291).

Bei den Chipkarten ist in besonderer Weise das datenschutzrechtliche Prinzip der Zweckbindung zu berücksichtigen. Es darf die Verarbeitung personenbezogener Daten nur für eindeutig festgelegte Zwecke erfolgen. Die Daten dürfen nicht darüber hinaus weiter verwendet werden.

In Hinsicht auf Zugangssysteme etwa kann eine edu.card auch mit einem einheitlichen Code für alle Schülerinnen und Schüler ausgestattet werden. Die Erfassung der personenbezogenen Daten bedarf im Sinne des Verhältnismäßigkeitsprinzips besonderer Rechtfertigung. Die Erfassung, wer wann welchen Raum betritt, ist grundsätzlich nicht erforderlich. Eine Speicherung personenbezogener Daten wäre jedenfalls aus datenschutzrechtlicher Sicht zeitlich stark zu begrenzen.

7. Weitere Fragestellungen

A. Vereinbarung mit Auftragsverarbeitern

Die im Rahmen der Schülerverwaltung durchgeführte Verarbeitung personenbezogener Daten kann aus unterschiedlichen Gründen die Involvierung von Dritten – Unternehmen – beinhalten, die für die Schulleitung die personenbezogenen Daten verarbeiten. Es handelt sich also **nicht um eine Weitergabe personenbezogener Daten an Dritte** (etwa an andere Schulen, Sponsoren etc.), sondern um eine **Überlassung von Daten an einen Auftragsverarbeiter**, der für die Schule tätig wird. Auftragsverarbeiter ist gem. Art. 4 Z 8 DSGVO „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“. Ein Auftragsverarbeiter wird von der Schulleitung beauftragt, für diese tätig zu werden. Zu denken ist etwa an Softwarebetreiber oder Webseitenanbieter, die für die Schule die Verarbeitung von Daten vornehmen. Fotografen sind nur bei Ausweiserstellung Auftragsverarbeiter; bei Klassenfotos durch professionelle Fotografen treten diese selbst als datenschutzrechtliche Verantwortliche auf und damit direkt in eine rechtliche Beziehung zu den Fotografierten, ohne dass die Schulleitung an dieser Rechtsbeziehung beteiligt ist.

ACHTUNG Bei Auftragsverarbeitern aus dem Ausland sind die datenschutzrechtlichen Rahmenbedingungen im Besonderen zu berücksichtigen. Generell gilt, dass die DSGVO auch auf die Verarbeitung personenbezogener Daten im Ausland anzuwenden ist.

Die DSGVO stellt Bedingungen für die Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen durch Auftragsverarbeiter auf. So erfolgt die Verarbeitung durch einen

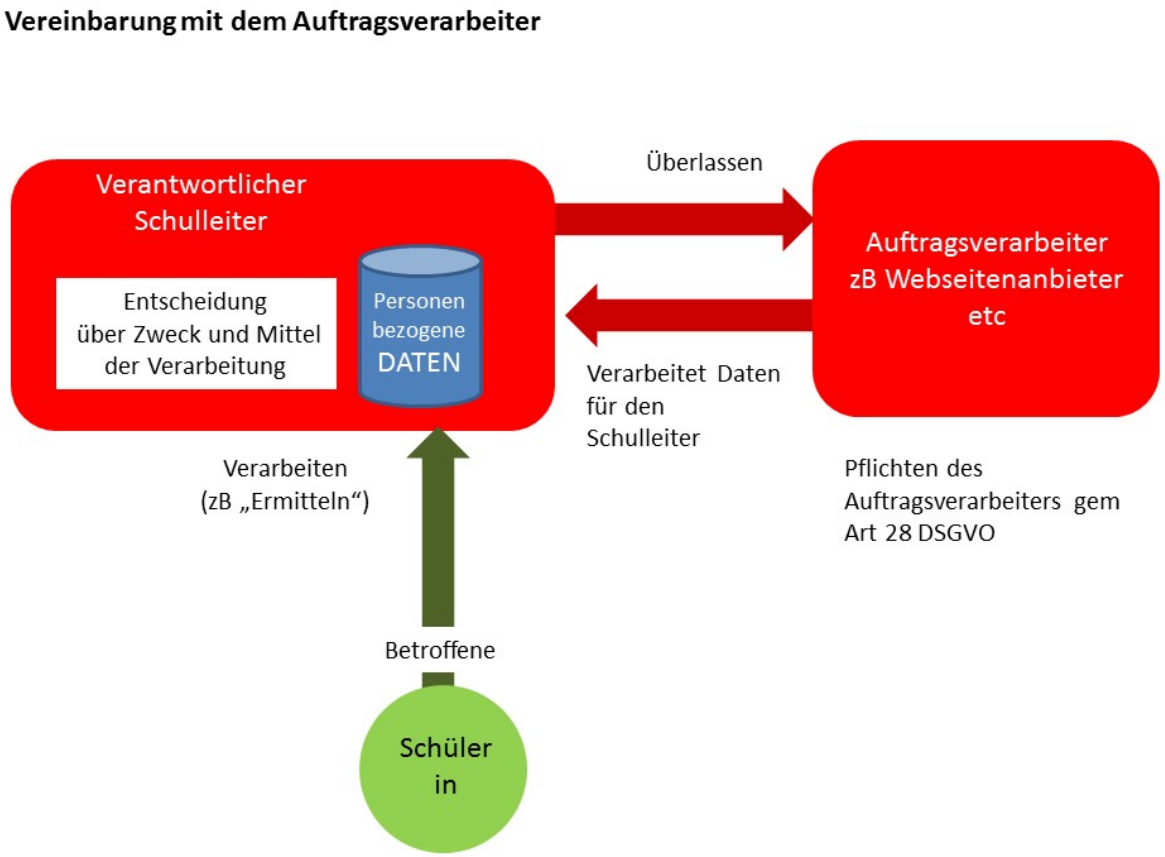
Auftragsverarbeiter auf der Grundlage eines Vertrags, der den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.

Recht im Originaltext:

Art 28 DSGVO:

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Abb. 9:



FRAGE: Welche Pflichten hat der Vertrag mit dem Auftragsverarbeiter zu enthalten?

Gem. Art. 28 Abs. 1 DSGVO sieht vor, dass der Auftragsverarbeiter

- ⇨ die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeitet;
- ⇨ gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben;
- ⇨ alle erforderlichen Maßnahmen der Datensicherheit ergreift;
- ⇨ Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters (z.B. Schriftlichkeit) einhält;
- ⇨ angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person nachzukommen;
- ⇨ unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;
- ⇨ nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
- ⇨ dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten zur Verfügung stellt und Überprüfungen — einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Siehe Näheres zur Vereinbarung mit dem Auftragsverarbeiter im Anhang.

Ein Muster für eine datenschutzrechtliche Vereinbarung mit einem Auftragsverarbeiter findet sich unter: https://bildung.bmbwf.gv.at/service/datenschutzvereinbarung.html

B. Umgang mit Gesundheitsdaten/SV-Nr.

Umgang mit Gesundheitsdaten

Im Kontext der Schülerverwaltung ist der Umgang mit **Gesundheitsdaten** immer wieder erforderlich. Aus datenschutzrechtlicher Sicht ist zu berücksichtigen, dass es sich bei Gesundheitsdaten um besondere Kategorien von Daten und damit um **besonders**

schützenswerte Daten handelt. Insoweit ist die Verhältnismäßigkeit beim Verwenden von Gesundheitsdaten von besonderer Bedeutung.

Der Umgang mit Gesundheitsdaten in der Schülerverwaltung ist unmittelbar mit dem **Schularzt** (siehe § 66 SchUG) verbunden, der nicht nur dem Datenschutz, sondern auch der ärztlichen Schweigepflicht entsprechen muss. Bekommt also der Schularzt ein ärztliches Attest einer Schülerin bzw. eines Schülers, so hat dieser nicht die Diagnose, sondern nur noch das dem Schüler bzw. der Schülerin gebotene Verhalten zu kommunizieren.

Weitere datenschutzrechtliche Fragestellungen im Zusammenhang mit Datenverarbeitung durch Schulärzte werden durch die zuständige Fachabteilung im BMBWF gerade auf Konformität zur DSGVO geprüft.

C. Videoüberwachung

Für Schulen wird die Möglichkeit der **Videoüberwachung** immer relevanter. Das DSG sieht in der Novelle des Datenschutz-AnpassungsG 2018 eine Neuregelung des Einsatzes von Videos vor. §§ 12, 13 DSG regeln die Zulässigkeit von Bildaufnahmen in Hinblick auf private Zwecke. Auch wenn diese Regeln somit für öffentliche Zwecke nicht zur Anwendung kommen, bleibt die DSGVO an sich auch für die Videoüberwachung im Bereich der Schule relevant.

FRAGE: Was bedeutet Bildaufnahme im Sinne des DSG?

Bildaufnahme bezeichnet die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu privaten Zwecken.

Soweit die **Videoüberwachung** an Schulen als ein privater Zweck verstanden wird, ist diese **zulässig**, wenn

- diese im lebenswichtigen Interesse einer Person erfoderlich ist,
- die betroffene Person zur Verarbeitung ihrer personenbezogenen Daten eingewilligt hat,
- sie durch **besondere gesetzliche Bestimmungen angeordnet** oder erlaubt ist, oder
- im Einzelfall **überwiegende berechtigte Interessen des Verantwortlichen** oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist.

Als **überwiegendes berechtigtes Interesse** wird gem. § 12 Abs 3 DSG auch die Bildaufnahme „für den **vorbeugenden Schutz von Personen oder Sachen** an öffentlich zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen, aufgrund bereits erfolgter Rechtsverletzungen oder eines in der Natur des Ortes liegenden besonderen Gefährdungspotenzials erforderlich ist und kein gelinderes geeignetes Mittel zur Verfügung steht“, verstanden.

Der **Schulleiter bzw. die Schulleiterin**, als der Verantwortliche der Videoüberwachung, hat dem Risiko des Eingriffs angepasste geeignete **Datensicherheitsmaßnahmen** zu ergreifen und dafür zu sorgen, dass der Zugang zur Bildaufnahme und eine nachträgliche Veränderung derselben durch Unbefugte ausgeschlossen ist sowie die Bildaufnahmen **geeignet zu kennzeichnen**. Aufgenommene personenbezogene Daten sind vom Verantwortlichen zu **löschen**, wenn sie für den Zweck, für den sie ermittelt wurden, nicht mehr benötigt werden und keine andere gesetzlich vorgesehene Aufbewahrungspflicht besteht. Eine länger als **72 Stunden** andauernde Aufbewahrung muss verhältnismäßig sein und ist gesondert zu protokollieren und zu begründen (§ 13 DSGVO).

Abb. 10:

Bei der Videoüberwachung in der Schule muss in besonderer Weise das **Verhältnismäßigkeitsprinzip** berücksichtigt werden. Dabei ist der Zweck der Videoüberwachung ebenso wie die Minimierung des Eingriffs in die Privatsphäre der erfassten Personen relevant. So kann etwa die Videoüberwachung auf Zeiten außerhalb des regulären Schulbetriebs beschränkt werden. Untersagt ist gem. § 13 DSG die Einrichtung einer Videoüberwachung an Orten, die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen (also etwa Toiletten).

FRAGE: Muss die Videoüberwachung im Verzeichnis von Verarbeitungstätigkeiten aufgenommen werden?

Die Videoüberwachung bedeutet die Verarbeitung personenbezogener Daten. Es bedarf daher eine Aufnahme in das Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DSGVO.

D. Schutz des persönlichen Bildnisses

In der Schule werden häufig Fotos geschossen und Videos aufgezeichnet. Zu betonen ist, dass es sich bei **Abbildungen** von Schülerinnen und Schülern bzw. Lehrerinnen und Lehrern **um personenbezogene Daten** im Sinne der DSGVO handelt. Dies deshalb, da die Identität der Betroffenen bestimmbar ist. Es ist daher schon aus datenschutzrechtlichen Erwägungen erforderlich, diese Daten zu schützen. Es sind daher von der Schule aufgenommene Fotografien/Videos nur mit **Einwilligung** der Erziehungsberechtigten bzw. der Schülerinnen und Schüler möglich. Es empfiehlt sich eine entsprechende Einwilligung am Anfang des Schuljahres durch die Einwilligungsberechtigten einzuholen.

Über die Regelungen des DSGVO hinaus finden sich in der Rechtsordnung weitere Bestimmungen zum Schutz des persönlichen Bildnisses. Hervorzuheben ist etwa **§ 78 UrheberrechtsG**[15]:

Recht im Originaltext:

Bildnisschutz
§ 78 Abs. 1 UrhG: „Bildnisse von Personen dürfen weder öffentlich ausgestellt noch auf eine andere Art, wodurch sie der Öffentlichkeit

[15] Siehe auch § 16 ABGB.

> zugänglich gemacht werden, verbreitet werden, wenn dadurch berechtigte Interessen des Abgebildeten oder, falls er gestorben ist, ohne die Veröffentlichung gestattet oder angeordnet zu haben, eines nahen Angehörigen verletzt würden."

ACHTUNG Vom urheberrechtlichen sowie datenschutzrechtlichen Schutz erfasst sind:

- nicht nur Portraits, sondern auch Gruppenbilder
- Bilder auch ohne Namensnennung

Der **Umgang mit Medien** in der Schule bedarf **klarer Regeln** (zB: Hausordnung, Verhaltensvereinbarungen). Dies beginnt bei den Fotos und Videos und geht bis zu der Veröffentlichung in unterschiedlichen Medien wie etwa Jahresberichten oder Webseiten. Entscheidend ist, dass sich die Einwilligung auf die unterschiedlichen Verarbeitungszwecke der medial erfassten personenbezogenen Daten bezieht. Insoweit ist bereits in den Einwilligungserklärungen der Medienumgang klarzulegen.

E. Empfehlungen zur Mediennutzung und zur IT-Policy

Nutzung digitaler Geräte an Schulstandorten (Internet-Policy

Die Verwendung von Internet im schulischen Alltag, aber auch in der Schülerverwaltung, ist heute beinahe eine Selbstverständlichkeit. So verfügen Schulen typischerweise über einen Außenauftritt im WorldWideWeb, zumeist in Form einer Homepage. Mit dem Internet sind vielfältige Herausforderungen, aber auch datenschutzrechtlich relevante Problemstellungen verbunden, derer sich die Schulleitung bewusst sein sollte. Insoweit sollten die **Richtlinien für den Umgang mit dem Internet in der Schule** generell durch die Schulleitung klar festgelegt und kommuniziert werden. Es bedarf daher einer Internet-Policy für Schulen.
Eine derartige **Internet-Policy** könnte etwa folgende Fragestellungen ansprechen:

- **Untersagung** der Nutzung von **illegalen** oder für Schüler/Schülerinnen ungeeigneten **Materialien**.
- Die **Internetnutzung** darf den **Schulbetrieb nicht beeinträchtigen**.
- Herunterladen von **urheberrechtlich geschütztem Material** nur mit Einwilligung der Urheber.
- **Keine übermäßige Nutzung von Speicherplatz**, kein übermäßiges Drucken.
- **Datenschutz**: Es dürfen keine personenbezogenen Daten von Schüler/Schülerinnen im Internet ohne Einwilligung veröffentlicht werden.
- **Persönliches Bildnis:** nur Bilder von Personen veröffentlichen, die damit einverstanden sind.

- **Zitierregeln**: alle Dokumente aus dem Internet, die für Referate, Hausarbeiten oder ähnliches verwendet werden, sind dort mit Quellenangabe und Autor/Autorin zu zitieren.
- Verbot der kommerziellen oder gewerblichen Verarbeitung (Zielgruppe: Lehrende)
- Keine Weitergabe von Passwörtern an Dritte
- Keine Verarbeitung illegaler Software
- Kein Einbringen von Schadsoftware

Siehe dazu ausführlich: Meinl et. al, Recht in virtuellen Lernumgebungen, BMUKK, 2010 http://www.saferinternet.at/uploads/tx_simaterials/Recht_in_virtuellen_Lernumgebungen_1012.pdf.

FRAGE: Dürfen personenbezogene Daten an Dritte, etwa Sponsoren, weitergegeben werden?

Nein, es ist nicht Aufgabe der Schulen, personenbezogene Daten an Dritte, wie etwa Sponsoren, weiterzugeben, die mit diesen Daten einen kommerziellen und damit schulfremden Zweck verfolgen. Überdies wäre eine solche Weitergabe an eine explizite Einwilligung der Erziehungsberechtigten bzw. der Schülerinnen und Schüler geknüpft, die die Übermittlung an Dritte konkret vorgibt und den Zweck der Übermittlung klarstellen muss.

FRAGE: Welche personenbezogenen Daten der Schülerinnen und Schüler dürfen auf der Webseite der Schule publiziert werden?

Ohne explizite Einwilligung der Erziehungsberechtigten bzw. der Schülerinnen und Schüler dürfen personenbezogene Daten nicht auf der Website der Schule publiziert werden. Dies wäre im Rahmen einer zwischen der Schulleitung und den Erziehungsberechtigten zu schließenden Vereinbarung – etwa am Schulanfang – klarzustellen. Dies bezieht sich auch auf Schulveranstaltungen und Videos, die öffentlich zur Verfügung gestellt werden sollen. Die Notwendigkeit einer Einwilligung setzt die Erkennbarkeit von Schülerinnen und Schülern voraus.

FRAGE: Wie steht es mit dem Betreiben einer eigenen Facebook-Seite durch die Schulleitung um Zwecke der Darstellung der Schule?

Facebook ist aus vielfältigen Gründen datenschutzrechtlich problematisch. Überdies sollen Schülerinnen und Schüler nicht dazu verpflichtet werden, sich bei einer sozialen Webplattform anzumelden. Von der Verarbeitung von sozialen Medien als offizielles Kommunikationsmedium der Schulleitung wird daher abgeraten. Die Thematisierung von sozialen Medien im Unterricht zwecks Sensibilisierung in Hinblick auf das Thema „Soziale Medien“ ist erwünscht. Damit verbunden sollte aber wiederum nicht eine Verpflichtung bzw. die Notwendigkeit sein, dass Schülerinnen bzw. Schüler selbst ein Konto auf der Webseite eröffnen müssen.

III. Anhang

1. Glossar

- **Verantwortlicher** ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (**Schulleitung**); unabhängig davon, ob sie die Daten selbst verwenden oder damit einen Auftragsverarbeiter beauftragen.

- **Betroffener** ist jede vom **Verantwortlichen** verschiedene Person, deren Daten verwendet werden (Schülerinnen und Schüler, Lehrerinnen und Lehrer).

- **Data Breach Notification** (Meldung von Verletzungen des Schutzes personenbezogener Daten): Wird dem Verantwortlichen bekannt, dass Daten aus einer seiner Datenanwendungen unrechtmäßig verwendet wurden oder andere Verletzungen des Datenschutzes vorgefallen sind, hat er darüber binnen 72 Stunden die Aufsichtsbehörde bzw. in bestimmten Situation den Betroffenen in geeigneter Form zu informieren.

- **Auftragsverarbeiter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (etwa Bundesrechenzentrum).

- **Personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

- **Besondere Kategorien personenbezogener Daten** bezieht sich auf die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,

Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

- **Verarbeiten von Daten**: jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

- **Videoüberwachung** bezeichnet die systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt (überwachtes Objekt) oder eine bestimmte Person (überwachte Person) betreffen, durch technische Bildaufnahme- oder Bildübertragungsgeräte.

- **Überlassen von Daten** bedeutet die Weitergabe von Daten zwischen Verantwortlicher und Auftragsverarbeiter im Rahmen des Auftragsverhältnisses.

- **Übermitteln von Daten** ist die Weitergabe von Daten an andere Empfänger als den/die Betroffene/n, den/die Verantwortliche oder einen Auftragsverarbeiter, insbesondere auch das Veröffentlichen von Daten (z.B. Weitergabe von Schülerstammdaten von Volksschule an Gymnasium an der Nahtstelle oder Übermittlung an den LSR); darüber hinaus auch die Verarbeitung von Daten für ein anderes Aufgabengebiet des Verantwortlichen(!)

- **Einwilligung** ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

2. Abkürzungsverzeichnis

Abs	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
Änd	Änderung
Anm	Anmerkung
Art	Artikel
Aufl	Auflage
BG	Bundesgesetz, Schweizer Bundesgericht
BGBl	Bundesgesetzblatt
BilDokG	Bildungsdokumentationsgesetz
BM	Bundesminister(ium)
BMUKK	Bundesminister(ium) für Unterricht, Kunst und Kultur
bPK	bereichsspezifischen Personenkennzeichen
BVwG	Bundesverwaltungsgericht
B-VG	Österreichisches Bundes-Verfassungsgesetz
DSG	Datenschutzgesetz
DSK	Datenschutzkommission
EMRK	Europäische Menschenrechtskonvention
Erk	Erkenntnis
EU	Europäische Union
f	folgend
ff	fortfolgend
G	Gesetz
gem	gemäß
GRC	Grundrechtecharta der Europäischen Union
Hrsg	Herausgeber
idF	in der Fassung
idZ	in diesem Zusammenhang
iSd	im Sinne des
iVm	in Verbindung mit
iZm	im Zusammenhang mit
lit	litera
LSR	Landesschulrat
Nr	Nummer
Nov	Novelle
Nr	Nummer

Rsp	Rechtsprechung
Rz	Randzahl
SchUG	Schulunterrichtsgesetz
TKG	Telekommunikationsgesetz
VfGH	Verfassungsgerichtshof
VO	Verordnung
VwGH	Verwaltungsgerichtshof
Z	Ziffer
zB	zum Beispiel

3. Literaturverzeichnis

A. Materialien

Empfehlungen zur Mediennutzung und zur IT-Policy Nutzung digitaler Geräte an Schulstandorten

Meinl et. al, Recht in virtuellen Lernumgebungen, BMUKK, 2010 http://www.saferinternet.at/uploads/tx_simaterials/Recht_in_virtuellen_Lernumgebungen_1012.pdf

Schutz der Privatsphäre im Internet, Unterrichtsmaterialien, Saferinternet et. al. http://www.saferinternet.at/uploads/tx_simaterials/Schulmaterial_Schutz_der_Privatsphaere_im_Internet.pdf

Datenschutzkommission, Broschüre: Du bestimmst – Datenschutz-Fakten und Gefahren

Menzel et. al., Edu.gov – E-Government im Unterricht, BMUKK, 2. Aufl., 2012 http://edugov.bildung.at/edugov/learning/Unterrichtsmaterialien.

Broschürenservice der Initiative SaferInternet.at http://www.saferinternet.at/broschuerenservice/

B. Weiterführende Links:

Datenschutzbehörde – www.dsb.gv.at

Österreichisches Rechtsinformationssystem – www.ris.bka.gv.at

Datenschutzgesetz gesamt (Stand: 01.03.2018): http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597

C. Rechtswissenschaftliche Literatur

Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) facultas.wuv.

Dohr/Pollierer/Weiss/Knyrim (Hrsg), DSG Kommentar. Manz Verlag.

Jahnel, Datenschutzrecht (2010) Jan Sramek Verlag.

Lachmayer, Die DSGVO im öffentlichen Bereich. Europarechtliche Vorgaben an die staatliche Verwaltung, Österreichische Juristenzeitung 2018, 112.

Lachmayer, Die Multidimensionalität des Datenschutzrechts. Zur Notwendigkeit der Ausdifferenzierung datenschutzrechtlicher Regelungen, in Feik/Winkler (Hrsg), Festschrift für Walter Berka (2013) Jan Sramek Verlag, 121-139.

Lehner, Recht auf Datenschutz, in: Heißl (Hrsg), Handbuch Menschenrechte (2008) facultas.wuv, 211.

Lehner/Lachmayer, Datenschutz im Verfassungsrecht, in: Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) facultas.wuv, 95.

N. Raschauer (Hrsg), Datenschutzrecht 2010 (2011) Jan Sramek Verlag.

Wohlkinger, Datenschutz im Bildungswesen, in: Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) facultas.wuv 273.

4. Vorlagen

A. Mustervereinbarung: Schule – Auftragsverarbeiter

Aktuelle Version unter:
https://bildung.bmbwf.gv.at/service/datenschutzvereinbarung.html

Vereinbarung zur Auftragsverarbeitung

abgeschlossen zwischen

Bundesgymnasium XYZ
Musterweg 5
3020 Wolkenhausen
Österreich
nachfolgend als „Auftraggeber“ oder „Verantwortlicher“ bezeichnet

und

<Name des Unternehmens (Firma)>
<Firmenbuchnummer, sofern vorhanden>
<Anschrift>
<Land>

nachfolgend als „Auftragnehmer“ oder „Auftragsverarbeiter“ bezeichnet

Präambel
Die Vertragsparteien haben am <DATUM> einen Vertrag über <z.B. die Erbringung von IT-Leistungen> geschlossen (im Folgenden kurz „Hauptvertrag“).
Der Auftragsverarbeiter betreut auf Grundlage des Hauptvertrages folgende Applikationen: <hier bitte eine taxative Aufzählung der durch den Auftragsverarbeiter betreuten Applikationen einfügen>:
und erbringt in diesem Zusammenhang folgende IT-Leistungen:

<Kurzbeschreibung der Tätigkeiten des Auftragsverarbeiters einfügen, beispielhaft: *Der* Auftragsverarbeiter *betreut den Auftraggeber als externer Dienstleister in IT-Fragen, erledigt den Second Level System Support für den Auftraggeber mittels Hotline* >

Dabei verarbeitet der Auftragnehmer als Auftragsverarbeiter personenbezogene Daten im Auftrag des Auftraggebers. Da die DSGVO vorsieht, dass eine solche Verarbeitung personenbezogener Daten im Auftrag eine vertragliche Grundlage erfordert, schließen die Vertragsparteien die vorliegende Vereinbarung:

Die vorliegende Vereinbarung stellt die vertragliche Basis für die Auftragsverarbeitung gemäß Artikel 28 DSGVO dar und regelt die Rechte und Pflichten der Vertragsparteien im Hinblick auf eine datenschutzkonforme Auftragsverarbeitung. Die vorliegende Vereinbarung konkretisiert somit den zwischen dem Auftraggeber (als Verantwortlichen nach Artikel 4 Abs 7 DSGVO) und dem Auftragnehmer abgeschlossenen „Hauptvertrag" bezüglich der Verarbeitung personenbezogener Daten durch den Auftragnehmer (als Auftragsverarbeiter nach Artikel 4 Abs 8 DSGVO) im Auftrag des Auftraggebers.

Die Kategorien der von der Datenverarbeitung betroffenen Personen lauten wie folgt: <beispielhaft, jeweils anzuführen, z.B: Schüler, Studierende, Eltern, Lehrer, Alumni etc>.
ODER ALTERNATIV DAZU (obenstehende Variante zu entfernen): Die Kategorien der von der Datenverarbeitung betroffenen Personen, ergeben sich aus <näher zu spezifizieren, z.B.: dem Hauptvertrag, Anlage XY etc.>
Art, Umfang und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag und der vorliegenden Vereinbarung (siehe insbesondere die Präambel).

Im Zuge der Leistungserbringung durch den Auftragnehmer unter dem Hauptvertrag verpflichtet sich der Auftragnehmer die folgenden datenschutzrechtlichen und datensicherheitstechnischen Bestimmungen einzuhalten:

1. Diese Vereinbarung tritt mit Beauftragung gemäß Hauptvertrag in Kraft und gilt für die gesamte Dauer der aufrechten Vertragsbeziehung zur Erbringung der Leistungen gemäß dem Hauptvertrag, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.
2. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er bei der Verarbeitung personenbezogener Daten alle anwendbaren Datenschutz- und Datensicherheitsbestimmungen, insbesondere jedoch nicht abschließend, die

Datenschutz-Grundverordnung (DSGVO) und das österreichische Datenschutzgesetz (DSG) einhält.

3. Bei Vorliegen der Voraussetzungen des Art 37 DSGVO ist der Auftragsverarbeiter (zumindest) für die Laufzeit dieser Vereinbarung verpflichtet, einen Datenschutzbeauftragten bestellen. Der Auftragsverarbeiter hat insbesondere sicherzustellen, dass der Datenschutzbeauftragte an allen Angelegenheiten, die den Datenschutz betreffen, ordnungsgemäß und frühzeitig beteiligt ist und dieser seinen Aufgaben gemäß Art 39 nachkommen kann. Der Auftragsverarbeiter teilt dem Auftraggeber die nach Art. 37 Abs. 7 DSGVO veröffentlichten Kontaktdaten des Datenschutzbeauftragten sowie den Link zur Veröffentlichung mit.
4. Der Auftragsverarbeiter führt ein Verzeichnis aller Verarbeitungstätigkeiten für den Auftraggeber gemäß Art. 30 Abs. 2 DSGVO. Der Auftraggeber stellt dem Auftragsverarbeiter auf Anfrage für diesen Zweck die relevanten Auszüge aus seinem Verzeichnis von Verarbeitungstätigkeiten in digitaler Form (PDF) zur Verfügung. Der Auftragsverarbeiter stellt sein Verzeichnis von Verarbeitungstätigkeiten auf Anfrage der Aufsichtsbehörde zur Verfügung (Art 30 Abs 4 DSGVO).
5. Pflichten, die sich nicht bereits aus dem Hauptvertrag oder dem objektiven Recht ergeben, hat der Auftraggeber durch gesonderte „Weisungen zur Datenverarbeitung“ in Anlage 2 auszudrücken, welche vom Auftragsverarbeiter einzuhalten sind. Der Auftraggeber kann alle Weisungen jederzeit durch eine entsprechende Mitteilung ändern oder ersetzen. Falls der Auftraggeber mündlich spezifische Weisungen zur Datenverarbeitung erteilt, müssen diese anschließend in Textform (z.B. per E-Mail) bestätigt werden.
6. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person dürfen Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der dokumentierten Aufträge und Weisungen des Auftraggebers verarbeiten und übermitteln, außer es liegt ein Ausnahmefall gemäß Art 28 Abs 3 lit a DSGVO (gesetzliche Verpflichtung des Auftragsverarbeiters) vor. Im letzteren Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt (Art. 28 Abs 3 letzter Satz DSGVO).
7. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Wahrung des Datengeheimnisses im Sinne des Art. 28 Abs. 3 lit. b DSGVO und § 6 österreichisches Datenschutzgesetz nachweislich verpflichtet hat und diese auf die strafrechtlichen Konsequenzen eines Verstoßes hingewiesen worden sind. Kopien dieser Verpflichtungserklärungen sind auf

formloses Ersuchen unverzüglich dem Auftraggeber zu übermitteln. Insbesondere bleibt die Verschwiegenheitsverpflichtung des Auftragsverarbeiters und der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht. Der Auftragsverarbeiter ist zudem verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäfts- und Betriebsgeheimnissen sowie Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln.

8. Alle dem Auftragsverarbeiter unterstellten Personen, die mit der Verarbeitung personenbezogener Daten im Verantwortungsbereich des Auftraggebers betraut sind, müssen im Hinblick auf Datenschutz, Datensicherheit und Vertraulichkeit angemessen geschult sein. Der Auftragsverarbeiter hat die erforderlichen Schritte zu unternehmen, um sicherzustellen, dass die ihm unterstellten Personen, die Zugang zu personenbezogenen Daten haben, diese nur gemäß den Weisungen des Auftraggebers verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet (Art 32 Abs 4 DSGVO).
9. Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er ausreichende technische und organisatorische Maßnahmen im Sinne des Art. 32 DSGVO ergriffen hat, um ein dem Risiko angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten zu erreichen und um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden. Zum Beleg der Einhaltung von technischen und organisatorischen Maßnahmen können vorhandene, gültige Zertifizierungen nach ISO 27000, ISO 29134, BSI-Grundschutz, CNIL oder ähnliche dienen, die dem Auftraggeber vor Unterzeichnung der vorliegenden Vereinbarung vorzulegen und welche als Anlage der Vereinbarung anzuschließen sind. Bei Fehlen entsprechender Zertifikate und Testate sind ausführliche Dokumentationen der getroffenen technischen und organisatorischen Maßnahmen vorzulegen und als Anlage dieser Vereinbarung anzuschließen, welche die Einhaltung eines dem Risiko angemessenen Schutzniveaus belegen.
10. Der Auftragsverarbeiter darf ein anderes Unternehmen als weiteren Auftragsverarbeiter nach Art. 4 Abs. 8 DSGVO nur dann heranziehen, wenn der Auftraggeber dem schriftlich zustimmt (Art. 28 Abs. 2 DSGVO). Der Auftragsverarbeiter muss mit dem Sub-Auftragsverarbeiter einen Vertrag im Sinne des Art. 28 Abs. 4 DSGVO abschließen. In diesem Vertrag hat der Auftragsverarbeiter sicherzustellen, dass der Sub-Auftragsverarbeiter nachweislich dieselben Verpflichtungen eingeht, die dem Auftragsverarbeiter auf Grund der DSGVO, dem DSG sowie dieser Vereinbarung und der zugrunde liegenden Beauftragung obliegen, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den

gesetzlichen Bestimmungen erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters (Art 28 Abs. 4 letzter Satz DSGVO).

11. Der Auftragsverarbeiter hat dem Auftraggeber unverzüglich alle erforderlichen Informationen zum Nachweis der Einhaltung seiner rechtlichen (insbesondere gem. DSGVO und DSG) und vertraglichen Pflichten zur Verfügung zu stellen. Der Auftragsverarbeiter trägt insbesondere für die technischen und organisatorischen Voraussetzungen Vorsorge, dass der Auftraggeber die Rechte betroffener Personen gemäß Art 12 bis 23 DSGVO (Auskunftsrecht, Recht auf Berichtigung, Recht auf Löschung etc.) gegenüber den betroffenen Personen innerhalb der gesetzlichen Fristen rechtskonform erfüllen kann. Für den Fall, dass sich eine betroffene Person direkt an den Auftragsverarbeiter zwecks Geltendmachung seiner Rechte wenden sollte, hat der Auftragsverarbeiter ihr Begehren unverzüglich an den Auftraggeber weiterzuleiten. Dem Auftragsverarbeiter ist es untersagt, der betroffenen Person nähere Informationen über die Datenverarbeitung des Auftraggebers zu erteilen, ausgenommen davon ist die Nennung des Namens und der Kontaktdaten des Auftraggebers..
12. Der Auftragsverarbeiter ist gemäß Art. 28 Abs. 3 lit. g DSGVO nach Beendigung der Verarbeitungsleistungen verpflichtet, nach Wahl des Auftraggebers alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben bzw. in dessen Auftrag für ihn weiter vor unbefugter Einsicht gesichert aufzubewahren oder (nach vorheriger Zustimmung des Auftraggebers) zu vernichten, sofern nicht nach dem Unionsrecht oder dem für den Auftragsverarbeiter geltenden nationalen Recht eine Verpflichtung zur weiteren Speicherung der personenbezogenen Daten besteht. Das Protokoll der Löschung (Vernichtung) ist auf Anforderung dem Auftraggeber unverzüglich vorzulegen. Wenn der Auftragsverarbeiter die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung seiner Verarbeitungsleistungen entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten erhalten hat oder in einem anderen, gängigen Format (für den Auftraggeber kostenfrei) herauszugeben.
13. Der Auftragsverarbeiter verpflichtet sich, bei der elektronischen Übermittlung von Daten technische Verfahren mit Authentifikation und Verschlüsselung nach den üblichen Sicherheitsstandards unter besonderer Berücksichtigung der Vorgaben nach Art. 32 DSGVO anzuwenden.
14. Sollte für die Auftragsverarbeitung eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO nötig sein, verpflichtet sich der Auftragsverarbeiter dem Auftraggeber alle für die Erstellung der DSFA erforderlichen Informationen zeitgerecht zur Verfügung zu

stellen. Der Auftragsverarbeiter verpflichtet sich, den Auftraggeber bei der Einhaltung der übrigen in den Art 32, 33, 34 und 36 DSGVO genannten Pflichten zu unterstützen und dem Auftraggeber dafür alle erforderlichen Informationen unverzüglich zu übermitteln.

15. Der Auftragsverarbeiter setzt geeignete technische und organisatorische Maßnahmen um, die sicherstellen, dass die Verarbeitung gemäß der Datenschutz-Grundverordnung erfolgt. Der Auftragsverarbeiter ist verpflichtet dem Auftraggeber einen entsprechenden Nachweis gemäß Art. 24 Abs. 1 vor Beginn der Verarbeitungstätigkeit zur Verfügung zu stellen.
16. Der Auftragsverarbeiter verpflichtet sich, geeignete technische und organisatorische Maßnahmen, wie Datenschutz durch Technikgestaltung und datenschutzrechtliche Voreinstellungen zu treffen, sowie Garantien in die Verarbeitung mitaufzunehmen, die sicherstellen, dass die Vorgaben des Art. 25 DSGVO eingehalten werden.
17. Der Auftragsverarbeiter übermittelt dem Auftraggeber vor Beginn der Verarbeitungstätigkeit alle Nachweise über eingehaltene Verhaltensregeln nach Art. 40 DSGVO, sowie erlangte Zertifikate nach Art. 42 DSGVO, welche die beauftragte Verarbeitungstätigkeit betreffen, zur Erstellung der Risikoabschätzung gemäß Art. 32 Abs. 1 DSGVO.
18. Für die IT-Systeme des Auftragsverarbeiters sind weiters die einschlägigen Vorgaben des Österreichischen Informationssicherheitshandbuches in der geltenden Fassung anzuwenden. So die Daten nicht auf der vom Auftraggeber bereitgestellten Server-Infrastruktur gehostet werden, ist nachzuweisen, dass die für den Betrieb herangezogenen Server-infrastruktur jedenfalls eine gültige Zertifizierung nach ISO 27001 oder gleichwertig besitzen.
19. Der Auftragsverarbeiter verpflichtet sich, Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 oder Art. 34 DSGVO unverzüglich schriftlich an den Auftraggeber, sowie per E-Mail an den Datenschutzbeauftragten des Auftraggebers unter datenschutz@bmbwf.gv.at zu melden.
20. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz, die Einhaltung der zwischen den Vertragsparteien getroffenen vertraglichen Regelungen sowie die Einhaltung der Weisungen des Auftraggebers durch den Auftragsverarbeiter jederzeit im erforderlichen Umfang zu kontrollieren bzw. durch im Einzelfall zu benennende, sachverständige Dritte (mit oder ohne Beisein des Auftraggebers) kontrollieren zu lassen. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen nach Art. 28 Abs. 3 lit. h DSGVO eingeräumt. Der Auftraggeber kann dazu die Kontrolle in der Betriebsstätte des

Auftragsverarbeiters zu den jeweils üblichen Geschäftszeiten vornehmen bzw. vornehmen lassen.

21. Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber unverzüglich von jedem Verstoß des Auftragsverarbeiters, seiner betrauten Mitarbeiter oder Dritter gegen anwendbare Datenschutzvorschriften oder in dieser Vereinbarung getroffene Pflichten und Weisungen in Kenntnis zu setzen. Der Auftragsverarbeiter trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
22. Der Auftragsverarbeiter ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber gemäß Art 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende (geplante) Maßnahmen vom Auftragsverarbeiter zu informieren.
23. Der Auftragsverarbeiter verpflichtet sich, die Datenverarbeitung im Auftrag ausschließlich in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Jedwede, sei es auch nur eine teilweise, Erbringung der Datenverarbeitung in einem Drittland bedarf der vorherigen ausdrücklichen Zustimmung des Auftraggebers. Sofern der Auftraggeber einer Erbringung der Datenverarbeitung in einem Drittland zugestimmt hat, darf diese nur dann erfolgen, wenn alle gesetzlichen und vertraglichen Voraussetzungen nachweislich erfüllt sind.
24. Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren.
25. Die Vertragsparteien schließen die Anwendung etwaiger im Hauptvertrag enthaltener Haftungsprivilegierungen bzw.- -beschränkungen zugunsten des Auftragsverarbeiters auf datenschutzrechtliche Verstöße ausdrücklich aus.
26. Änderungen und Ergänzungen zu diesem Vertrag bedürfen der Schriftform. Gleiches gilt für die Vereinbarung, vom Erfordernis der Schriftform abzugehen. Die dieser Vereinbarung beigefügten Anhänge bilden einen integrierenden Vertragsbestandteil.
27. Diese Vereinbarung unterliegt dem österreichischen Recht sowie dem sachlich anwendbaren Unionsrecht. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und in Zusammenhang mit dieser Vereinbarung ist Wien, Österreich.
28. Diese Vereinbarung wird in zwei (2) Originalen ausgefertigt, von welchen jede Vertragspartei ein Original erhält.

Für den Auftraggeber:	Für den Auftragnehmer:
Unterschrift:	Unterschrift:
Name:	Name:
Funktion:	Funktion:
Datum:	Datum:

ANLAGEN

Anlage 1

Technische und organisatorische Maßnahmen des Auftragsverarbeiters

<Führen Sie im Folgenden die jeweils getroffenen technischen und organisatorischen Maßnahmen an bzw. legen Sie die Dokumentation darüber bei.>

Anlage 2

Weisungen zur Datenverarbeitung

********* TEXTENDE *********

B. Mustervereinbarung: Schule – Erziehungsberechtigte

„Ich, xxx (*Name, Adresse)* stimme zu, xxx
dass meine persönlichen Daten, - ODER , dass die personenbezogenen Daten meines xxx, Name xxx,
nämlich [Datenarten aufzählen, zB Name, Adresse, Geburtsdatum …]
zum Zweck der
[genauen Zweck anführen,]

verarbeitet werden und

an
[Anführung des/der genauen Übermittlungsempfänger(s), zB XY GmbH]
zum Zweck der [genauer Übermittlungszweck] übermittelt werden.

Diese Einwilligung kann ich jederzeit schriftlich mittels Brief an die Schulleitung(Name der Schule, Adresse) widerrufen.

C. D A T E N S C H U T Z I N F O R M A T I O N gemäß Artt 12ff DSGVO im Rahmen der Schulverwaltung an österr. Schulen gemäß Art. 14 B-VG

Verarbeitungstätigkeit

Datenverarbeitungen, die im Vollzug des Schulrechts erfolgen. (siehe hier insbesondere Anlage 1, 1a und 2 Bildungsdokumentationsgesetz), sowie Serviceleistungen auf Schülerwunsch (zB Kopiersystem, Essensbestellung)

Verantwortlicher

Generell Angaben zur jeweiligen Schulleitung gemäß § 2 Abs. 3 Bildungsdokumentationsgesetz

Bei Veröffentlichung auf Schulhomepage, hier Namen und Kontaktdaten des Schulleiters / der Schulleiterin eintragen

Kontaktinformationen finden sich für alle österr. Schulen gem. Art. 14 B-VG im offiziellen Schulverzeichnis www.schulen-online.at

Kontaktdaten des Datenschutzbeauftragten (sofern vorhanden)

An den Landesschulräten ist für Bundesschulen, sowie für Pflichtschulen, sofern es sich um Bundesvollzug handelt, ein Datenschutzbeauftragter für das jeweilige Bundesland eingerichtet.. Die Liste der Datenschutzbeauftragten in den Landesschulräten sowie für Zentrallehranstalten und Pädagogische Hochschulen finden Sie unter: https://bildung.bmbwf.gv.at/ministerium/datenschutz/index.html

Rechtsgrundlage und Zwecke der Datenverarbeitungen an österr. Schulen

- Alle schulgesetzlichen Verpflichtungen, die für die Wahrnehmung von Aufgaben erforderlich sind, die im öffentlichen Interesse liegen (Art 6 (1) lit e DSGVO bzw die zur Erfüllung einer rechtlichen Verpflichtung im Zuge der Schulverwaltung (Art 6 (1) lit c DSGVO erforderlich sind. (siehe hier insbesondere Anlage 1, 1a und 2 Bildungsdokumentationsgesetz). Hier besteht auf Grund des Schulrechts die gesetzliche Verpflichtung der Schüler/innen bzw. Erziehungsberechtigten zur Bereitstellung der erforderlichen personenbezogenen Daten.
- Serviceleistungen auf Schülerwunsch (zB Kopiersystem, Essensbestellung, Bereitstellung von edu.Lizenzen) sowie Öffentlichkeitsarbeit der Schule (zB Fotos von Schüler/innen bei Schulveranstaltungen) gemäß Art 6 (1) lit a oder c. Soweit die

Datenverarbeitung auf Einwilligung beruht besteht das jederzeitige Recht auf Widerruf gemäß Art 7 DSGVO.

- Weitergabe von Daten im Notfall - zB Übergabe der Kontaktdaten der Eltern eines Schülers bei Verletzung an die Rettung – (Art 6 (1) lit d

Datenkategorien

Die Aufzählung der für die Vollziehung des Schulrechts zu verarbeitenden Datenkategorien ist in §§ 3ff in Verbindung mit den Anlagen des Bildungsdokumentationsgesetzes gesetzlich geregelt. Generell werden im Rahmen der Schulverwaltung Daten nur bei den Schüler/innen bzw. Erziehungsberechtigten selbst erhoben.

Übermittlung und Empfänger

Gesetzliche Regelungen:

- Zuständiger Bundesminister zur Führung der Gesamtevidenzen (im Wege über die Bundesanstalt „„Statistik Österreich“„) und der Evidenz über den Personal-, Betriebs- und Erhaltungsaufwand der Bildungseinrichtung;
- Bundesanstalt „„Statistik Österreich“„
- Stammzahlenregisterbehörde im Rahmen ihrer Befugnisse nach dem E-Government-Gesetz.

Auf Grund der Einwilligung der Schüler/innen bzw Erziehungsberechtigten

- Verkehrsverbünde im Zuge der Schülerfreifahrt
- Alumni-Verbände an Schulen, Elternvereine
- IT-Dienstleister (zB zum Nachweis der Berechtigung des Bezugs verbilligter Edu-Lizenzen
- etc

Übermittlung in Drittländer oder Internationale Organisationen

Im Zuge der Schulverwaltung an österr. Schulen erfolgt grundsätzlich keine Datenübermittlung an Staaten außerhalb der EU. Für Datenübermittlungen im Bereich der österr. Auslandsschulen sind die Bestimmungen in den jeweiligen völkerrechtlichen Verträgen nach Maßgabe der Grundsätze der DSGVO anzuwenden. Datenübermittlungen im Zuge des internationalen Schüleraustausches (zB Erasmus) beruhen prinzipiell auf Einwilligung.

Eventuell Daten von Schülertestungen an OECD

Speicherdauer

Durch die jeweiligen gesetzlichen Materienbestimmungen vorgegeben (siehe etwa: § 77 SchUG zum Klassenbuch, § 77a SchUG zur Aufbewahrung von [Prüfungs]protokollen und Aufzeichnungen)

Rechte des Betroffenen

Die Rechte des Betroffenen müssen gegenüber dem Verantwortlichen geltend gemacht werden . Dies ist gemäß § 2 Abs. 3 Bildungsdokumentationsgesetz der jeweilige Schulleiter. Kontaktinformationen finden sich für alle österr. Schulen gem. Art. 14 B-VG im offiziellen Schulverzeichnis www.schulen-online.at.

- Soweit die Datenverarbeitung auf Einwilligung beruht besteht das jederzeitige Recht auf Widerruf gemäß Art 7 DSGVO.
- Eine betroffene Person das Recht, Auskunft darüber zu verlangen, ob personenbezogene Daten von ihm verarbeitet werden. (Art 15 DSGVO)
- Eine betroffene Person hat das Recht, unverzüglich die Berichtigung unrichtiger personenbezogener Daten oder deren Vervollständigung zu verlangen. (Art 16 DSGVO)
- Eine betroffene Person hat das Recht, zu verlangen, dass die personenbezogenen Daten unverzüglich gelöscht werden, soferne die in Art 17 Abs 1 DSGVO genannten Gründe erfüllt sind. (Art 17 DSGVO)
- Eine betroffene Person hat das Recht, zu verlangen, dass die Verarbeitung der personenbezogenen Daten eingeschränkt wird, soferne die in Art 18 Abs 1 DSGVO genannten Gründe erfüllt sind. (Art 18 DSGVO)
- Eine betroffene Person hat das Recht, seine personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, sofern die Datenverarbeitung auf einer Einwilligung oder einem Vertrag beruht und mithilfe automatisierter Verfahren erfolgt (Art 20 DSGVO).
- Eine betroffene Person hat das Recht, jederzeit gegen die Verarbeitung seiner personenbezogenen Daten Widerspruch einzulegen, soferne der Verantwortliche nicht zwingende schutzwürdige Gründe für die Verarbeitung nachweist (zB Gesetzesvollzug), die die Interessen, Rechte und Freiheiten der Betroffenen Person überwiegen (Art 21 DSGVO)

Automatisierte Entscheidungsfindung

Im Bereich der Schulverwaltung sowie Leistungsbeurteilung finden keine automatisierten Entscheidungsfindungen einschließlich Profiling statt, die dem Betroffenen gegenüber rechtliche Wirkung entfaltet oder diesen in ähnlicher Weise erheblich beeiträchtigt.

Aufsichtsbehörde

Österreichische Datenschutzbehörde

www.dsb.gv.at

Telefon: +43 1 52 152-0

E-Mail: dsb@dsb.gv.at

Beschwerderecht (Art 77 DSGVO)

Eine betroffene Person hat das Recht auf Beschwerde bei der Aufsichtsbehörde, wenn er der Ansicht ist, dass die Verarbeitung der ihn betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.

********* TEXTENDE *********

5. Checkliste

CHECKLISTE

Wenn in der Schülerverwaltung personenbezogene Daten verwendet werden sind folgende Fragen zu beantworten:

- ✓ Wer ist datenschutzrechtlich Verantwortlicher?
  - ☐ Schulleitung ☐ BMBWF ☐ Anderer: _____
- ✓ Wer sind die betroffenen Personen?
  - ☐ Schülerinnen und Schüler ☐ Lehrerinnen und Lehrer
  - ☐ Erziehungsberechtigte ☐ Andere: _____
- ✓ Welche personenbezogenen Daten werden verwendet?
  - ☐ Namen ☐ Adresse ☐ Bildnis
  - ☐ Andere: _____
    _____
    _____
- ✓ Werden besonderen Kategorien personenbezogenen Daten verwendet?
  - ☐ Nein ☐ Ja
  - Wenn ja, welche?
    - ☐ ethnische/rassische Herkunft
    - ☐ religiöse/philosophische Überzeugung
    - ☐ Gesundheit/Sexualleben
    - ☐ Andere (politische Meinung, Gewerkschaftszugehörigkeit)
- ✓ Zu welchem Zweck werden die personenbezogenen Daten verwendet?
  - ☐ Aufnahme in die Schule ☐ Prüfung
  - ☐ Schulveranstaltung ☐ Anderer: _____
- ✓ Wie werden die personenbezogenen Daten verwendet?

☐ Erfassen von neuen Daten ☐ Verändern
☐ Abfragen/Benützen ☐ Verknüpfen
☐ Löschen/Vernichten ☐ Anders: _____

✓ Werden die personenbezogenen Daten weitergegeben?
☐ Nein ☐ Ja
Wenn ja, an wen?
☐ Übermittlung an Dritte: _____
Wenn Dritte, auf welcher Grundlage?
_____
☐ Überlassung an Auftragsverarbeiter:
_____
Wenn Auftragsverarbeiter, wurde eine Dienstleistungsvereinbaung abgeschlossen?
☐ Ja ☐ Nein

✓ Ist die Verarbeitung erforderlich bzw. verhältnismäßig? Wieso ist die Verarbeitung das gelindeste Mittel?
☐ Begründung: _____
_____

✓ Auf welcher rechtlichen Grundlage werden die personenbezogenen Daten verwendet?
☐ Explizite gesetzliche Grundlage:
☐ BilDokG ☐ SchUG ☐ Andere
Konkrete Bestimmung nennen: _____
☐ Implizite gesetzliche Grundlage (, da Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt); welche gesetzlich vorgesehene Aufgabe?
☐ SchUG ☐ Andere
Konkrete Bestimmung nennen: _____
☐ Einwilligung:
Schriftliche Einwilligung der Betroffenen eingeholt? ☐ Ja ☐ Nein
☐ bis 14. Lbj. Erziehungsberechtigte
☐ ab Vollendung des 14. Lbj. Schülerinnen und Schüler
☐ Lebenswichtiges Interesse (Medizinischer Notfall)

☐ Andere rechtliche Grundlage: _____