BM BF
Bundesministerium für
Bildung und Frauen

efit 21
digitale bildung

Datenschutz für die digitale Schülerverwaltung

Datenschutz für die digitale Schülerverwaltung

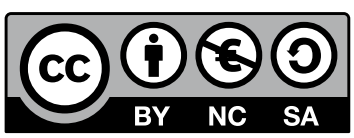
Priv.-Doz. Dr. Konrad Lachmayer
in Zusammenarbeit mit
Dr. Thomas Menzel

Projekt des Bundesministeriums für Bildung und Frauen

Wien, 2015

Impressum

Medieninhaberin, Verlegerin und Herausgeberin:
Bundesministerium für Bildung und Frauen
Minoritenplatz 5, 1014 Wien
Tel.: +43 1 531 20-0
www.bmbf.gv.at
Inhalt/Autoren: Priv.Doz. Dr. Konrad Lachmayer, Dr. Thomas Menzel
Grafiken: Priv.Doz. Dr. Konrad Lachmayer
Grafische Gestaltung: BKA | ARGE Grafik
Cover: BMBF
Druck: BMBF
Wien, Mai 2015



Inhalt

Management Summary

Datenschutz als gesetzliche Rahmenbedingung der Schülerverwaltung

- Das Datenschutzgesetz (DSG) regelt neben dem Grundrecht auf Datenschutz und dem Rechtsschutz die zentralen Begriffe und die wichtigsten Prinzipien des Datenschutzrechts. Das DSG beinhaltet konkrete Vorgaben, wann personenbezogene Daten verwendet werden können; es sieht Datensicherheitsmaßnahmen, Dokumentations- und Protokollierungsvorschriften ebenso wie ein Registrierungsverfahren vor. Gem. § 3 BilDokG ist die Schulleitung Auftraggeber im Sinne des Datenschutzgesetzes.
- Die zentralen datenschutzrechtlichen Begriffe sind »personenbezogene Daten«, »sensible Daten« , »Auftraggeber«, »Betroffener«, »Dienstleister« sowie das »Verwenden von Daten«, das »Verarbeiten von Daten« und das »Übermitteln von Daten«.
- Die wichtigsten datenschutzrechtlichen Prinzipien sind »Treu und Glauben«, die »Zweckbindung« und die »Verhältnismäßigkeit«.
- Neben den Bestimmungen 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.
- Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten werden gem §8 DSG nicht verletzt, wenn eine ausdrückliche gesetzliche Ermächtigung besteht, die Betroffenen der Datenverwendung zugestimmt haben oder lebenswichtige Interessen der Betroffenen die Verwendung erfordern.
- Auch wenn keine explizite gesetzliche Ermächtigung zur Verwendung 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 Zustimmung ist eine wichtige Möglichkeit der datenschutzrechtlich zulässigen Verwendung personenbezogener Daten. Dabei ist zu beachten, dass die Zustimmung von jedem/jeder einzelnen Schüler bzw. Schülerin einzuholen ist, dass die Zustimmung freiwillig erfolgt, und wer die Zustimmung 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 Maßnahmen zur Datensicherheit (§14 DSG), die Meldepflicht einer Datenanwendung gem. §§17 ff DSG (siehe aber die Ausnahme für Standardanwendungen für die Schülerverwaltung) und die Meldung von Datenmissbrauch *(Data Breach Notification)*.

Grundrecht auf Datenschutz

- Die **österreichische Verfassung** gewährt Betroffenen ein Grundrecht auf Datenschutz. Dies bedeutet, dass die Verwendung personenbezogener Daten nur unter bestimmten Voraussetzungen möglich ist. Liegen die Voraussetzungen nicht vor, bedeutet dies eine

Verletzung des Grundrechts auf Datenschutz.

- Die Verwendung personenbezogener Daten muss verhältnismäßig erfolgen. Dies bedeutet, dass die Datenverwendung zur Erfüllung der Aufgaben notwendig ist.
- Die Schulleitung ist verpflichtet, das Grundrecht auf Datenschutz zu gewährleisten. Die aus dem Grundrecht auf Datenschutz erfließenden Rechte der betroffenen Schülerinnen und Schüler sind das Recht auf Geheimhaltung, das Recht auf Auskunft sowie die Rechte auf Richtigstellung und Löschung.
- Die Betroffenen können ihre Rechte, wenn ihnen diese nicht durch die Schulleitung gewährt werden, mittels Beschwerde bei der unabhängigen Datenschutzbehörde geltend machen.

Besondere datenschutzrechtliche Fragestellungen in der Schülerverwaltung

- Die digitale Schülerverwaltung führt zu einer neuen Systemarchitektur an den Schulen. Die datenschutzrechtlichen Verpflichtungen des Schulleiters/der Schulleiterin als Auftraggeber bleiben bestehen. Die Datenerfassung beruht auf den expliziten datenschutzrechtlichen Bestimmungen des SchUG und des BilDokG sowie auf den schulrechtlichen Regelungen des SchUG, soweit die Datenverwendung 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 Zustimmung der Betroffenen beruht.
- Im Rahmen des BilDokG bestehen unterschiedliche datenschutzrechtliche Schnittstellen zwischen der Schulleitung und dem BMBF bzw. den LSR. Hervorzuheben ist die Erstellung von Gesamtevidenzen, etwa auch der Schülerinnen und Schüler gem §5 BilDokG. Hier werden nur indirekt personenbezogene 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. In diesem Fall findet sich eine datenschutzrechtliche Grundlage nicht nur in der Zustimmung des Betroffenen, sondern auch in den einschlägigen Bestimmungen des SchUG (§§3 ff, 22, 56, 61, 77 SchUG).
- Das elektronische Klassenbuch basiert auf den Bestimmung der §§77, 56, 54 SchUG. Aus datenschutzrechtlicher Sicht bestehen Determinierungsfragen in Hinblick auf den Eintrag von besonderen Vorkommnissen.
- Die edu.card ist derzeit gesetzlich nicht verpflichtend vorgesehen. Insoweit bleibt die Verwendung der edu.card generell von der Zustimmung der Schülerinnen und Schüler bzw. der Erziehungsberechtigten abhängig.
- Weitere Fragestellungen ergeben sich in Hinblick auf den Umgang mit der Videoüberwachung, einer allfälligen Dienstleistungsvereinbarung, dem Schutz des persönlichen Bildnisses und einer Internet-Policy für Schulen.

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[1] bedeutet aber auch die zunehmende Verwendung von personenbezogenen Daten, vor allem von Schülerinnen und Schülern. **Die Verwendung 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-KustodInnen und SystembetreuerInnen und generell für alle Lehrerinnen und Lehrer stellen sich zahlreiche, immer komplexer werdende Fragen der Verwendung personenbezogener Daten in der Schule.

Diesem Bedarf nach Antworten bzw. Richtlinien **für datenschutzkonforme Verwendung 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 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 Auftraggeber, Zweckbindung des Datenschutzrechts, Besonderheit sensibler Daten, BilDokG etc.).

Über diese allgemeinen Grundlagen hinaus werden im zweiten Teil **spezielle datenschutzrechtliche Fragestellungen** aus dem **schulischen Alltag** behandelt. Insbesondere wird auf die digitale Schülerverwaltung sowie datenschutzrechtliche Fragen des Schulwechsels, des elektronischen Klassenbuches, der Dienstleistungsvereinbarung, 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 Verwendung personenbezogener Daten sowie Auszüge aus Gesetzen und Verordnungen zur Verfügung gestellt.

1 Grundlegend dazu der Erlass des BMBF: Digitale Kompetenz – IT-Einsatz und Internet Policy an Österreichs Schulen, download unter: https://www.bmbf.gv.at/schulen/efit21/web20/dig_erlass_bl1_20117.pdf?4du4y2

I. Allgemeine datenschutzrechtliche Grundlagen für die Schülerverwaltung

1. Datenschutz als gesetzliche Rahmenbedingung der Schülerverwaltung

A. Überblick

Das **Datenschutzgesetz** setzt – neben den grundrechtlichen Rahmenbedingungen – **zentrale Vorgaben** für das Verwenden personenbezogener Daten für die Schülerverwaltung. Ausgangspunkt sind die durch das DSG vorgesehenen Begriffe gem §4 DSG (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 Datenverwendung etwa auch die Zustimmung, die Datensicherheit, das Registrierungsverfahren oder die sog. Data Breach Notification betreffen.

Über die Bestimmungen des 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 politischen Debatten auf europäischer Ebene gesehen werden. Die EU Kommission hat bereits Anfang 2012 einen Entwurf für eine europäische Datenschutz-Grundverordnung vorgestellt. Sollte die Diskussion zwischen Rat der EU und dem Europäischen Parlament zu einem positiven Abschluss führen, so ist in den nächsten 2–3 Jahren mit einem völlig neuen Datenschutzrecht zu rechnen, das sodann auf europäischer Ebene die Details des Datenschutzes auch für Österreich bzw. die österreichische Schülerverwaltung vorgibt. Mit der Beschlussfassung würde das österreichische DSG außer Kraft treten bzw. nur mehr Details zu den europäischen Vorgaben wiedergeben können. Es ist also von einer großen Reform des Datenschutzrechts in den nächsten Jahren auszugehen.

B. Zentrale datenschutzrechtliche Begriffe

§4 DSG definiert die wichtigsten Begriffe des Datenschutzrechts. Die Begriffsbestimmungen sind allerdings zum Teil sehr kompliziert ausgefallen und verwirrend. Dennoch ist es wichtig, die zentralen Bestimmungen zu kennen.

Ausgangspunkt ist der Begriff der personenbezogenen Daten:

- **Personenbezogene Daten** sind Angaben über **Betroffene**, deren Identität bestimmt oder bestimmbar ist; »nur indirekt personenbezogen« sind Daten, wenn der Personenbezug der Daten derart ist, daß dieser **Auftraggeber** (Schulleiter/Schulleiterin, §3 BilDokG) die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.

Eine besondere Definition gibt es für besonders schutzwürdige Daten, die als sog. »sensible Daten« bezeichnet werden und an deren Verwendung das DSG höhere Anforderungen knüpft:

- **Sensible Daten** sind personenbezogene Daten in Bezug auf die rassische und ethnische **Herkunft**, politische **Meinung, Gewerkschaftszugehörigkeit**, religiöse oder philosophische **Überzeugung, Gesundheit** oder das **Sexualleben.**

Die zwei zentralen **Rollen** im Datenschutz sind der **Betroffene** und der **Auftraggeber:**

- **Betroffener** ist jede vom **Auftraggeber** verschiedene Person, deren Daten verwendet werden (primär also Schülerinnen und Schüler).
- **Auftraggeber** ist eine natürliche oder juristische **Person** oder ein **Organ** einer **Gebietskörperschaft** beziehungsweise die Geschäftsapparate solcher Organe, wenn sie alleine oder gemeinsam mit anderen die **Entscheidung getroffen** haben, **Daten zu verwenden** (**Schulleiter/Schulleiterin, §3 BilDokG**), unabhängig davon, ob sie die Daten selbst verwenden oder damit einen Dienstleister beauftragen.

An dieser Stelle kommt der sogenannte **Dienstleister** als weitere Rolle in 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).

- **Dienstleister** ist jede natürliche oder juristische Person, jedes Organ einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwendet (etwa Bundesrechenzentrum).

Neben den im Datenschutzrecht bestehenden Rollen werden auch die Handlungen definiert. **Überbegriff** ist das **Verwenden der Daten.** Dieses teilt sich in das **Verarbeiten von Daten** und das **Übermitteln von Daten:**

- **Verwenden von Daten** ist jede Art der Handhabung von Daten, also sowohl das Verarbeiten als auch das Übermitteln von Daten.
- **Verarbeiten von Daten:** das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns von Daten.
- **Übermitteln von Daten** ist die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, 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 Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers(!)
- **Überlassen von Daten** bedeutet die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses.

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

- Zustimmung ist die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt.

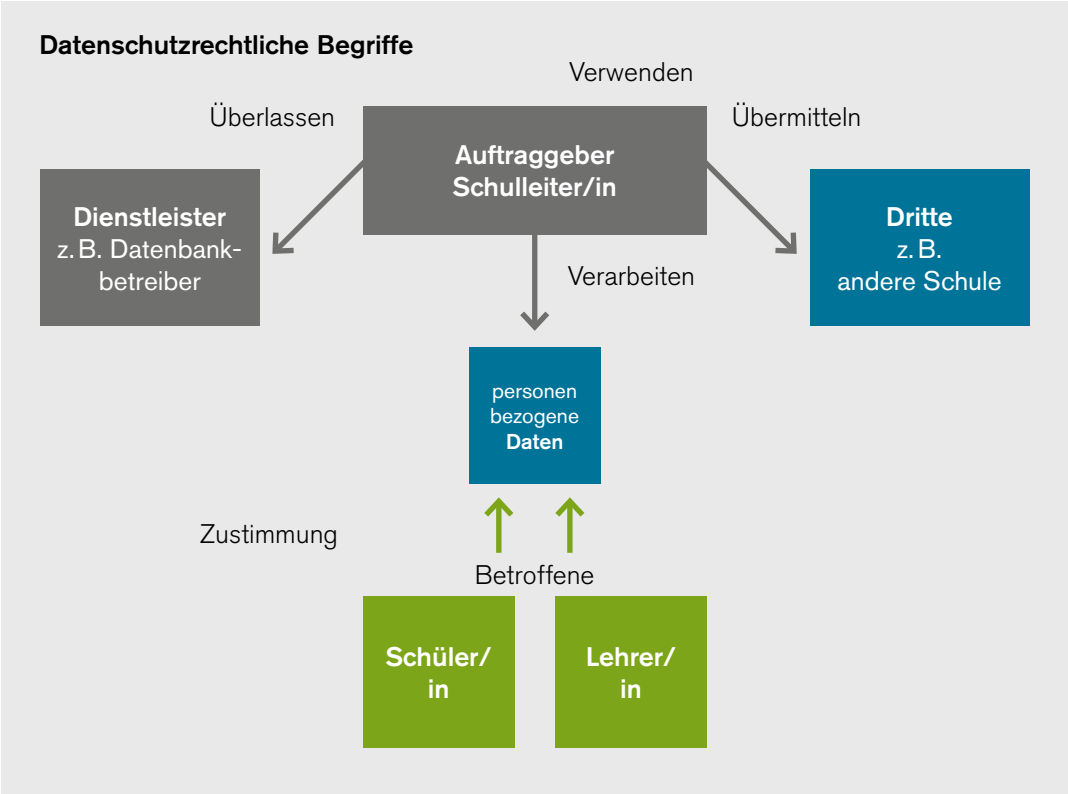


Abb. 1

C. Datenschutzrechtliche Prinzipien

Die **wichtigsten** datenschutzrechtlichen **Prinzipien** sind:

- **Verhältnismäßigkeit**
- **Zweckbindung**
- **Treu und Glauben**

Die **Verhältnismäßigkeit** der Datenverwendung verlangt, dass die Datenverwendung für den damit verfolgten Zweck geeignet und erforderlich ist. Die **Eignung** bezieht sich darauf, dass die Datenverwendung zur Erreichung des Zwecks der Datenverwendung beitragen können muss. Ist die Datenverwendung nicht geeignet, so ist sie auch nicht verhältnismäßig. Zentrales Kriterium ist die **Erforderlichkeit**. Ist die Datenverwendung wirklich notwendig, um den Zweck der Datenverwendung zu erreichen oder könnte dasselbe Ziel auch ohne die Verwendung personenbezogener Daten erreicht werden. Ist die Datenverwendung nicht erforderlich, so ist sie nicht verhältnismäßig. Die Erforderlichkeit ist auch zeitlich zu interpretieren; dies bedeutet: wie lange ist die Datenverwendung erforderlich und ab wann ist sie nicht mehr erforderlich.

Recht im Originaltext:
Zulässigkeit der Verwendung von Daten

§7 Abs 3 DSG: Die **Zulässigkeit** einer Datenverwendung setzt voraus, daß die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz **nur im erforderlichen Aus-**

maß und mit den **gelindesten** zur Verfügung stehenden **Mitteln** erfolgen und dass die Grundsätze des §6 eingehalten werden.

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

Zweckbindung ist ein fundamentaler Grundsatz des Datenschutzrechts. Dieser besagt, dass personenbezogene Daten nur »für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden« dürfen (§6 Abs 1 Z 2 DSG). 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 Datenverwendung 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.

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 Datenverwendung 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 Meldepflichten erfüllt.[2]

D. Datenschutzrechtliche Regeln

a. Die rechtlichen Rahmenbedingungen der Datenverwendung

Das **Datenschutzgesetz** regelt unter Verwendung der datenschutzrechtlichen Begriffe gem § 4 DSG und unter Heranziehung der datenschutzrechtlichen Prinzipien, wann personenbezogene Daten verwendet werden dürfen. Grundsätzlich wird zwischen Anforderungen für die **Datenverarbeitung** und die **Datenübermittlung** unterschieden (Begriffe siehe oben):

Recht im Originaltext:
Zulässigkeit der Verwendung von Daten

§7. (1) Daten dürfen nur **verarbeitet** werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.

(2) Daten dürfen nur **übermittelt** werden, wenn

1. sie aus einer gemäß Abs. 1 zulässigen Datenanwendung stammen und

2 *Jahnel*, Handbuch Datenschutzrecht (2010) Rz 4/99.

2. der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis … im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und

3. durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

Datenverwendung (= Datenverarbeitung + Datenübermittlung)

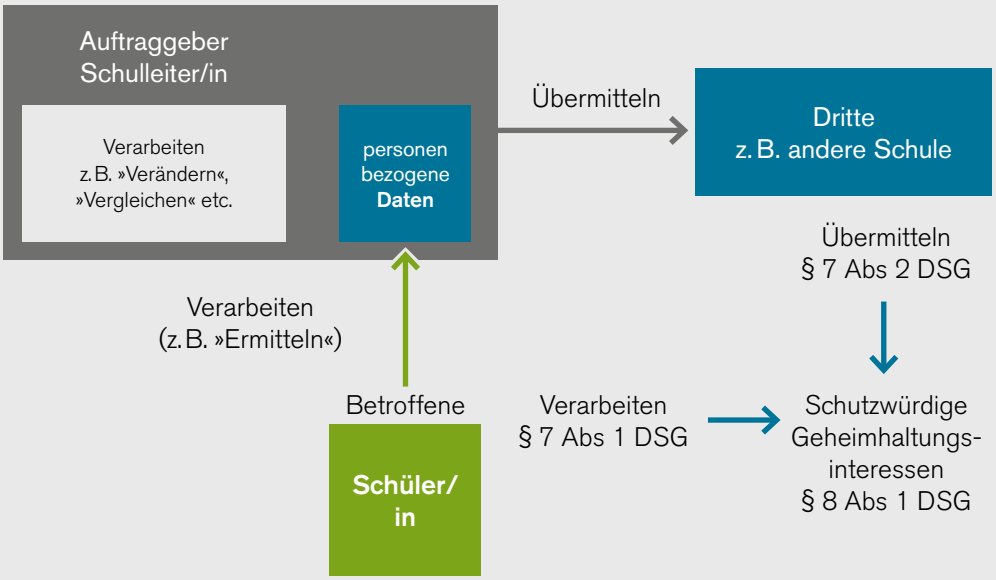


Abb. 2

Das Gesetz unterscheidet in weiterer Folge, ob eine Datenverwendung mit nicht-sensiblen Daten (Normalfall) oder mit sensiblen Daten (Politische Meinung, Religion, Gesundheit) erfolgt.

Schutzwürdige Geheimhaltungsinteressen bei **Verwendung nicht-sensibler Daten** werden gem § 8 DSG nicht verletzt, wenn

- eine **ausdrückliche gesetzliche Ermächtigung** zur Verwendung der Daten besteht oder
- der **Betroffene** der Verwendung seiner Daten **zugestimmt** hat, wobei ein **Widerruf jederzeit möglich** ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
- **lebenswichtige Interessen** des **Betroffenen** die Verwendung erfordern (akuter medizinische Notfall) oder
- **überwiegende berechtigte Interessen des Auftraggebers** (also des Schulleiters/der Schulleiterin) die Verwendung erfordern.

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

Frage: Wann ist die Datenverwendung 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 Datenverwendung 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 SchUG zu. § 56 SchUG 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 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.

Zulässige Verwendung personenbezogener Daten

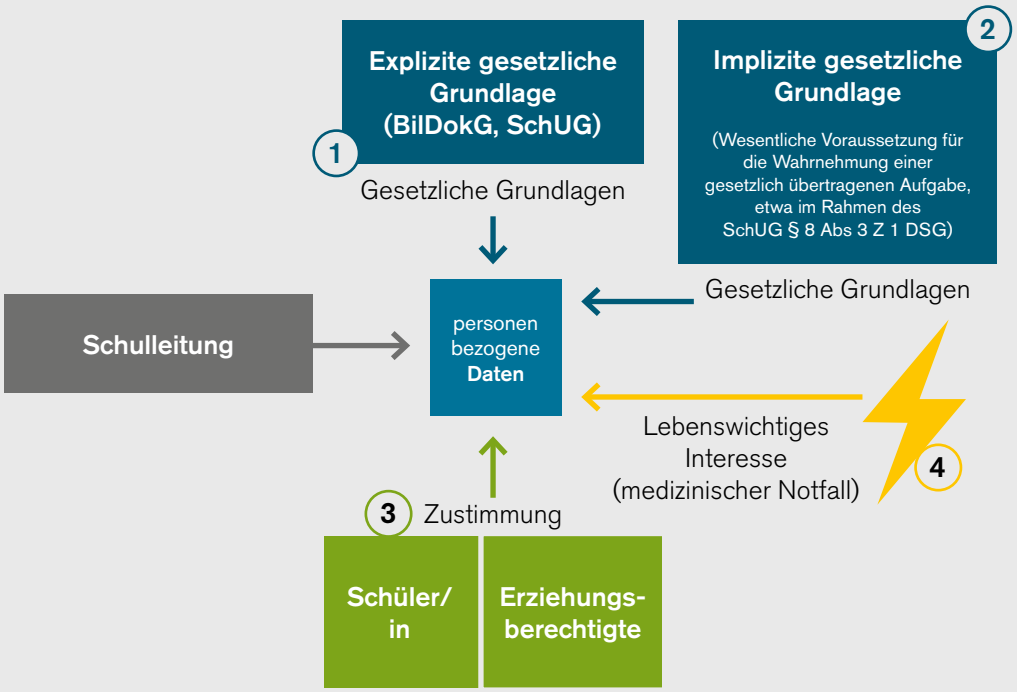


Abb. 3

Bei **sensiblen Daten** (politische Meinung, Religion, Gesundheit) sind die Vorgaben zwar ähnlich, im Detail aber **noch strenger**. Diese dürfen nur verwendet werden, wenn:

- der Betroffene die Daten offenkundig selbst öffentlich gemacht hat oder
- die Daten in nur indirekt personenbezogener Form verwendet werden oder
- sich die **Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen,** oder
- der **Betroffene** seine **Zustimmung** zur Verwendung der Daten **ausdrücklich erteilt** hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
- die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder
- die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist.

b. Die Zustimmung

Die **Zustimmung** ist auch aus Sicht der Schülerverwaltung ein **unverzichtbarer Teil** des Umgangs mit Datenschutz. Besteht **keine gesetzliche Grundlage** (DSG, SchUG, BilDokG), so können die personenbezogenen Daten nur mit Zustimmung verwendet werden. Mit Zustimmung ist auch die Verwendung sensibler Daten möglich.

Achtung – in Hinblick auf die Zustimmung sind allerdings wichtige Aspekte zu beachten:

1. Es bedarf einer **Zustimmung jedes einzelnen** Schülers bzw. jeder einzelnen Schülerin. Eine Zustimmung 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. Zustimmung kann daher nur für Systeme verwendet werden, bei denen nicht zwingend alle Schülerinnen und Schüler erfasst werden.
2. Die **Zustimmung** 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 Zustimmung fehlt es sodann an der Zulässigkeit der Datenverwendung. Eine Weiterverwendung ist nicht mehr möglich. Bei der Zustimmung ist also zu beachten, dass, selbst wenn anfänglich etwa alle Schülerinnen und Schüler einer Klasse eine Zustimmung zur Verwendung der Daten geben, durch Widerruf die Zustimmung aller wieder verloren gehen kann.
3. 3. Die Zustimmung muss **freiwillig** und für den **konkreten Fall** erfolgen. Da die Schulleitung hoheitlich tätig wird, ja zum Teil sogar mit Schulpflicht verbunden ist, ist die vom DSG geforderte Freiwilligkeit (»gültige, insbesondere ohne Zwang abgegebene Willenserklärung«) der betroffenen Schülerinnen und Schüler entscheidend. Es darf kein Druck ausgeübt werden. Die Zustimmung als Grundlage der Datenverwendung kann nur für Bereiche dienen, in denen die Schule nicht zwingend auf die Zustimmung angewiesen ist. Überdies kann eine Zustimmung nicht pauschal erfolgen, also etwa für alle in der Schule vorgesehenen Datenverwendungen. Es muss eine Einwilligung in Kenntnis der Sachlage für den konkreten Fall der Datenverwendung sein. Der Zweck und die Form der Datenanwendung muss daher auch offengelegt werden.

Zusammenfassend ist daher festzuhalten, dass eine **Zustimmungslösung oft nicht optimal** ist, vor allem dann, wenn möglichst alle Schülerinnen und Schüler beteiligt werden sollen. Die Zustimmung jedes einzelnen Schülers zu erhalten, stellt schon einen beachtlichen Aufwand

dar. Dabei ist es ganz wichtig, dass die Freiwilligkeit der Zustimmung 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 Zustimmungen rasch wieder reduzieren kann. Umgekehrt ist zu betonen, dass bei fehlender gesetzlicher Grundlage bzw. wenn nicht argumentiert werden kann, dass es sich bei dieser Datenverwendung um eine wesentliche Voraussetzung für die Wahrnehmung einer der Schulleitung gesetzlich übertragenen Aufgabe handelt, die Schulleitung auf das Zustimmungsmodell angewiesen ist.

Frage: Wer erteilt die datenschutzrechtliche Zustimmung? Die Erziehungsberechtigten oder die Schülerinnen und Schüler?
Die **einschlägigen Gesetze** geben **keine Auskunft** über die Möglichkeit einer datenschutzrechtlichen Zustimmung von Minderjährigen.[3] Es besteht allerdings in der rechtswissenschaftlichen Literatur eine Debatte darüber, ob auch Minderjährige eine datenschutzrechtliche Zustimmung geben können. **Letztlich muss die unabhängige Datenschutzbehörde bzw. müssen die Gerichte diese Frage entscheiden.** Bis jetzt fehlt es aber an einschlägigen Urteilen.

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

2. Fraglich ist, ob es sich bei der datenschutzrechtlichen Zustimmung um eine **öffentlich-rechtliche** oder eine **privatrechtliche** Erklärung handelt. Für ein öffentlich-rechtliches Verständnis spricht bei der Schülerverwaltung der hoheitliche Rahmen, in dem diese Erklärung abgegeben wird. Generell spricht mehr für eine privatrechtliche Erklärung, da die Zustimmung vor allem auch bei privaten Geschäften zur Anwendung kommt. Diese Frage ist strittig.

3. An dieser Stelle wird die Meinung vertreten, dass unabhängig davon, ob es sich um eine öffentlich-rechtliche oder um eine privatrechtliche Erklärung handelt, die Schülerinnen und Schüler die Erklärung selbst abgeben können.

3 Siehe zur Diskussion um die Zustimmung Lachmayer, Die Multidimensionalität des Datenschutzrechts. Zur Notwendigkeit der Ausdifferenzierung datenschutzrechtlicher Regelungen, in Feik/Winkler (Hrsg.), Festschrift für Walter Berka (2013) Jan Sramek Verlag, 121; Kastelitz/Neugebauer, Aspekte der datenschutzrechtlichen Zustimmung(sfähigkeit) Minderjähriger, Jahrbuch Datenschutzrecht 2011, 71 (78ff); Duschanek, §1 DSG, in Korinek/Holoubek (Hrsg.), Österreichisches Bundesverfassungsrecht Rz 46; aA Jahnel, Handbuch Datenschutzrecht (2010) 3/141; Kuderna, Die Zustimmung des Betroffenen zur Übermittlung von Daten, DRdA 1992, 421; Reimer, Verfassungs- und europarechtliche Überlegungen zur datenschutzrechtlichen Zustimmung, in Jahnel/Siegwart/Fercher (Hrsg.), Aktuelle Fragen des Datenschutzrechts (2007) 183 (201); ders, Die datenschutzrechtliche Zustimmung (unveröff Diss, 2010) 157.

Öffentlich-rechtliche Erklärung: Diesbezüglich hängt es von der konkreten **Einsichtsfähigkeit** des **Minderjährigen** ab.[4] Bei einer Durchschnittsbetrachtung sollte ein vierzehnjähriger Schüler in der Lage sein, die Konsequenzen der Zustimmung der Verwendung der personenbezogenen Daten im Kontext der Schülerverwaltung zu verstehen. Es kommt aber auf die konkrete Einsichtsfähigkeit des einzelnen Schülers bzw. der einzelnen Schülerin an. Zur Verbesserung der konkreten Einsichtsfähigkeit könnten auch **Grundzüge des Datenschutzes im Unterricht** thematisiert werden.

Privatrechtliche Erklärung: In Hinblick auf die Minderjährigen ab dem 14. Lebensjahr gilt, dass diese altersübliche Geschäfte abschließen können. In der heutigen Zeit ist davon auszugehen, dass es sich bei datenschutzrechtlichen Zustimmungen auch um **altersübliche Geschäfte** handeln kann. Diesbezüglich ist es wieder entscheidend, welche Daten zu welchem Zweck verarbeitet werden sollen. So kann die Zustimmung zur Verwendung des Namens etwa als altersüblich angesehen werden. Die Zustimmung zur Verwendung von Gesundheitsdaten wäre nicht als altersüblich zu bezeichnen.

4. Konsequenz der Zulässigkeit der Zustimmungserklärung durch die Schülerinnen und Schüler ab dem 14. Lbj. ist, dass die Eltern diese Erklärung nicht für ihre Kinder abgeben dürfen, da es sich beim Datenschutzrecht um ein höchstpersönliches Recht handelt. Es empfiehlt sich jedenfalls, die Erziehungsberechtigten über die datenschutzrechtliche Zustimmung zu informieren.

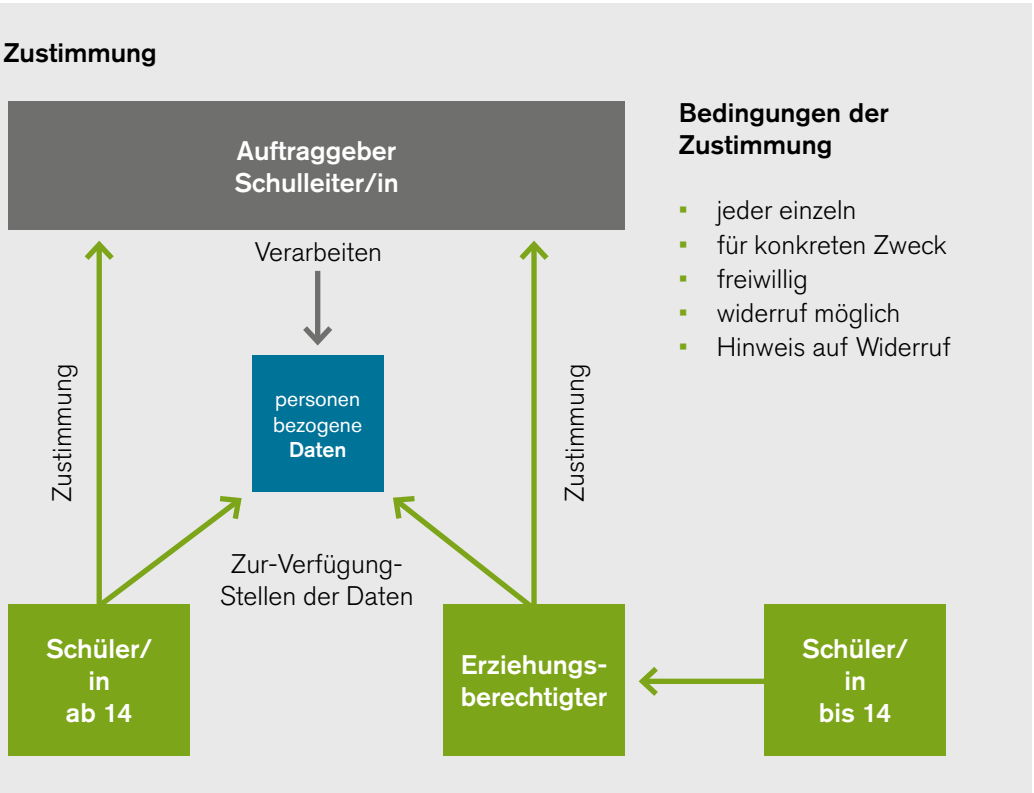


Abb. 4

4 *Jahnel*, Handbuch Datenschutzrecht (2010) 3/147.

c. 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 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
- Echtheit, Überprüfbarkeit, Vertrauenswürdigkeit, Nichtabstreitbarkeit
- Verfügbarkeit

Recht im Originaltext:
§ 14 Abs. 1 DSG: Für alle Organisationseinheiten eines **Auftraggebers** […] die Daten verwenden, sind **Maßnahmen zur** Gewährleistung der **Datensicherheit** zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.

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 Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitenden ausdrücklich festzulegen
- die Verwendung von Daten ist an das Vorliegen **gültiger Aufträge** der anordnungsbefugten Organisationseinheiten und Mitarbeitenden zu binden
- jede(r) **Mitarbeitende** muss über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten **belehrt werden**
- die **Zutrittsberechtigung** zu den Räumlichkeiten des Auftraggebers oder Dienstleisters ist zu regeln
- die **Zugriffsberechtigung** auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung 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 Verwendungsvorgänge, 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.

In Hinblick auf die Datensicherheit ist auch auf den Erlass des BMBF »Digitale Kompetenz an Österreichs Schulen (Zl. 17.200/110-II/872010)« zu verweisen.[5]

d. Registrierung

Das **Datenverarbeitungsregister** wird von der DSB geführt und ist für jedermann einsehbar. Es dient den Betroffenen dazu, über die Datenverwendungen von Auftraggebern nähere Informationen zu erlangen. § 17 Abs. 1 DSG stellt klar, dass jeder Auftraggeber (Schulleiter/Schulleiterin) vor Aufnahme einer Datenanwendung eine Meldung an die **Datenschutzbehörde** mit dem in § 19 festgelegten Inhalt[6] zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten hat. Dies gilt nicht für Standardanwendungen im Sinne der Verordnung über Standard und Musteranwendungen

Frage: Muss jeder Schulleiter / jede Schulleiterin eine Meldung bei der DSB vornehmen?
Grundsätzlich nicht: § 17 Abs 2 Z 6 DSG sieht eine wichtige Ausnahme vor: die sog. **Standardanwendung**. Diese ist nicht meldepflichtig! So ist jedenfalls die elektronische Schulverwaltung in der Standard- und Musterverordnung berücksichtigt und daher durch die Schulleitung nicht meldepflichtig. Generell ist davon auszugehen, dass Anwendungen, die vom BMBF zentral betrieben werden (z.B. BilDok, PH-Online, edu.moodle etc.) nicht durch die einzelnen Schulleiter der Datenschutzkommission gemeldet werden müssen. Im Zweifel wenden Sie sich bitte an Abt. IT/2, BMBF.

5 Verfügbar unter http://www.bmbf.gv.at/medienpool/20117/dig_erlass_bl1.pdf.

6 Notwendiger Inhalt der Meldung gem § 19 Abs 1 DSG:
- der Name bzw. die sonstige Bezeichnung und die Anschrift des Auftraggebers sowie die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde, und
- der Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit des Auftraggebers, soweit dies erforderlich ist, und
- den Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den anderen Angaben ergeben, und
- die Erklärung, ob die Datenanwendung einen oder mehrere der Tatbestände für die Vorabkontrollpflicht erfüllt, und
- die Kreise der von der Datenanwendung Betroffenen und die über sie verarbeiteten Datenarten sowie
- allgemeine Angaben über die getroffenen Datensicherheitsmaßnahmen, die eine vorläufige Beurteilung der Angemessenheit der Sicherheitsvorkehrungen erlauben.

Standardanwendungen werden im Rahmen einer Verordnung (VO) des Bundeskanzlers festgelegt. Es handelt sich konkret um die Verordnung über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004), BGBl. II Nr. 312/2004.

In Anlage 1 findet sich die **Standardanwendung SA025 Evidenzen der Schüler und Schülerinnen und Studierenden sowie Evidenz über den Aufwand für Bildungseinrichtungen.** Diese regelt jene Datenanwendungen (insbesondere jene Datenkategorien), die bei der DSB nicht gemeldet werden müssen.

Siehe den gesamten Text der Standardanwendung im Anhang.

Achtung: Werden über den Anwendungsbereich der Verordnung hinaus Daten in der Schülerverwaltung verwendet (insbesondere, wenn die Initiative zur Datenverarbeitung von der Schule ausgeht), so ist eine Meldung an die DSB erforderlich. Die damit verbundene DVR-Nummer ist insoweit anzugeben, als sie Betroffenen die Möglichkeit gibt, Einsicht in das Datenverarbeitungsregister zu nehmen. Bei der Verwendung von sensiblen Daten ist eine Vorabkontrolle von der DSB erforderlich (§ 18 Abs 2 DSG). Eine bloße Meldung reicht nicht.

e. Data Breach Notification

Mit der DSG-Novelle 2010 wurde eine Bestimmung zur sog. »Data Breach Notification«, also zur **Informationspflicht bei Datenmissbrauch** normiert.

Recht im Originaltext:
§24a Abs 2 DSG: Wird dem Auftraggeber bekannt, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht, hat er darüber **unverzüglich** die Betroffenen in geeigneter Form zu **informieren.** Diese Verpflichtung besteht nicht, wenn die Information angesichts der Drohung eines nur geringfügigen Schadens der Betroffenen einerseits oder der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert.

Im Fall eines Datenmissbrauches soll jedenfalls zuerst die zuständige Abteilung des BMBF kontaktiert werden (zentraleinformatik@bmbf.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 Auftraggeber anzusehen ist. § 3 BilDokG verweist in Hinblick auf den **Zweck der automationsunterstützten Verwendung 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
- Erstes Jahr der allgemeinen Schulpflicht
- Festgestellter sonderpädagogischer Förderbedarf
- Eigenschaft als o. oder ao. Schüler
- Schulkennzahl, Schulformkennzahl
- andere mit dem Schulbesuch zusammenhängende Daten über die Teilnahme an Unterrichts- und Betreuungsangeboten, den Schulerfolg, die Schul- bzw. Unterrichtsorganisation, den Bildungsverlauf sowie die Inanspruchnahme von Transferleistungen aus dem Familienlastenausgleich

b. Das Schulunterrichtsgesetz

Ausgangspunkt der Verpflichtungen des Schulleiters/der Schulleiterin als datenschutzrechtlicher Auftraggeber 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 Verwendung personenbezogener Daten im Rahmen der Schülerverwaltung herangezogen werden können. Ausgangspunkt ist die Führung von Amtsschriften gem. **§77 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. Folgende Amtsschriften haben die Schulen gem. §77 SchUG zu führen:

- **Schülerstammblätter**, in die die für die Ausstellung von Zeugnissen (§22) notwendigen Daten sowie die Noten der Jahreszeugnisse und die darin enthaltenen Entscheidungen und Verfügungen aufzunehmen sind;
- **Klassenbücher** für jede Klasse, die zur Eintragung der Namen der Schüler der Klasse, der Unterrichtsgegenstände eines jeden Schultages, der unterrichtenden Lehrer bzw. Lehrerinnen, des durchgenommenen Lehrstoffes, der vom Unterricht fernbleibenden Schüler bzw. Schülerinnen und besonderer Vorkommnisse ua. bestimmt werden können;
- **Prüfungsprotokolle** über die Durchführung von Einstufungsprüfungen (§3 Abs. 6), Aufnahms- und Eignungsprüfungen (§§6 bis 8), Feststellungsprüfungen (§20 Abs. 2), Nach-

tragsprüfungen (§20 Abs. 3), Prüfungen über Kenntnisse und Fertigkeiten des praktischen Unterrichtes (§20 Abs. 4), Wiederholungsprüfungen (§23), Reifeprüfungen, …; 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.

In Hinblick auf die **Schülerstammdaten** 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

Gemäß **§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 ihrer rechtlichen Bedeutung. Das Datenschutzrecht ist nicht nur eine gesetzliche Vorgabe. **Datenschutz ist** ein verfassungsgesetzlich gewährleistetes Recht, ein **Grundrecht der österreichischen Verfassung** (§1 Datenschutzgesetz – DSG).[7] 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 jene Angaben von betroffenen Personen, deren Identität bestimmt oder bestimmbar ist (siehe näher unter I.2.B.)

7 §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.

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 allgemein verfügbar sind (etwa im Internet, nicht aber auf eingeschränkt zugänglichen Foren oder schulinternen Seiten[8]) 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).

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 (im DSG, im SchUG oder in anderen Gesetzen, etwa dem BilDokG) oder einer Zustimmung der Schülerinnen und Schüler bzw. der Erziehungsberechtigten.
- Überdies muss das Verwenden personenbezogener Daten verhältnismäßig sein. Die Verwendung 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 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.

8 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 Schülers vorliegt oder dieser selbst seine Daten im Internet veröffentlicht, liegt »allgemeine Verfügbarkeit« vor und die personenbezogenen Daten unterliegen nicht dem Grundrecht auf Datenschutz.

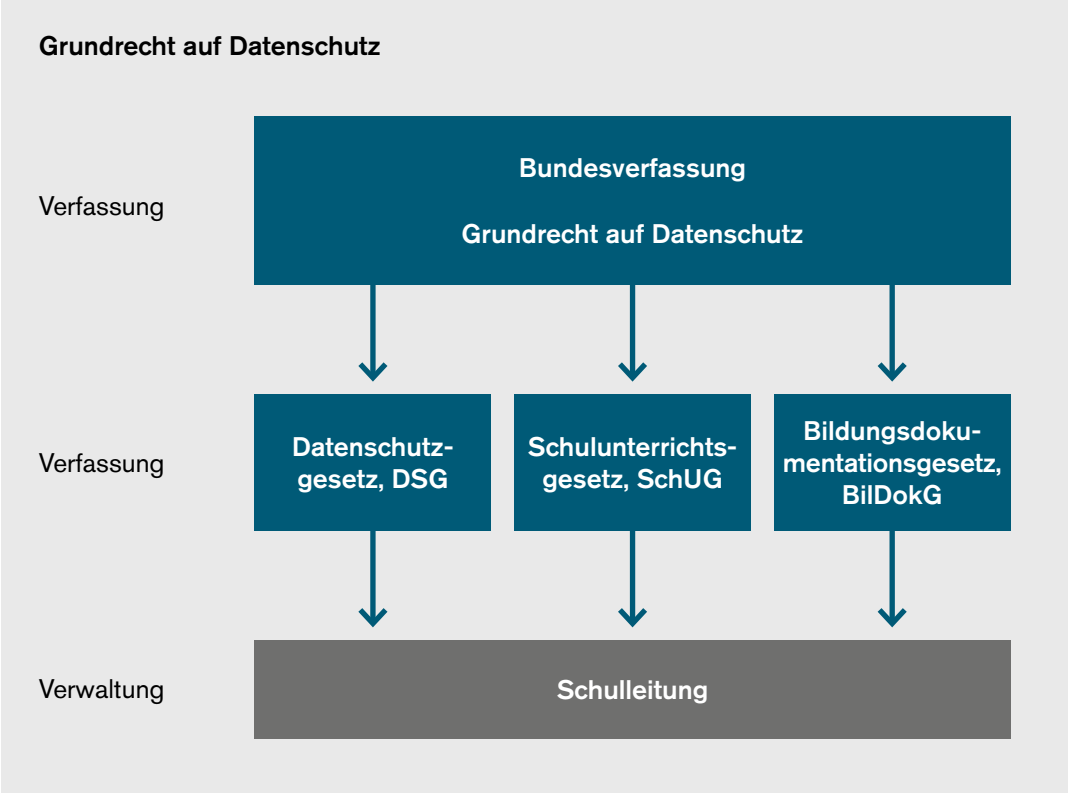


Abb. 5

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)[9]

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

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.[10] **Ausgangspunkt ist, dass der Betroffene überhaupt keine Daten zur Verfügung stellen muss**. Das Recht auf Geheimhaltung bezieht sich nicht nur auf auto-

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

10 *Jahnel*, Handbuch Datenschutzrecht (2010) Rz 2/15.

mationsunterstützte Datenanwendung, sondern auch auf manuelle Daten sowie alle anderen Formen der Datenverwendung.[11]

Frage: Wer ist »Betroffener« des Grundrechts auf Datenschutz?
Betroffener ist eine natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet werden. Im Kontext der Schülerverwaltung sind also primär die Schülerinnen und Schüler betroffen, da ihre Daten verwendet 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 Verwendung personenbezogener Daten, also ein Eingriff auf 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 »Zustimmung« gemeint?
Zustimmung ist eine gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt (siehe näher unter I.2.B.)

In Hinblick auf die Schülerverwaltung bedeutet dies:

- Primär muss es eine **gesetzliche Grundlage** geben, die sich aus dem DSG, dem SchUG, dem BilDokG oder anderen Gesetzen ergibt, um datenschutzrechtlich tätig werden zu können.
- Gibt es keine gesetzliche Grundlage, so ist die **Zustimmung der Betroffenen** bzw. ihrer Erziehungsberechtigten einzuholen.
- Nur im **Ausnahmefall** kann eine Verwendung personenbezogener Daten im Kontext der Schülerverwaltung als »im **lebensnotwendigen Interesse des Betroffenen**« angesehen werden. Es geht um Umstände, die »sich auf das Leben des Betroffenen im **medizinischen [!] Sinn** auswirken«.[12] Primärer Zweck ist es, die Zustimmung des Betroffenen zu ersetzen,

11 *Jahnel*, Handbuch Datenschutzrecht (2010) Rz 2/14.
12 *Jahnel*, Handbuch Datenschutzrecht (2010) Rz 2/35.

weil dieser aufgrund der Schwere des Falls nicht mehr in der Lage ist, selbst eine Zustimmung zu geben. Im Zusammenhang mit der Schülerverwaltung ermöglicht diese Bestimmung es der Schule (Direktion, Lehrpersonal), auch ohne die Zustimmung der Erziehungsberechtigten zur Weitergabe von personenbezogenen Daten bei schwerwiegenden Unfällen von Schülerinnen und Schülern rasch zu handeln, ohne Fragen des Datenschutzes klären zu müssen.

Zulässige Verwendung personenbezogener Daten

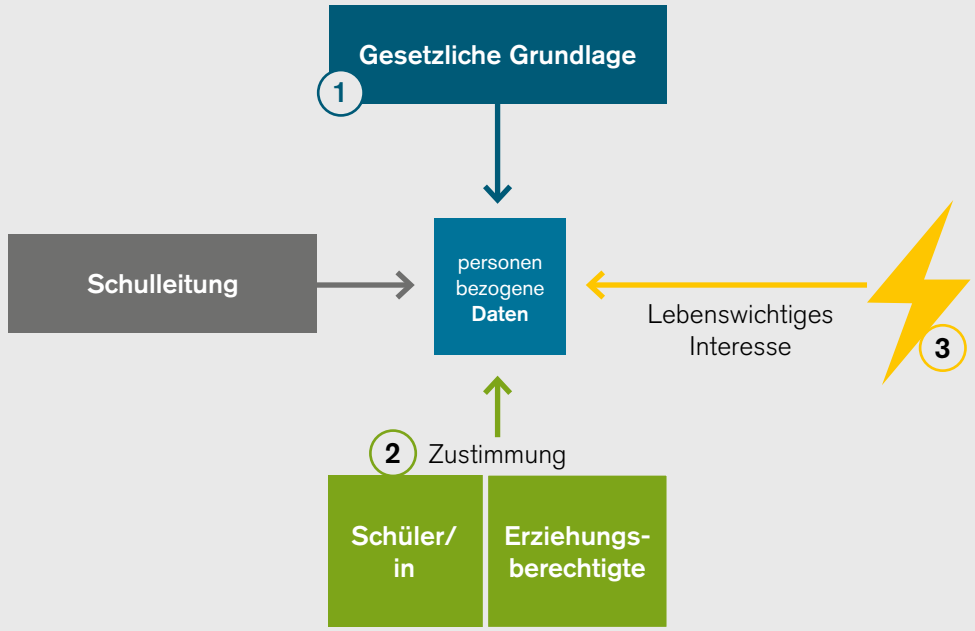


Abb. 6

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

b. 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 Au-

tomationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

4. 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;

5. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.«

Recht auf Auskunft

Das **Recht auf Auskunft** bedeutet, dass sich die Schülerinnen und Schüler 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.

Recht auf Auskunft

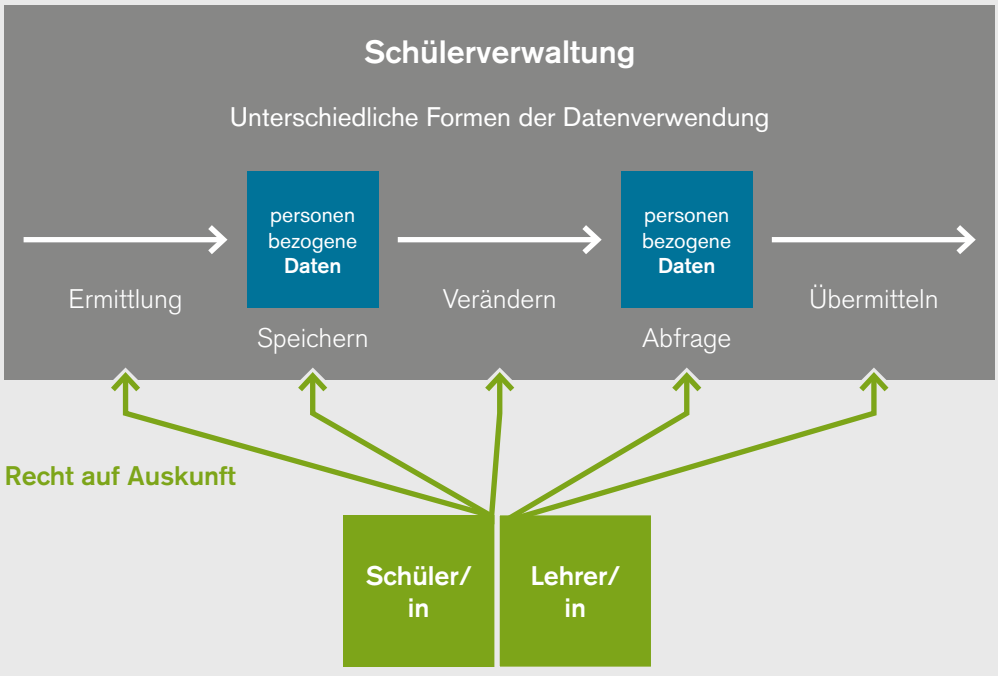


Abb. 7

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 Zustimmung 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 Datenverwendung sowie die Rechtsgrundlagen hierfür in allgemein verständlicher Form **anzuführen.**

- Mit Zustimmung 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 acht Wochen nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen,** warum sie nicht oder nicht vollständig erteilt wird. Von der Erteilung der Auskunft kann auch deshalb abgesehen werden, weil der Auskunftswerber am Verfahren nicht mitgewirkt oder weil er den Kostenersatz nicht geleistet hat.

- 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 Auftraggeber 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.

- Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Auskunftswerber innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde an die DSB bis zum rechtskräftigen Abschluß des Verfahrens nicht vernichten. Diese Frist gilt nicht, wenn einem Löschungsantrag des Auskunftswerbers zu entsprechen ist.

Siehe §26 DSG.

Das Recht auf Richtigstellung

Das **Recht auf Richtigstellung** ist ein Folgerecht des Auskunftsrechts. Wurden Daten falsch erfasst oder haben sich diese verändert, so haben die Schülerinnen und Schüler 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. 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 Datenverwendung (etwa erfolgreiche Aufnahme des Schülers) weg, so dürfen diese Daten nicht mehr gespeichert werden. Der Schüler 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 auch **auf Antrag von Betroffenen** vorzugehen.
- **Innerhalb von acht Wochen** 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 ein **Vermerk über die Bestreitung** beizufügen. Der Bestreitungsvermerk darf nur mit Zustimmung des / der Betroffenen oder auf Grund einer Entscheidung des zuständigen Gerichtes oder der DSB gelöscht werden.

Siehe §27 DSG.

C. Die Schulleitung als Grundrechtsverpflichteter

Die **Schulleitung** von Bundesschulen ist organisatorisch Teil der **Bundesverwaltung** und somit ein **Organ einer Gebietskörperschaft**. Überdies wird die Schulleitung in Vollziehung der Gesetze und damit hoheitlich tätig. Die Vollziehung des Schulrechts fällt in den Bereich der Hoheitsverwaltung. Dies gilt auch für Schulen anderer Schulerhalter, da sie als Beliehene im Bereich der Vollziehung des Schulrechtes hoheitliche tätig werden (§ 5 Abs. 2 Z 2 DSG). Aus Sicht des Datenschutz haben alle Schulen (unabhängig ob der Bund oder andere öffentlich- wie privatrechtliche Schulerhalter sind) die gleichen Rechte und Pflichten wie Bundesschulen. Die Zuordnung der Schulleitung zum Bund ist für das Datenschutzrecht von erheblicher Bedeutung, da § 5 DSG zwischen dem öffentlichen und dem privaten Bereich unterscheidet. Datenanwendungen sind dem öffentlichen Bereich im Sinne dieses Bundesgesetzes zuzurechnen, wenn sie für Zwecke eines »Auftraggebers des öffentlichen Bereichs« durchgeführt werden. Als »Auftraggeber des öffentlichen Bereichs« versteht § 5 DSG alle Auftraggeber, die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft.

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

Recht im Originaltext:
§4 Z 4 DSG **Auftraggeber:** natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden (Z 8), unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen. …

§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 Auftraggeber** iSd § 4 DSG.[13] ISd § 5 DSG ist der Schulleiter/die Schulleiterin, als Organ des Bundes, Auftraggeber des öffentlichen Bereichs. Den Schulleiter/die Schulleiterin als datenschutzrechtlichen Auftraggeber 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 Auftraggeber.[14]

An den Auftraggeber knüpfen sich die **datenschutzrechtlichen Verpflichtungen**. So ist der **Schulleiter/die Schulleiterin** als Auftraggeber zur Einhaltung des Grundrechts auf Datenschutz verpflichtet. Der Auftraggeber hat nicht nur für die Geheimhaltung der personenbezogenen Daten zu sorgen, sondern ist auch Adressat des Auskunftsrechts sowie des Rechts auf Richtigstellung bzw. Löschung. Soweit er die Datenverarbeitung einem Dienstleister überlässt, hat er im Zuge eines Vertrages mit diesem eine Dienstleistervereinbarung abzuschließen. Soweit das BMBF zentral einen Dienstleister beauftragt hat (z.B. Sokrates, Web-Untis, edu.moodle, lms.

13 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.

14 Siehe *Wohlkinger*, Datenschutz im Bildungswesen, in: Bauer/Reimer (Hrsg.), Handbuch Datenschutzrecht (2009) facultas.wuv 273 (282).

at) wurde diese Dienstleistervereinbarung durch das BMBF abgeschlossen. Diesbezüglich ist der Abschluss einer eigenen Dienstleistervereinbarung auf Schulebene daher nicht mehr nötig. Im Zweifel wenden Sie sich bitte an Abt. IT/2, BMBF.

D. Der Rechtsschutz von Schülerinnen und Schülern

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

Seit 1.1.2014 wurde die DSK durch eine **unabhängige Datenschutzbehörde** ersetzt, der nicht mehr eine Kommission, sondern ein Behördenleiter vorsteht. Die Kompetenzen der neuen Datenschutzbehörde entsprechen den Zuständigkeiten der DSB. Gegen den Bescheid der Datenschutzbehörde besteht die Möglichkeit einer Bescheidbeschwerde an das mit dem Jahr 2014 neu eingerichtete **Bundesverwaltungsgericht** (BVwG). Das BVwG schafft eine neue Form des gerichtlichen Rechtsschutzes 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. Das BVwG entscheidet in Form eines gerichtlichen Urteils, das als »Erkenntnis« bezeichnet wird. Gegen die Erkenntnis des BVwG besteht sodann die Möglichkeit, die Gerichtshöfe des öffentlichen Rechts anzurufen. Gem. Art. 144 B-VG kann eine **Erkenntnisbeschwerde** beim **VfGH** eingebracht werden, in der der Betroffene die Verletzung in seinem Grundrecht auf Datenschutz geltend macht. Gem. Art. 133 B-VG kann Revision an den **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.[15]

15 Art 133 Abs. 4 B-VG idF BGBl I 2012/51.

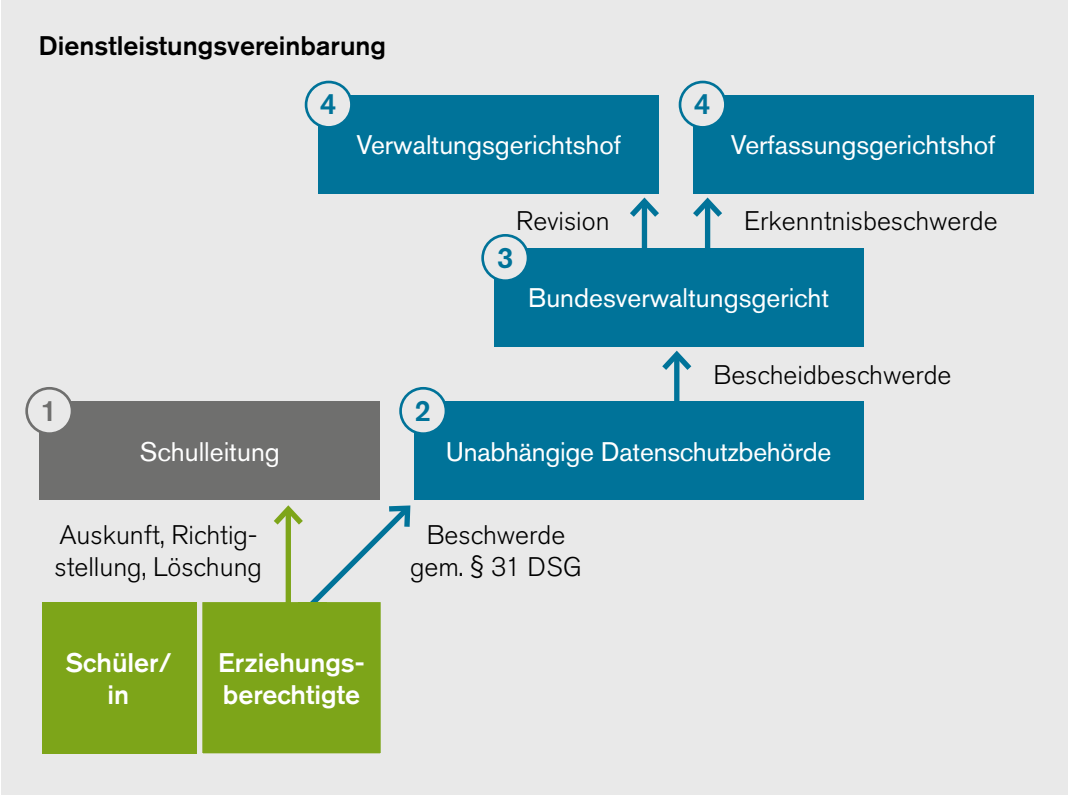

Dienstleistungsvereinbarung
4
Verwaltungsgerichtshof
4
Verfassungsgerichtshof
Revision
Erkenntnisbeschwerde
3
Bundesverwaltungsgericht
Bescheidbeschwerde
1
Schulleitung
2
Unabhängige Datenschutzbehörde
Auskunft, Richtig-
stellung, Löschung
Beschwerde
gem. § 31 DSG
Schüler/
in
Erziehungs-
berechtigte

Abb. 8

II. Besondere datenschutzrechtliche Fragestellungen in der Schülerverwaltung

1. Überblick

Über die allgemeinen datenschutzrechtlichen Grundlagen in Hinblick auf die Schülerverwaltung hinaus ergeben sich zahlreiche **konkrete datenschutzrechtliche Fragestellungen im Schulalltag.** Die Fragestellungen sind vielfältig und zum Teil sehr komplex. Schließlich sind mit Datenanwendungen oft vielfältige Prozesse der Verwendung 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 Fragestellungen 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. Ein Schwerpunkt liegt auf den technischen Neuerungen, wie etwa das Führen eines elektronischen Klassenbuchs oder der edu.card. Für die Schülerverwaltung von besonderer Relevanz ist ebenso der Schutz des persönlichen Bildnisses, die Verwendung von Videoüberwachung, die Vereinbarung mit Dienstleistern sowie die Internet-Policy für Schulen. Abschließend werden noch weitere Fragen kurz erläutert (Sponsoren, Facebook, Website, Handyblocker).

2. Digitale Schülerverwaltung Neu

Die **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

Auftraggeber im Sinne des DSG sind in der digitalen Schülerverwaltung weiterhin die **Schulleiter**/die **Schulleiterinnen**. 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 BMBF zugreifen. Datenschutzrechtlich handelt es sich daher nicht um ein Informationsverbundsystem gem §4 Z 13 DSG (Informationsverbundsystem bedeutet »die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber [Schulleiter/Schulleiterin] und die gemeinsame Benützung der Daten in der Art, daß jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden«. 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 Zustimmung freiwillig** der Schulleitung zur Verfügung gestellt werden.

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

Die **Datenerfassung beruht auf den expliziten datenschutzrechtlichen Bestimmungen des SchUG und des BilDokG** sowie auf den schulrechtlichen Regelungen des SchUG, soweit die Datenverwendung 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/BMBF

Im Rahmen des BilDokG ist vorgesehen, dass auch Daten der Schülerverwaltung an das BMBF (»den zuständigen Bundesminister«) übermittelt werden **müssen**. Es handelt sich dabei um explizite gesetzliche Grundlagen der Datenverwendung 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 oder nur **indirekt personenbezogene Daten der Lehrerinnen und Lehrer**. Gem **§5 BilDokG** werden »Gesamtevidenzen der Schüler« vorgesehen. Der zuständige Bundesminister hat als datenschutzrechtlicher Auftraggeber »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 **indirekt personenbezogen** gespeichert.

Frage: Was sind indirekt personenbezogene Daten?
»Nur indirekt personenbezogen« sind Daten für einen Empfänger einer Übermittlung (also das BMBF) dann, wenn der **Personenbezug** der Daten derart ist, dass dieser Übermittlungsempfänger die Identität des Betroffenen **mit rechtlich zulässigen Mitteln nicht bestimmen kann.**

Siehe §4 Z 1 DSG.

Das BMBF 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 Unterricht, Kunst und Kultur 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 BMBF 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 bzw. BSR.

4. Schulwechsel

Mit dem **Übertritt eines Schülers bzw. einer Schülerin von einer Schule in eine andere** ist datenschutzrechtlich ein Wechsel des Auftraggebers (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 Zustimmung erteilt, dass eine Schule 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.

Eine automatisierte Übermittlung der Daten zwischen den Schülerverwaltungen ist derzeit nicht möglich.[16]

5. Elektronisches Klassenbuch[17]

Bereits die bestehenden Klassenbücher sind als manuelle Dateien iSd § 4 Z 6 DSG anzusehen. 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 SchUG** stützten. Eine entsprechende Pflicht zum Führen eines solchen ergibt sich gem. § 77 iVm 56 Abs 4,[18] 54 Abs. 2 SchUG. Die gem. § 77 lit b SchUG vorgesehenen Klassenbücher sehen als zu erfassende Daten vor:

- die Klasse
- die Namen der Schüler und Schülerinnen der Klasse
- die Unterrichtsgegenstände eines jeden Schultages
- die unterrichtenden Lehrer und Lehrerinnen
- den durchgenommenen Lehrstoff
- die vom Unterricht fernbleibenden Schüler und Schülerinnen
- und besondere Vorkommnisse

Auch die Verwendung personenbezogener Daten in Bezug auf das elektronische Klassenbuch muss gem. § 7 Abs. 1 DSG von den gesetzlichen Zuständigkeiten des jeweiligen Auftraggebers gedeckt sein und darf die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.

In Hinblick auf die gesetzlichen Zuständigkeiten des Auftraggebers konkretisiert **§ 77 SchUG** die Pflichten, für die letztlich der Schulleiter/die Schulleiterin verantwortlich ist, klar. In Hinblick auf die schutzwürdigen Geheimhaltungsinteressen iSd § 8 Abs. 1 DSG besteht bereits eine ausdrückliche gesetzliche Ermächtigung iSd Z 1 leg cit. Da in Hinblick auf die »**besonderen Vorkommnisse**« argumentiert werden kann, dass eine derartige ausdrückliche gesetzliche Ermächtigung fehlt, kann auf § 8 Abs. 1 Z 4 DSG, also die überwiegend berechtigten Interessen des Auftraggebers, zurückgegriffen werden. Die Verwendung der personenbezogenen Daten im Rahmen des elektronischen Klassenbuchs sind »eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe« gem. § 8 Abs. 3 Z 1 DSG. Auch in Hinblick auf das elektronische Klassenbuch ist die Verhältnismäßigkeit zu wahren. Die **Verwendung sensibler Daten ist jedenfalls nicht zulässig.**

16 *Wohlkinger,* Datenschutz im Bildungswesen, in: Bauer/Reimer (Hrsg.), Handbuch Datenschutzrecht (2009) facultas.wuv 273 (290f).

17 Siehe dazu grundlegend *Forgo,* Datenschutzrechtliche Fragen der digitalen Schulverwaltung (DADISCH) unveröff. Studie (2011) 1, 39ff.

18 Siehe dazu schon oben unter I.1.D.a.

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 Servicefunktionen** verbunden, etwa Zugangsmöglichkeiten zu Räumen wie der Bibliothek. Sie kann aber auch mit einer Kopierkarten- oder Geldbörsefunktion (Quick) ausgestattet werden.

Datenschutzrechtlicher Auftraggeber der edu.card ist der Schulleiter / die Schulleiterin. Für die Ausgabe der edu.card ist derzeit die Zustimmung der betroffenen Schülerinnen und Schüler bzw. der Erziehungsberechtigten erforderlich. Die Einführung und der Einsatz der edu.card können jedenfalls auf Basis der **datenschutzrechtlichen Zustimmung** erfolgen. Die Zustimmung zur edu.card muss durch den einzelnen Schüler bzw. die einzelne Schülerin erfolgen. Dabei ist – wie oben dargestellt – in besonderer Weise auf die Zustimmung der Erziehungsberechtigten bzw. der Schüler sowie auf die damit verbundene Freiwilligkeit der Zustimmung zu achten. Dies bedeutet aber auch, dass es für Schülerinnen und Schüler, die keine Zustimmung geben, zu keinen strukturellen Nachteilen bei der Benützung der Schulinfrastruktur kommen kann (etwa bei dem Zugang zu Räumen).[19]

Bei den Chipkarten ist in besonderer Weise das datenschutzrechtliche Prinzip der Zweckbindung zu berücksichtigen. Es darf die Verwendung 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. Dienstleistungsvereinbarung

Die an der Schule durchgeführte Verwendung 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 Dienstleister,** der für die Schule tätig wird. Typischerweise erledigt er IT-Aufgaben für die Schule. Dienstleister sind gem. §4 Z 5 DSG Personen, die personenbezogene »Daten nur zur Herstellung eines ihnen aufgetragenen Werkes

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

verwenden«. Sie werden 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 Dienstleister; bei Klassenfotos durch professionelle Fotografen treten diese selbst als datenschutzrechtliche Auftraggeber auf und damit direkt in eine rechtliche Beziehung zu den Fotografierten, ohne dass die Schulleitung an dieser Rechtsbeziehung beteiligt ist.

Generell ist davon auszugehen, dass Anwendungen, die vom BMBF zentral beauftragt werden auch eine Dienstleistungsvereinbarung abgeschlossen wurde (z.B. BilDok, PH-Online, edu.moodle, MS-Ach-Vertrag bezüglich Office365 etc.). Daher muss diesbezüglich nicht durch die einzelnen Schulleiter eine Dienstleistungsvereinbarung abgeschlossen werden. Im Zweifel wenden Sie sich bitte an Abt. IT/2, BMBF.

Ein Muster für eine Dienstleistervereinbarung findet sich im Anhang A dieses Dokuments.

Achtung: Bei Dienstleistern aus dem Ausland sind die datenschutzrechtlichen Rahmenbedingungen zu berücksichtigen. Generell gilt, dass das DSG auch auf die Verwendung personenbezogener Daten im Ausland anzuwenden ist, wenn die Verwendung in anderern EU-Mitgliedsstaaten für Zwecke eines österreichischen Auftraggebers erfolgt (§ 3 Abs 1 DSG).

Das DSG stellt Bedingungen für die Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen auf:

Recht im Originaltext:
§ 10. (1) **Auftraggeber dürfen bei ihren Datenanwendungen Dienstleister in Anspruch nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten.** Der Auftraggeber hat mit dem Dienstleister die hierfür notwendigen Vereinbarungen zu treffen und sich von ihrer Einhaltung durch Einholung der erforderlichen Informationen über die vom Dienstleister tatsächlich getroffenen Maßnahmen zu überzeugen.

Dienstleistungsvereinbarung

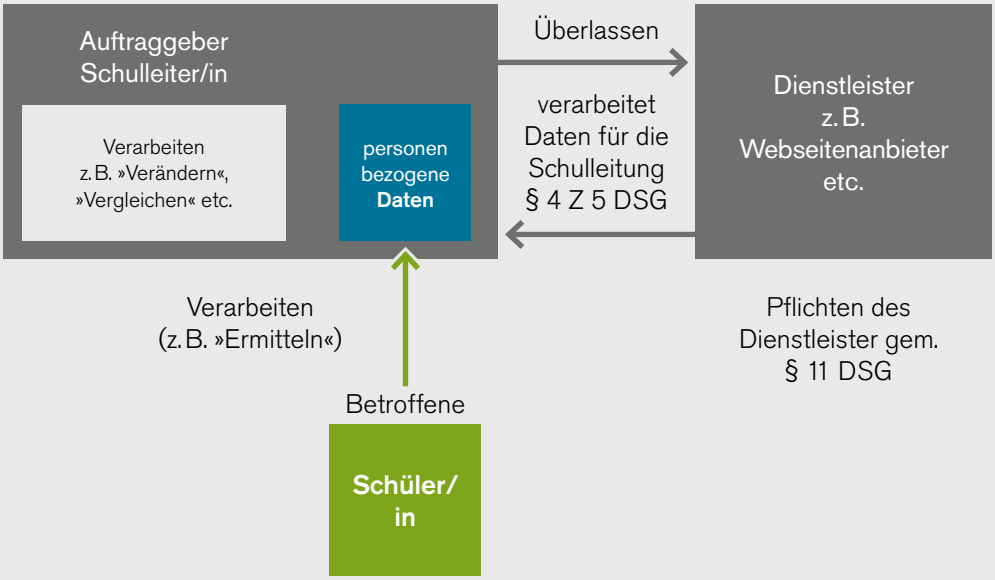


Abb. 9

Frage: Welche Pflichten hat ein Dienstleister?
Gem. §11 DSG hat der Dienstleister bei der Verwendung von personenbezogenen Daten für den Auftraggeber folgende Pflichten, die unabhängig von allfälligen vertraglichen Vereinbarungen des Auftraggebers mit dem Dienstleister bestehen:

1. die Daten **ausschließlich im Rahmen der Aufträge des Auftraggebers** zu verwenden; insbesondere ist die Übermittlung der verwendeten Daten ohne Auftrag des Auftraggebers verboten;

2. alle gemäß §14 erforderlichen **Datensicherheitsmaßnahmen** zu treffen; insbesondere dürfen für die Dienstleistung nur solche Mitarbeitende herangezogen werden, die sich dem Dienstleister gegenüber zur Einhaltung des Datengeheimnisses verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen;

3. **weitere Dienstleister nur mit Billigung des Auftraggebers heranzuziehen** und deshalb den Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann;

4. – sofern dies nach der Art der Dienstleistung in Frage kommt – im Einvernehmen mit dem Auftraggeber die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflicht des Auftraggebers zu schaffen;

5. nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten;

6. dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der genannten Verpflichtungen notwendig sind.

(2) Vereinbarungen zwischen dem Auftraggeber und dem Dienstleister über die nähere Ausgestaltung der genannten Pflichten sind zum Zweck der Beweissicherung **schriftlich festzuhalten.**

Siehe Näheres zur Dienstleistungsvereinbarung im Anhang.

B. Videoüberwachung

Für Schulen wird die Möglichkeit der **Videoüberwachung** immer relevanter. Mit der DSG Nov 2010 wurde mit den Bestimmungen gem. **§§50a ff DSG** ein eigener Abschnitt über die Videoüberwachung in das DSG aufgenommen.

Frage: Was bedeutet Videoüberwachung im Sinne des DSG?
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.

Zulässig ist die Videoüberwachung, wenn

- diese im lebenswichtigen Interesse einer Person erfolgt, oder
- Daten über ein Verhalten verarbeitet werden, das ohne jeden Zweifel den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden, oder
- der Betroffene der Verwendung seiner Daten im Rahmen der Überwachung ausdrücklich zugestimmt hat.
- **bestimmte Tatsachen die Annahme rechtfertigen,** das **überwachte Objekt** oder die überwachte Person könnte das Ziel oder **der Ort eines gefährlichen Angriffs** werden, oder
- sich die Überwachung in einer bloßen Echtzeitwiedergabe von das überwachte Objekt/die überwachte Person betreffenden Ereignissen erschöpft, diese also weder gespeichert (aufgezeichnet) noch in sonst einer anderen Form weiterverarbeitet wird (Echtzeitüberwachung), und sie zum Zweck des Schutzes von Leib, Leben oder Eigentum des Auftraggebers erfolgt.

Von den genannten Gründen sind für die Schülerverwaltung nur die letzten zwei Gründe von Praxisrelevanz. Ein gefährlicher Angriff bezieht sich auf strafbare Handlungen im Sinne des Strafgesetzbuchs, aber etwa auch des Suchtmittelgesetzes. Die Videoüberwachungsdaten sind zu verschlüsseln und es ist unter Hinterlegung des einzigen Schlüssels bei der Datenschutzbehörde sicherzustellen, dass eine Auswertung der Videoaufzeichnungen nur im begründeten Anlassfall durch eine bestimmte Stelle stattfindet. Der Schulleiter bzw. die Schulleiterin als der Auftraggeber der Videoüberwachung hat diese **geeignet zu kennzeichnen.** Die Kennzeichnung hat örtlich derart zu erfolgen, dass jeder potenziell Betroffene, der sich einem überwachten

Objekt oder einer **überwachten Person** nähert, tunlichst **die Möglichkeit hat, der Videoüberwachung auszuweichen** (§ 50d DSG).

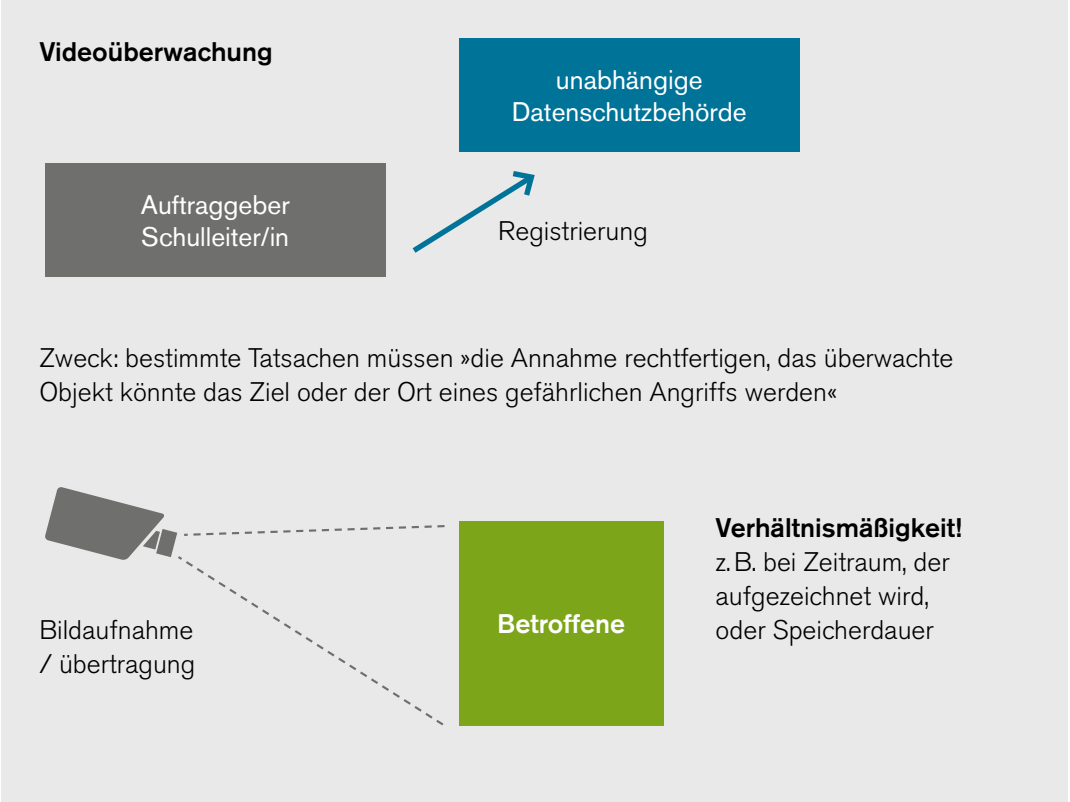


Abb. 10

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. § 50a Abs. 5 DSG die Einrichtung einer Videoüberwachung an Orten, die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen (also etwa Toiletten).

Frage: Muss die Videoüberwachung registriert werden?
Die Videoüberwachung bedarf der Meldung bei der unabhängigen Datenschutzbehörde (§50c DSG). Eine Echtzeitüberwachung bedarf nicht der Registrierung. Die Standard- und Muster-Verordnung sieht in ihrem Anhang derzeit keine Ausnahme von Registrierung für Schulen vor.

C. 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 **um personenbezogene Daten** im Sinne des DSG 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 **Zustimmung** der Erziehungsberechtigten bzw. der Schülerinnen und Schüler möglich. Es empfiehlt sich eine entsprechende Zustimmung am Anfang des Schuljahres durch die Zustimmungsberechtigten einzuholen.

Über die Regelungen des DSG hinaus finden sich in der Rechtsordnung weitere Bestimmungen zum Schutz des persönlichen Bildnisses. Hervorzuheben ist etwa **§78 UrheberrechtsG**[20]:

Recht im Originaltext:
Bildnisschutz

§78 Abs. 1 UrhG: »Bildnisse von Personen dürfen weder öffentlich ausgestellt noch auf eine andere Art, wodurch sie der Öffentlichkeit 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** (z.B.: 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 Zustimmung auf die unterschiedlichen Verwendungszwecke der medial erfassten personenbezogenen Daten bezieht. Insoweit ist bereits in den Zustimmungserklärungen der Medienumgang klarzulegen.

Frage: Dürfen personenbezogene Daten an Dritte, etwa Sponsoren, (Schulbuch)verlage, Softwarehersteller bzw. Betreiber von Webservices (Soziale Nezte, Mailservices, Cloudspace etc.) 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 Zustimmung der Erziehungsberechtigten bzw. der Schülerinnen und Schüler geknüpft, die die Übermittlung an Dritte konkret vorgibt und den Zweck der Übermittlung klarstellen muss.

20 Siehe auch §16 ABGB.

Frage: Welche personenbezogenen Daten der Schülerinnen und Schüler dürfen auf der Webseite der Schule publiziert werden?
Ohne explizite Zustimmung 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 Zustimmung 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 Verwendung 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

Glossar

Auftraggeber ist eine natürliche oder juristische **Person** oder ein **Organ** einer **Gebietskörperschaft** beziehungsweise die Geschäftsapparate solcher Organe, wenn sie alleine oder gemeinsam mit anderen die **Entscheidung getroffen** haben, **Daten zu verwenden (Schulleitung),** unabhängig davon, ob sie die Daten selbst verwenden oder damit einen Dienstleister beauftragen.

Betroffener ist jede vom **Auftraggeber** verschiedene Person, deren Daten verwendet werden (primär also die Schülerinnen und Schüler).

Data Breach Notification (Meldung bei Datenmissbrauch): Wird dem Auftraggeber bekannt, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht, hat er darüber unverzüglich die Betroffenen in geeigneter Form zu informieren.

Dienstleister ist jede natürliche oder juristische Person, sowie jedes Organ einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwenden (etwa Bundesrechenzentrum).

Personenbezogene Daten sind Angaben über **Betroffene,** deren Identität bestimmt oder bestimmbar ist; »nur indirekt personenbezogen« sind Daten, wenn der Personenbezug der Daten derart ist, dass der **Auftraggeber** (Schulleitung) die Identität des/der Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.

Sensible Daten sind personenbezogene Daten in Bezug auf die rassische und ethnische **Herkunft**, politische **Meinung, Gewerkschaftszugehörigkeit,** religiöse oder **philosophische Überzeugung, Gesundheit** oder das **Sexualleben.**

Verwenden von Daten ist jede Art der Handhabung von Daten, also sowohl das Verarbeiten als auch das Übermitteln von Daten.

Verarbeiten von Daten: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns von Daten.

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 Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses.

Übermitteln von Daten ist die Weitergabe von Daten an andere Empfänger als den/die Betroffene/n, den/die Auftraggeber/in oder einen Dienstleister, insbesondere auch das Veröf-

fentlichen von Daten (z.B. Weitergabe von Schülerstammdaten von Volksschule an Gymnasium an der Nahtstelle oder Übermittlung an den LSR); darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers(!)

Zustimmung ist die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt.

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)
BMBF	Bundesminister(ium) für Bildung und Frauen
bPK	bereichsspezifischen Personenkennzeichen
BVwG	Bundesverwaltungsgericht
B-VG	Österreichisches Bundes-Verfassungsgesetz
DSB	Datenschutzbehörde
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
z.B.	zum Beispiel

Literaturverzeichnis

A. Materialien

Erlass des BMBF »Digitale Kompetenz an Österreichs Schulen (Zl. 17.200/110-II/872010) http://www.bmbf.gv.at/medienpool/20117/dig_erlass_bl1.pdf

Meinl et. al, Recht in virtuellen Lernumgebungen, BMBF, 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, BMBF, 2. Aufl., 2012

http://edugov.bildung.at/edugov/learning/Unterrichtsmaterialien

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

B. Weiterführende Links:

Datenschutzkommission – www.dsk.gv.at

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

Datenschutzgesetz gesamt (Stand: 28.09.2013): 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.

Duschanek, §1 DSG, in Korinek/Holoubek (Hrsg.), Österreichisches Bundesverfassungsrecht.

Jahnel, Datenschutzrecht (2010) Jan Sramek Verlag.

Kastelitz/Neugebauer, Aspekte der datenschutzrechtlichen Zustimmung(sfähigkeit) Minderjähriger, Jahrbuch Datenschutzrecht 2011, 71.

Kuderna, Die Zustimmung des Betroffenen zur Übermittlung von Daten, DRdA 1992, 421.

Lachmayer, Zur Reform des Europäischen Datenschutzes. Eine erste Analyse des Entwurfs der Datenschutz-Grundverordnung, Österreichische Juristenzeitung 2012, 841

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.

Reimer, Verfassungs- und europarechtliche Überlegungen zur datenschutzrechtlichen Zustimmung, in Jahnel/Siegwart/Fercher (Hrsg.), Aktuelle Fragen des Datenschutzrechts (2007) 183 (201).

Reimer, Die datenschutzrechtliche Zustimmung (unveröff Diss, 2010) 157.

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

Vorlagen

A. Mustervereinbarung: Schule – Dienstleister

Dienstleistervereinbarung
Es wird zwischen Auftraggeber (Schule XYZ) und Dienstleister (Fotograf, Homepagegestalter etc.) vereinbart:

1. Der Dienstleister verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden.
2. Der Dienstleister erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Wahrung des Datengeheimnisses im Sinne des § 15 DSG 2000 verpflichtet hat. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Dienstleister aufrecht.
3. Der Dienstleister erklärt rechtsverbindlich, dass er ausreichende Sicherheitsmaßnahmen im Sinne des § 14 DSG 2000 ergriffen hat, um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden.
4. Der Dienstleister kann ein anderes Unternehmen als weiteren datenschutzrechtlichen Dienstleister nur dann heranziehen, wenn der Auftraggeber zustimmt. Der Dienstleister muss mit dem Subverarbeiter einen Vertrag im Sinne des § 10 DSG 2000 abschließen. In diesem Vertrag hat der Dienstleister sicherzustellen, dass der Subverarbeiter dieselben Verpflichtungen eingeht, die dem Dienstleister auf Grund des DSG 2000 sowie dieser Vereinbarung und der zugrunde legenden Beauftragung obliegen.
5. Der Dienstleister trägt für die technischen und organisatorischen Voraussetzungen Vorsorge, dass der Auftraggeber die Bestimmungen der § 26 (Auskunftsrecht) und § 27 (Recht auf Richtigstellung oder Löschung) DSG 2000 gegenüber dem Betroffenen innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen.
6. Der Dienstleister ist nach Beendigung der Dienstleistung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber in einem allgemein verfügbaren Format zu übergeben bzw. in dessen Auftrag für ihn weiter vor unbefugter Einsicht gesichert aufzubewahren oder ansonsten zu vernichten.
7. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen eingeräumt. Der Dienstleister verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.
8. Der Dienstleister verpflichtet sich, bei einer elektronischen Übermittlung von Daten technische Verfahren mit Authentifikation und Verschlüsselung nach den üblichen Sicherheitsstandards anzuwenden.
9. Für die IT-Systeme des Dienstleisters sind die einschlägigen Vorgaben des Österreichischen Informationssicherheitshandbuches in der geltenden Fassung anzuwenden. Das für den Betrieb herangezogene Rechenzentrum muss jedenfalls eine gültige Zertifizierung nach ISO 27001 besitzen.

B. Mustervereinbarung: Schule – Erziehungsberechtigte

Soweit die Datenverarbeitung ausschließlich im Rahmen der Digitalen Schülerverwaltung – Sokrates im Bund und anderer vom BMBF generell beauftragter Verwaltungsanwendungen (z.B. Web-Untis) erfolgt ist keine explizite Zustimmung erforderlich. Sie ist erforderlich, wenn die Verarbeitung personenbezogener Schülerdaten nicht auf Grund einer gesetzlichen Grundlage erfolgt (z.B. Ausstellung einer edu.card, Verarbeitung von Daten auf der Schulhomepage, etc.).

Ich, xxx (Name, Adresse) stimme zu, xxx

dass meine persönlichen Daten, – ODER , dass die personenbezogenen Daten meines Kindes, Name xxx,

nämlich [Datenarten aufzählen, z.B. Name, Adresse, Geburtsdatum …]

zum Zweck der [genauen Zweck anführen,]

verarbeitet werden.

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

Checkliste

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

- Wer ist datenschutzrechtlicher Auftraggeber?

☐ Schulleitung ☐ BMBF ☐ Anderer: _____

- Wer sind die Betroffenen?

☐ Schülerinnen und Schüler

☐ Erziehungsberechtigte ☐ Andere: _____

- Welche personenbezogenen Daten werden verwendet?

☐ Namen ☐ Adresse ☐ Bildnis

☐ Andere: _____

_____

_____

- Werden sensible personenbezogenen Daten verwendet?

☐ Nein ☐ Ja

Wenn ja, welche

☐ ethnische/rassische Herkunft

☐ religiöse/philosophische Überzeugung

☐ 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 Dienstleister: _____

Wenn Dienstleister, Dienstleistungsvereinbaung abgeschlossen?

☐ Ja ☐ Nein

- Ist die Verwendung erforderlich bzw. verhältnismäßig? Wieso ist die Verwendung 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 wesentliche Voraussetzung für die Wahrnehmung einer gesetzlich übertragenen Aufgabe); welche gesetzlich übertragene Aufgabe?

  - SchUG
  - Andere

  Konkrete Bestimmung nennen: _____

- Zustimmung

  Schriftliche Zustimmung der Betroffenen eingeholt?

  - Ja
  - Nein

- Lebenswichtiges Interesse (Medizinischer Notfall)
- Andere rechtliche Grundlage: _____

Rechtstexte

Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000 idF BGBl. I Nr. 57/2013)

Artikel 1 (Verfassungsbestimmung)
Grundrecht auf Datenschutz

§ 1. (1) 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.

(2) 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. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) 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.

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

(5) Gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, ist, soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen. In allen übrigen Fällen ist die Datenschutzbehörde zur Entscheidung zuständig, es sei denn, daß Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind.«

…

2. Abschnitt
Verwendung von Daten
Grundsätze

§ 6. (1) Daten dürfen nur

1. nach Treu und Glauben und auf rechtmäßige Weise verwendet werden;
2. für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden; die Weiterverwendung für wissenschaftliche oder statistische Zwecke ist nach Maßgabe der §§ 46 und 47 zulässig;
3. soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;
4. so verwendet werden, daß sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind;
5. solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

(2) Der Auftraggeber trägt bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der in Abs. 1 genannten Grundsätze; dies gilt auch dann, wenn er für die Datenanwendung Dienstleister heranzieht.

…

§ 7. (1) Daten dürfen nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.

(2) Daten dürfen nur übermittelt werden, wenn

1. sie aus einer gemäß Abs. 1 zulässigen Datenanwendung stammen und
2. der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis – soweit diese nicht außer Zweifel steht – im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und
3. durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

(3) Die Zulässigkeit einer Datenverwendung setzt voraus, daß die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und daß die Grundsätze des § 6 eingehalten werden. Schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten

§ 8. (1) Schutzwürdige Geheimhaltungsinteressen sind bei Verwendung nicht-sensibler Daten dann nicht verletzt, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder
2. der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
3. lebenswichtige Interessen des Betroffenen die Verwendung erfordern oder

4. überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern.

(2) Bei der Verwendung von zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten gelten schutzwürdige Geheimhaltungsinteressen als nicht verletzt. Das Recht, gegen die Verwendung zulässigerweise veröffentlichter Daten gemäß §28 Widerspruch zu erheben, bleibt unberührt.

(3) Schutzwürdige Geheimhaltungsinteressen sind aus dem Grunde des Abs. 1 Z 4 insbesondere dann nicht verletzt, wenn die Verwendung der Daten

1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist oder
2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder
3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist oder
4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenem erforderlich ist oder
5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
6. ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat oder
7. im Katastrophenfall, soweit dies zur Hilfeleistung für die von der Katastrophe unmittelbar betroffenen Personen, zur Auffindung und Identifizierung von Abgängigen und Verstorbenen und zur Information von Angehörigen notwendig ist; im letztgenannten Fall gilt §48a Abs. 3.

Bundesgesetz über die Dokumentation im Bildungswesen Bildungsdokumentationsgesetz, BGBl. I Nr. 12/2002 idF BGBl. I Nr. 77/2013

2. Teil
Evidenzen der Bildungseinrichtungen und Gesamtevidenzen
Evidenzen der Schüler und Studierenden

§3. (1) Der Leiter einer Bildungseinrichtung gemäß §2 Abs. 1 Z 1 lit. a, b, c, f, g und h sowie Z 2 hat für die Vollziehung des Schulunterrichtsgesetzes, BGBl. Nr. 472/1986, des Schulunterrichtsgesetzes für Berufstätige, Kollegs und Vorbereitungslehrgänge, BGBl. I Nr. 33/1997, des Hochschulgesetzes 2005, BGBl. I Nr. 30/2006, des Universitätsgesetzes 2002, BGBl. I Nr. 120, sowie der sonstigen schul- und hochschulrechtlichen Vorschriften folgende schülerbezogene und studierendenbezogene Daten nach Maßgabe der technischen Möglichkeiten automationsunterstützt zu verarbeiten (§4 Z 9 Datenschutzgesetz 2000, BGBl. I Nr. 165/1999):#

1. die Namen (Vor- und Familien- bzw. Nachnamen, einschließlich allfälliger akademischer Grade),
2. das Geburtsdatum,
3. die Sozialversicherungsnummer,
4. das Geschlecht,
5. die Staatsangehörigkeit,
6. die Anschrift am Heimatort und, sofern zusätzlich vorhanden, des der Bildungseinrichtung nächst gelegenen Wohnsitzes (Zustelladresse) entsprechend den Angaben der Erziehungsberechtigten bzw. des Schülers bzw. des Studierenden,

7. das Beginndatum der jeweiligen Ausbildung unter Angabe deren Bezeichnung,
8. das Beendigungsdatum und die Beendigungsform der jeweiligen Ausbildung unter Angabe der Bezeichnung der beendeten Ausbildung und
9. das allfällige bildungseinrichtungsspezifische Personenkennzeichen (z. B. Matrikelnummer).

(2) Der Leiter einer Bildungseinrichtung gemäß § 2 Abs. 1 Z 1 lit. a, b, c, f, g und h hat über Abs. 1 hinaus folgende Daten schülerbezogen zu verarbeiten:

1. das von den Erziehungsberechtigten bzw. vom Schüler angegebene Religionsbekenntnis,
2. das erste Jahr der allgemeinen Schulpflicht,
3. einen festgestellten sonderpädagogischen Förderbedarf,
4. die Eigenschaft als ordentlicher oder außerordentlicher Schüler,
5. die Schulkennzahl,
6. die Schulformkennzahl,
7. andere 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.

…

(4) Im Fall der Ablegung einer Externistenprüfung gemäß § 42 des Schulunterrichtsgesetzes, BGBl. Nr. 472/1986 (einschließlich § 8c des Schulorganisationsgesetzes, BGBl. Nr. 242/1962), bzw. § 42 des Schulunterrichtsgesetzes für Berufstätige, Kollegs und Vorbereitungslehrgänge, BGBl. I Nr. 33/1997, sowie im Fall der Ablegung einer Prüfung gemäß §§ 11 Abs. 4, 13 Abs. 3 und § 22 Abs. 4 des Schulpflichtgesetzes 1985, BGBl. Nr. 76, hat der Leiter der Bildungseinrichtung, an der die Externistenprüfung durchgeführt wird, die Prüfungskandidaten evident zu halten. Der Leiter dieser Bildungseinrichtung hat nach Maßgabe der technischen Möglichkeiten automationsunterstützt prüfungskandidatenbezogene Daten gemäß Abs. 1, Abs. 2 Z 2, 5 und 6 sowie gemäß Anlage 2 zu verarbeiten.

(5) Sofern von einer Prüfung gemäß § 13 Abs. 3 des Schulpflichtgesetzes 1985, BGBl. Nr. 76, abgesehen wird sowie bei Befreiung vom Besuch der Berufsschule gemäß § 23 des Schulpflichtgesetzes 1985, BGBl. Nr. 76, und bei Befreiung vom Schulbesuch gemäß § 15 des Schulpflichtgesetzes 1985, BGBl. Nr. 76, kann der jeweils zuständige Landesschulrat bzw. Bezirksschulrat mit der Evidenthaltung dieser Personen den Leiter der Bildungseinrichtung betrauen, welcher nach Maßgabe des dauernden Aufenthaltes der betreffenden Person und unter Bedachtnahme auf die jeweilige vom Landes- bzw. Bezirksschulrat entschiedene Angelegenheit geeignet ist. Der jeweils zuständige Landesschulrat oder Bezirksschulrat bzw. der betraute Leiter der Bildungseinrichtung hat nach Maßgabe der technischen Möglichkeiten automationsunterstützt personenbezogene Daten gemäß Abs. 1 und Abs. 2 Z 2 und 7 zu verarbeiten.

(6) Der Schüler … hat die Sozialversicherungsnummer dem Leiter der Bildungseinrichtung bekannt zu geben. Sofern eine österreichische Sozialversicherungsnummer nicht besteht, hat die Bildungseinrichtung der Bundesanstalt »Statistik Österreich« Familien- bzw. Nachnamen und Vornamen, Geschlecht, Geburtsdatum und Anschrift am Heimatort zwecks Zuweisung eines Ersatzkennzeichens im automationsunterstützten Datenverkehr bekannt zu geben; liegt der Heimatort im Ausland und besteht ein Wohnsitz im Inland, so ist letzterer zu verwenden. Geben solche Schüler … später der Bildungseinrichtung eine Sozialversicherungsnummer bekannt, so ist bei deren erstmaliger Übermittlung an die Bundesanstalt »Statistik Österreich« die

Ersatzkennzeichnung zusätzlich anzugeben. Der Empfänger hat alle Datensätze dieser Person auf die Sozialversicherungsnummer zusammenzuführen und entsprechend zu speichern.

(7) Die Bundesanstalt »Statistik Österreich« ist berechtigt, mittels der für das Ersatzkennzeichen vorhandenen Daten eine Abfrage im Zentralen Melderegister durchzuführen und für das Ersatzkennzeichen das verschlüsselte bereichsspezifische Personenkennzeichen »Sozialversicherung« und das verschlüsselte bereichsspezifische Personenkennzeichen »Amtliche Statistik« gemäß § 9 des E-Government-Gesetzes (E-GovG), BGBl. I Nr. 10/2004, zu ermitteln. Auf Verlangen der Bundesanstalt hat der Hauptverband der österreichischen Sozialversicherungsträger die Sozialversicherungsnummern zu den verschlüsselten bereichsspezifischen Personenkennzeichen »Sozialversicherung« zu ermitteln und die Sozialversicherungsnummern mit den verschlüsselten bereichsspezifischen Personenkennzeichen »Amtliche Statistik« an die Bundesanstalt Statistik Österreich zu übermitteln.