Überarbeitete Erläuterungen

Ergänzt und eingearbeitet wurden Anregungen und Präzisierungen, die sich aus Stellungnahmen im Zuge der Begutachtung ergaben.

Allgemeiner Teil

Hauptgesichtspunkte des Entwurfes:

Mit dem Bildungsdokumentationsgesetz 2020 – BilDokG 2020, BGBl. I Nr. 20/2021, dem Bundesgesetz zur Finanzierung der Digitalisierung des Schulunterrichts – SchDigiG, BGBl. I Nr. 9/2021 und der Novelle zu den §§ 14a und 70a Schulunterrichtgesetz – SchUG, BGBl. I Nr. 19/2021 wurden rechtliche Rahmenbedingungen für den IT-Einsatz im Schulbereich festgelegt sowie insbesondere in § 4 BilDokG 2020 und § 6 SchDigiG Bestimmungen zur Datensicherheit eingeführt. Diese legistische Entwicklung zeigt die Bedeutung des IT-Einsatzes an Schulen wie auch die Umsetzung des Strategiepapiers „Masterplan des Bundesministers für Bildung, Wissenschaft und Forschung für die Digitalisierung im Bildungswesen“ aus dem Jahr 2019 (https://www.bmbwf.gv.at/Themen/schule/zrp/dibi/mp.html). Der vorliegende Entwurf soll eine der rechtlichen Grundlagen für die Umsetzung des am 17. Juni 2020 durch den Bundesminister für Bildung, Wissenschaft und Forschung gemeinsam mit dem Herrn Bundeskanzler der Öffentlichkeit vorgestellten 8-Punkte-Plans für den digitalen Unterricht sein.

Die Zwecke der Verarbeitung von Daten, insbesondere gemäß der Art. 5 und 6 DSGVO im Zusammenhang mit der Bildungsdokumentation ergeben sich überwiegend aus den Regelungen zur Bildungsdokumentation, den Bestimmungen des Schulrechts sowie aus anderen einschlägigen Bestimmungen einzelner Materiengesetze wie zB § 42g des Urheberrechtsgesetzes, BGBl. Nr. 111/1936 (Öffentliche Zurverfügungstellung von Werken für Unterricht und Lehre) oder aus dem Familienlastenausgleichsgesetz 1967, BGBl. Nr. 376/1967. Weitere Verarbeitungszwecke ergeben sich, wenn auch nur zu einem geringen Ausmaß, aus der Erbringung von Serviceleistungen durch das schulische Umfeld auf Schülerinnen- oder Schülerwunsch (etwa: Kopiersysteme, WLAN-Zugänge an Schulen, Essensbestellungen, Berechtigungsnachweise für die Schülerfreifahrt oder Bereitstellung von vergünstigten Software-Lizenzen).

Aufgrund der Bestimmungen der DSGVO sind neben den Verarbeitungszwecken angemessene Mittel für die Datenverarbeitung (zB Schulverwaltungsprogramme) und damit zusammenhängend geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit zu definieren. Die Festlegung der Mittel für die schulische Datenverarbeitung erfolgte bisher in sehr heterogener Art durch unterschiedliche Akteure im Bildungswesen (BMBWF, Schulerhalter, Bildungsdirektionen, Schulleitungen, Lehrpersonal sowie diesbezügliche schulgemeinschaftliche Gremien).

Hauptziel dieser Verordnung ist die Festlegung gemeinsamer Standards hinsichtlich der Datensicherheit und damit die Harmonisierung der Anforderungen an die eingesetzten Mittel, insbesondere an die Software (im Sinne von IT-Systemen und Diensten) im Bereich der Schulverwaltung. Zu diesem Zweck legt die Verordnung in Entsprechung der Art. 25 und 32 DSGVO in Verbindung mit Erwägungsgrund 78 der DSGVO geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus fest. Diese Maßnahmen haben insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge zu tun. Neben den schulgesetzlichen Vorgaben berücksichtigt die Verordnung auch die Dokumentationen, die gemäß § 4 Abs. 2 BilDokG 2020 zu führen sind, eine durch das BMBWF durchgeführte Datenschutz-Folgenabschätzung, Verzeichnisse der schulischen Verarbeitungstätigkeiten gemäß Art. 30 DSGVO, sowie die regelmäßig aktualisierte Datenschutzinformation des BMBWF (https://www.bmbwf.gv.at/Themen/schule/schulrecht/ds.html) gemäß Art. 12 ff DSGVO im Rahmen der Schulverwaltung an österreichischen Schulen.

Neben diesen technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit regelt die Verordnung auch die gegenseitigen Verpflichtungen bei Datenverarbeitungen durch gemeinsame Verantwortliche gemäß Art. 26 DSGVO. Nicht Gegenstand dieser Verordnung sind Regelungen gemäß § 4 Abs. 3 Z 2 BilDokG 2020, wobei aber geplant ist, den in § 6 dieser Verordnung geregelten Bildungsportalverbund auch für Zwecke der Ermittlung des bereichsspezifischen Personenkennzeichens aus dem Stammzahlenregister gemäß den Bestimmungen einer späteren Verordnung zu § 4 Abs. 3 Z 2 BilDokG 2020 einzusetzen.

Neben dem großen Bereich des Datenschutzes in der Schulverwaltung enthält die Verordnung einen zweiten großen Bereich zum IT-Einsatz im pädagogischen Umfeld (IKT-gestützter Unterricht).

Die Verordnung ist somit folgendermaßen aufgebaut:

Zuerst werden Kategorien von schulischen Verarbeitungstätigkeiten festgelegt. Auf diesen aufbauend werden technische und organisatorische Maßnahmen zum Hosting, zur Authentifizierung an Endgeräten, zum Aufbau eines Identity- und Access-Management-Systems im Rahmen von Bildungsstammportalen, sowie zu IT-Systemen und Diensten sowie zu den eingesetzten Endgeräten geregelt. Neben der Festlegung geeigneter technischer und organisatorischer Maßnahmen werden schließlich IT-Nutzungsbedingungen festgelegt, die einen über den Datenschutz hinausgehenden rechtskonformen IT-Einsatz im schulischen Umfeld, insbesondere bezüglich urheberrechtlicher, strafrechtlicher oder wettbewerbsrechtlicher Vorschriften, gewährleisten sollen.

Aus Gründen der Effizienz und Vereinheitlichung der Verwaltung werden hier auch allgemeine Standards und Richtlinien der österreichischen E-Government-Strategie berücksichtigt, wie etwa das E-Government-Gesetz,– E-GovG, BGBl. I Nr.10/2004, das Netz- und Informationssystemsicherheitsgesetz – NISG, BGBl. I Nr. 111/2018, das Portalverbundprotokoll (https://neu.ref.wien.gv.at/at.gv.wien.ref-live/web/reference-server/ag-iz-portalverbund), Ergebnisse der Interministerielle Arbeitsgruppe Cloud Computing (AG Cloud), sowie Schnittstellen im Rahmen des Registerverbundes etwa zum Stammzahlenregister und anderen behördlichen Registern (Registerverbundsystem).

Besonderer Teil

Zu §§ 1 und 2 (Geltungsbereich und Regelungszweck):

Geltungsbereich und Regelungszweck sollen aufzeigen, dass mehrere Regelungsbereiche mit Bezug zum Schulwesen im Interesse der Rechtsklarheit und der Verständlichkeit für die Normadressaten in einer einheitlichen Verordnung geregelt werden sollen.

Zu § 4 (Begriffsbestimmungen):

Zu Z 1 bis 4:

In den Z 1 bis 4 werden vier unterschiedliche Kategorien von schulischen Verarbeitungstätigkeiten definiert, „Schulverwaltung“, „Endgeräteverwaltung (Mobile Device Management)“, „Unterrichtsdokumentation“ und „IT-Services für pädagogische Zwecke“. Aufbauend auf dieser inhaltlichen Abgrenzung ordnen die weiteren Bestimmungen der Verordnung unterschiedliche technische und organisatorische Maßnahmen bezüglich der einzelnen technischen Verfahren (Authentifizierung und Berechtigungsverwaltung der Benutzer und Benutzerinnen im Bildungsstammportal, Hosting und weitere Anforderungen an IT-Systeme und Dienste sowie Anforderungen an Endgeräte und deren Verwaltung (MDM)) zu.

Aufgrund der besonderen Schutzbedürftigkeit der im Rahmen der Schulverwaltung zu verarbeitenden Daten sollen in Z 1 für die Verarbeitungstätigkeiten der Organe der Schulverwaltung höhere Anforderungen vorgesehen werden als für Verarbeitungstätigkeiten zu pädagogischen Zwecken (zB zur Unterrichtsdokumentation). Bei der Risikobeurteilung wurde berücksichtigt, dass schulische Organe im Rahmen von Tätigkeiten der Schulverwaltung Zugriffsmöglichkeiten auf größere Datensätze, zB auf die Daten aller Schülerinnen und Schüler einer Schule, benötigen, als einzelne Lehrpersonen im Rahmen der Unterrichtsdokumentation. Die Verarbeitung personenbezogener Daten nach Art. 9 DSGVO ist ausschließlich Teil der Verarbeitungstätigkeit Schulverwaltung nach Z 1 mit Ausnahme jener Daten, die im Rahmen der Unterrichtsdokumentation für den Vollzug des Schulunterrichtsgesetzes notwendig sind, wie insbesondere die Aufzeichnung von Rechtfertigungsgründen bei einer Verhinderung an der Teilnahme am Unterricht gemäß § 45 SchUG oder § 9 des Schulpflichtgesetzes 1985, BGBl. Nr. 76/1985. Dabei sind die Datensicherheitsmaßnahmen zum Klassenbuch gemäß § 77 Abs. 2 bis 4 des Schulunterrichtsgesetzes, insbesondere hinsichtlich der (programmtechnischen) Zugriffsbeschränkungen und der Löschungsbestimmung, zu beachten. Der Zugriff für Lehrpersonen soll auf einzelne Klassen und die von der Lehrperson unterrichteten Schülerinnen und Schüler beschränkt sein und sich inhaltlich im Wesentlichen auf die Unterrichtsdokumentation, einschließlich kontinuierlicher Leistungsfeststellung (zB Dokumentation der Mitarbeit) beziehen.

Zu Z 2 und 5:

Der Terminologie des § 6 SchDigiG folgend soll bezüglich der sicheren Integration mobiler Endgeräte in die IKT-Infrastruktur der Schule (Schulnetz im Sinne der Verordnung) zwischen „Endgeräteverwaltung“ und „Fernverwaltung“ unterschieden werden. Die Endgeräteverwaltung wird in § 10 des gegenständlichen Entwurfs näher geregelt. Für die Fernverwaltung ist auf Grund hinreichender Determinierung in § 6 SchDigiG keine weitere Regelung von technischen Maßnahmen durch die Verordnung notwendig. Insbesondere ist diesbezüglich schon direkt in § 6 Z 2 SchDigiG vorgeschrieben, dass eine Fernverwaltung

nur während des Unterrichts, nur auf Geräte der gerade teilnehmenden Schülerinnen und Schüler und nicht unbemerkt durch diese stattfinden kann.

Die Endgeräteverwaltung soll dabei nicht auf Endgeräte gemäß § 6 Z 1 SchDigiG eingeschränkt sein, sondern auch zur Verwaltung anderer schulbezogener Endgeräte eingesetzt werden können. Typische Lösungen umfassen eine Serverkomponente (Client-Server-Modell), die die Verwaltungsbefehle an die mobilen Geräte sendet, und eine Clientkomponente, die auf dem verwalteten Gerät ausgeführt wird und die Verwaltungsbefehle empfängt und implementiert.

Zu Z 9:

Unter Auftragsverarbeiterinnen und Auftragsverarbeitern für IT-Systeme und Dienste sollen nicht nur spezialisierte Unternehmen aus der Privatwirtschaft zu verstehen sein, sondern auch Rechenzentren, die von der öffentlichen Hand betrieben werden und die Bildungsstammportale, Lernplattformen und andere schulische IT-Systeme und Dienste betreiben. Im Sinne eines Shared Service für mehrere Schulen sollen unter Einhaltung der Anforderungen des § 8 Abs. 3 der Verordnung auch IT-Services für mehrere Schulen oder mehrere Schulerhalter bei einer Auftragsverarbeiterin oder einem Auftragsverarbeiter gehostet werden können.

Zu Z 10:

Mit dieser Bestimmung soll verdeutlicht werden, dass die im Rahmen des SchDigiG durch den Bund zentral beschafften und ausgegebenen Endgeräte Arbeitsmittel gemäß § 14a iVm § 61 SchUG darstellen.

Zu Z 11:

Zu Z 11 ist zu erwähnen, dass auch ein Zugang mit dem Endgerät über VPN ortsunabhängig vom Schulstandort eine Verwendung des Schulnetzes ist.

Zu § 5 (Authentifizierung):

Grundsätzlich ist bei der Anmeldung zur Nutzung von IT-Systemen eine Authentifizierung durch Benutzerkennung und Passwort erforderlich, wobei die Passwörter ausreichend komplex sein müssen. Hinsichtlich der Datenverarbeitungen zu Zwecken der Schulverwaltung und der Endgeräteverwaltung bestehen höhere Maßstäbe. Hier ist zusätzlich eine Mehr-Faktor-Authentifizierung erforderlich.

Da zurzeit die Bürgerkarte/E-ID am stärksten in der Ausprägung der Handysignatur im Schulwesen Einzug gefunden hat, empfiehlt sich diese konkrete Technik zur Umsetzung der Zwei-Faktor-Authentifizierung. An fixen Arbeitsplätzen, zu denen ausschließlich durch Bedienstete der jeweiligen Dienststelle Zutritt besteht, kann der Zugangstoken zum Raum als zweiter Faktor angesehen werden, um eine Kompatibilität zu den mit Bundes-Clients ausgestatteten Verwaltungsarbeitsplätzen zu gewährleisten. Dies ist als Mindestanforderung zu verstehen, so können auch sicherheitstechnisch höherwertige Systeme, wie etwa eine Mehr-Faktor-Authentifizierung eingesetzt werden

Zu § 6 (Bildungsstammportale und Bildungsportalverbund):

Auf Grund des quantitativen Umfangs der beteiligten Personen und Dienststellen, (rund 1 Million Schülerinnen und Schüler, 120.000 Lehrpersonen, 6.000 Schulleitungen) ist ein hochwertiges Identity-und Access-Management-System zu verschiedenen Anwendungen im Bildungsbereich nur über Bildungsstammportale und des in der föderalen Verwaltung seit 20 Jahren bewährten Portalverbundprotokolls hinreichend sicher und effizient zu realisieren. Neben der datenschutzrechtlich notwendigen hochwertigen Authentifizierung und Berechtigungskontrolle kann durch Stammportale auch die Verwaltung von bereichsspezifischen Personenkennzeichen-Bildung und Forschung (bPK-BF) für alle Schülerinnen und Schüler sowie Lehr- und Schulverwaltungspersonal effizient gewährleistet werden. Technisch baut der Bildungsportalverbund weitgehend auf den Spezifikationen des allgemeinen Verwaltungs-Portalverbundes auf. Insbesondere auf Grund der Größe des Benutzerkreises (alle Schülerinnen und Schüler, Lehr- und Verwaltungspersonal) werden dafür technisch erforderliche Adaptionen im Rahmen des Bildungsportalverbundprotokolls und einer dazugehörigen Bildungsportalverbundvereinbarung unter Federführung des BMBWF spezifiziert und auf der Webseite des Ressorts veröffentlicht.

Die Notwendigkeit eines Bildungsportalverbundes kommt durch Erwägungsgrund 49 der DSGVO klar zum Ausdruck, der die Verarbeitung personenbezogener Daten als berechtigtes Interesse darlegt, „soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Ein solch berechtigtes

Interesse könnte beispielsweise darin bestehen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of service"-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren."
Der Bildungsportalverbund verfolgt dieselben Zwecke und Ziele wie der bestehende E-Government-Portalverbund, der auf Vereinbarungsebene zwischen Portalverbundbetreibern gegründet ist.
Unterschiede können in technischen und organisatorischen Maßnahmen auftreten, da Bildungsstammportale im Gegensatz zu E-Government-Stammportalen nicht nur Bedienstete verwalten, sondern auch die große Gruppe der Schülerinnen und Schüler und der Erziehungsberechtigten umfassen.
Auch die Bildungsportalverbundvereinbarung, die für die Betreiber aller teilnehmenden Stammportale gilt, dient der Festlegung von Rechten und Pflichten.

Abs. 1 soll vorsehen, dass das für die Schulverwaltung verantwortliche oberste Organ der Bundesverwaltung, die Bundesministerin bzw. der Bundesminister für Bildung, Wissenschaft und Forschung, für alle öffentlichen und privaten Schulen ein Bildungsstammportal betreiben soll. Dieses Bildungsstammportal soll die Benutzer (Schülerinnen, Schüler, Lehr- und Verwaltungspersonal) aller Schulen umfassen, sofern nicht die Regelung des Abs. 2 greift. Die Integration privater Schulen ergibt sich daraus, dass das Bildungsstammportal auch Anwendungen zum Vollzug des Bildungsdokumentationsgesetzes zugänglich macht und dieser Teil der Verordnung auf dem für alle Schulen anzuwendenden BilDokG 2020 beruht.

Abs. 2 soll für Stellen nach § 15 Z. 2 der Verordnungdie Möglichkeit schaffen, ein Bildungsstammportal für den eigenen Bereich zu errichten und zu betreiben. Diese kann sich unmittelbar aus der Eigenschaft als Schulerhalter ergeben, aus einer Vollzugszuständigkeit oder durch eine zivilrechtliche Vereinbarung begründet werden.

Abs. 4 enthält eine Bestimmung zur Kostentragung. Nützt eine solche Stelle bzw. ein Dienstgeber das Bildungsstammportal des Bundes gemäß Abs. 1, so hat dieser die Kosten zu tragen, die durch die Herstellung und den Betrieb der Schnittstelle zur Anbindung seiner Schülerverwaltungs- bzw. Personalverwaltungssoftware an das Bildungsstammportal des Bundes entstehen.

Zu § 7 (Anforderungen an IT-Systeme und Dienste):

In Österreich sowie auch international gibt es einen mannigfaltigen Markt unterschiedlichster Anwendungen von einer Vielzahl von Firmen oder gemeinnützigen Institutionen, die Services für den Schulbereich anbieten. Grundsätzlich ist davon auszugehen, dass ein Anbieter eines solchen IT-Systems oder Dienstes die Einhaltung aller rechtlichen Anforderungen (insb. jener dieser Verordnung) gewährleistet und dies der jeweiligen Auftraggeberin oder dem jeweiligen Auftraggeber als Verantwortlicher oder Verantwortlichem zusichert.

Für die aus Sicht des BMBWF bundesweit relevanten Anwendungen und Anbieter soll nach Absolvierung eines Qualitätssicherungsprozesses, der Überprüfung der IT-Sicherheit und einer generellen Testung eine Auftragsverarbeitervereinbarung mit den Anbietern abgeschlossen werden. Der Text dieser Auftragsverarbeitervereinbarung ist unter https://www.bmbwf.gv.at/Themen/schule/schulrecht/ds.html#12 veröffentlicht.

Wenn solche IT-Systeme und Dienste bundesweit für alle Schulen über das Portal Digitale Schule (PoDS) zur Verfügung gestellt werden, ist der Abschluss der Vereinbarung durch das BMBWF vorgesehen. Wenn sie jedoch nur regional eingesetzt werden (etwa ein Schulverwaltungsprogramm für Pflichtschulen eines Bundeslandes), ist eine solche Vereinbarung durch jene Stelle gemäß § 15 Z. 2 abzuschließen. Die Verwendung des Vertragsmusters des BMBWF für den Abschluss einer Auftragsverarbeitervereinbarung im Bildungsbereich wird auch anderen Schulerhaltern empfohlen, die eine Auftragsverarbeitervereinbarung gemäß § 7 dieser Verordnung abschließen.

Um die sicherheitstechnischen Anforderungen an Endgeräte möglichst gering zu halten, ist darauf zu achten, dass im Regelfall bei Verwendung eines IT-Systems und Dienstes keine personenbezogenen Daten am Endgerät selbst gespeichert werden. Dies wird am besten durch eine strikte webbasierte Strukturierung der IT-Systeme und Dienste sichergestellt, sodass durch die Endgeräteverwaltung nur eine sichere Webbrowser-Umgebung zur Verfügung gestellt werden muss. Durch die Verlagerung der IT-Sicherheitsmaßnahmen auf die zentral bereitgestellten IT-Systeme und Dienste wird dort eine diesbezügliche Sicherheitstestung erforderlich. Daher sieht Abs. 2 die verpflichtende Durchführung eines PEN-Testes und einer Third-Party-Review vor Inbetriebnahme vor, wie es bei Verwaltungsanwendungen ein üblicher Sicherheitsstandard ist. Diese Tests werden etwa durch externe Experten (etwa A-SIT, SBA-Research, TÜV-Trust uä.) durchgeführt. Damit soll im Wesentlichen auch die erforderliche Datensicherheit bei Zulässigkeit der Verwendung privater Geräte von Lehrpersonen sichergestellt werden.

Zu § 8 (Hosting):

Die Anforderungen an Rechenzentren, in denen IT-Systeme und Dienste gemäß § 4 Z 1 (Schulverwaltung) gehostet werden, sind direkt aus den diesbezüglichen Bestimmungen des § 17 des Netz- und Informationssystemsicherheitsgesetzes – NISG, BGBl. I Nr. 111/2018, übernommen und wurden dort als ausreichende Sicherheitsvorkehrungen für Betreiber wesentlicher [IT-]Dienste definiert. Für IT-Systeme aus dem Bereich der Schulverwaltung, die direkt durch das BMBWF beauftragt wurden, ist nach derzeitigem Stand sichergestellt, dass alle IT-Systeme in Rechenzentren der öffentlichen Hand gehostet werden. Auch werden die Schulverwaltungssysteme der Pflichtschulerhalter weitgehend in den Rechenzentren der Landesregierungen gehostet. Da dies aber nicht auch durchgehend für Schulverwaltungssysteme anderer Schulerhalter zutrifft, soll diesbezüglich auf die in § 17 NISG geregelten (Mindest-)Anforderungen zurückgegriffen werden. Die beauftragten Rechenzentren sind als Auftragsverarbeiter gem. Art. 4 Z 8 DSGVO anzusehen.

Die Anforderungen an Rechenzentren, in denen IT-Systeme und Dienste gemäß § 4 Z 2 bis 4 dieser Verordnung gehostet werden sollen, sollen um Clouddiensteanbieterinnen und -anbieter erweitert werden, die alle diesbezüglichen Anforderungen des BMBWF erfüllen. Dieser Befund ergibt sich aus einer vom BMBWF vorgenommenen ausführlichen Risikobeurteilung, welche im Wesentlichen zum Ergebnis kommt, dass die IT-Sicherheit für die betreffende Größe der Benutzergruppe am besten durch pädagogische IT-Services und Dienste zu realisieren ist. Dies ist in den vom BMBWF herausgegebenen „Rahmenbedingungen für den Einsatz privater Clouddiensteanbieter im IT-gestützten Unterricht“ vom 25. September 2020 ausführlich beschrieben und setzt u.a. geeignete Nachweise durch die Clouddiensteanbieterinnen und -anbieter voraus, um zu dokumentieren, dass alle Anforderungen der DSGVO (insbesondere auch die Erkenntnisse des EuGH im Fall Schrems II) berücksichtigt wurden. Clouddiensteanbieterinnen und -anbieter, die diese Nachweise gegenüber dem BMBWF erbracht haben, sind auf der Homepage des Ressorts gelistet (https://www.bmbwf.gv.at/Themen/schule/schulrecht/ds.html#08).

Zu § 9 (Organisatorische Datensicherheitsmaßnahmen):

Die DSGVO sieht sowohl technische als auch organisatorische Maßnahmen zur Gewährleistung der erforderlichen Datensicherheit vor. Die jeweiligen organisatorischen Maßnahmen sind überwiegend vor Ort an den Schulstandorten zu realisieren, daher sollen die Schulleitungen als Verantwortliche vorgesehen werden.

Die Belehrungen können im Zuge der allgemeinen Seminare für neueintretende Bedienstete an den Schulstandorten abgehalten werden oder in verkürzter Form auch im Rahmen der regelmäßig stattfindenden pädagogischen Konferenzen erfolgen. Schulungsunterlagen wurden im Publikationenshop des BMBWF (https://pubshop.bmbwf.gv.at/index.php?article_id=10) veröffentlicht.

Zu § 10 und § 11 (Endgeräteverwaltung für digitale Endgeräte und Anwendungsbezogene Anforderungen an digitale Endgeräte):

Wie schon in den gesetzlichen Erläuterungen grundsätzlich ausgeführt, ist zur Sicherung von Funktionalität und Sicherheit der Geräte als geeignete technische Maßnahme die Integration der Geräte in eine durch die Schule betriebene Endgeräteverwaltung (Mobile Device Management – MDM) vorgesehen. Dadurch können von der Schule im Unterricht benötigte Anwendungen und Richtlinien einfach auf alle Geräte eines Schulstandortes aufgebracht werden. Allein aufgrund der hohen Zahl an Geräten, im Endausbau – dh. über alle vier Schulstufen der Sekundarstufe I sind dies, einschließlich der Geräte für Lehrpersonen rund vierhunderttausend Geräte – wäre keine andere Vorgangsweise möglich. Schon ab zehn Geräten ist eine gute Wartung der Geräte ohne MDM durch eine „Einzeladministration“ de facto nicht mehr leistbar.

Das Endgerätemanagement dient als technische Maßnahme im Rahmen der IT-Sicherheit, die Programmteile (Betriebssystem und Anwendungen) aktualisiert hält. Die Funktionen des MDM sind so auszugestalten, dass auf die Bereiche am Endgerät nicht über die obigen Aspekte der IT-Sicherheit (Schutz von Schadsoftware, Einhaltung der IT-Sicherheitsrichtlinien) hinausgehend zugegriffen wird, da eine Einbeziehung der persönlichen Ablage von Dateien des Geräteinhabers (zB eigene Dokumente, Übungsblätter, Fotos, Browserverlauf, Chat-Inhalte usw.) nicht Gegenstand der Maßnahmen sein darf.

Das Device Management hat daher die Anforderungen des § 6 Z 1 SchDigiG: „Funktionalität und Sicherheit aller Geräte […] sicherzustellen […] und die Umsetzung des schulischen Digitalisierungskonzeptes zu unterstützen“. Dabei ist die Möglichkeit des Geräteinhabers, eigene Apps zu installieren grundsätzlich aufrecht zu erhalten.

Daher sind bei konkreter technischer Ausgestaltung des MDMs, das der Umsetzung der §§ 10 und 11 dient, im Zuge einer Risikoanalyse der Zielgrad der Erreichung der Anforderungen die IT-Sicherheit mit Datenschutz und Eingriff auf Endgeräte abzuwägen.

Die vom BMBWF ausgearbeiteten Services im Rahmen der Einrichtung und des Betriebs eines MDMs (Handreichungen, Anleitungen, Schulungen Musterkonfiguration inklusive datenschutzfreundlicher Voreinstellungen sowie Supportstrukturen für die lokale IT-Betreuung an den Schulen) werden allen Schulen kostenfrei zur Verfügung gestellt. Weitere Information unter: https://digitaleslernen.oead.at/de/fuer-schulen/geraetemanagement-mdm

Erfahrungen aus Schulversuchen und anderen Pilotprojekten mit Schüler-Tablets an unterschiedlichen Schulstandorten haben gezeigt, dass nur bei einer einheitlichen Geräteausstattung der Schülerinnen und Schüler ein effektiver und effizienter Support geleistet werden kann. Daher wurde in § 11 Abs. 2 die Grundlage geschaffen, dass verpflichtend jene Geräte, die am Schulstandort im Digitalisierungskonzept gemäß § 2 Abs. 2 SchDigiG ausgewählt wurden, für alle Schülerinnen, Schüler und das Lehrpersonal im Unterricht einzusetzen sind.

Wenn der Zugriff auf Verarbeitungstätigkeiten ausschließlich über Remote Desktop Services erfolgt, die gewährleisten, dass alle Anforderungen dieser Verordnung über die Funktionalität des Remote Desktop Services erfüllt werden, kann die direkte Installation der MDM-Komponenten am Endgerät in dem Maß entfallen, als dies durch das Remote Desktop Service abgedeckt wird.

§ 11 Abs. 3 regelt Ausnahmebestimmungen für „kleine“ Schulen, die auf Grund der geringen Schülerzahl über keine webbasierte Schulverwaltung verfügen. Ist eine solche Schulverwaltung etwa ausschließlich bzw. überwiegend durch clientbasierte Text- und Tabellenverwaltung realisiert, so sind auf den eingesetzten Endgeräten gleichwertige Maßnahmen (etwa Festplattenverschlüsselung, Application-Whitelisting), die einen Schutz der personenbezogenen Schülerdaten gewährleisten, durch die Stelle gem. § 15 Z. 2 vorzusehen.

§ 11 Abs. 4: Eine Remote Desktop Verbindung direkt auf ein dienstliches Endgerät am Schulstandort kann verwendet werden um Personen temporär Zugriff zu gewähren, die kein dienstliches mobiles Endgerät zur Verfügung haben, aber außerhalb der Schule auf Schulverwaltungsdaten nach § 4 Z 1 zugreifen müssen. Diese können diese Verarbeitungstätigkeiten auf einem beliebigen Endgerät durchführen, solange diese nur innerhalb der Remote Desktop Session bleiben.

Zu § 12 (IT-Nutzungsbedingungen):

In den IT-Nutzungsbedingungen sollen Rahmenbedingungen für die Nutzung digitaler Endgeräte festgelegt werden. In Abs. 2 werden jene Verwendungen aufgezählt, die jedenfalls unzulässig sind wie beispielsweise Verstöße gegen das Urheberrechtsgesetz, das Hass im Netz Bekämpfungs-Gesetz – HiNBG, BGBl. I Nr. 148/2020, oder sonstige Verwendung der Endgeräte im Schulnetz zu illegalen Zwecken. Darüber hinaus können Schulleiter weitere standortspezifische IT-Nutzungsbedingungen anordnen.

Zu § 13 und § 14 (Funktionalitäten der Endgeräte im IKT-gestützten Unterricht, Elektronische Kommunikation mit Erziehungsberechtigten):

Hier werden im Wesentlichen die Erfahrungen aus dem corona-bedingten ortsungebundenen Unterricht, die in die gesetzlichen Regelungen zu § 14a und § 70a SchUG eingeflossen sind, durch nähere Determinierung umgesetzt. Grundsätzlich ist die Anforderung zur Aktivierung der Kamera nach pädagogischer Notwendigkeit an Hand der Zielerreichung zur Unterrichtsarbeit nach § 17 SchUG zu beurteilen. Der Verhältnismäßigkeitsgrundsatz sowie die Grundsätze der Zweckbindung und Datenminimierung sind dabei durch die Lehrpersonen im Einzelfall zu beachten. Da es sich beim IKT-gestützten Unterricht nach § 14a um Schulrechtsvollzug zur Erreichung der Ziele des § 17 SchUG handelt, ist gemäß der Systematik nach Art. 6 DSGVO keine Einwilligung erforderlich. Beim IKT-gestützten Unterricht handelt es sich nicht um Bildaufnahme zu privaten Zwecken gemäß §§ 12 und 13 DSG.

Dafür sind grundsätzlich keine Aufzeichnungen erforderlich und daher auch nicht zulässig. Eine Aufzeichnung ist im Wesentlichen nur dann sinnvoll, wenn es etwa für die Einbindung kranker Mitschülerinnen und Mitschüler während eines längeren Krankenhausaufenthaltes und damit verbundenen Besuchs einer Heilstättenschule handelt. An einigen Standorten steht diesbezügliche Infrastruktur zur Einbindung der Heilstättenschüler in den ursprünglichen Klassenverband der Regelschule bereit. Soweit hier eine Aufzeichnung technisch erforderlich ist, darf dies nur nach Zustimmung aller erfolgen.

Nähere Projektdefinition unter https://heilstaettenschule.schule.wien.at/avatar/ abrufbar.

Dabei sind unter „im IKT-Unterricht eingesetzten IT-Systemen und Diensten“ insbesondere die Videokonferenzsysteme zu verstehen, die im ortsungebundenen Unterricht bisher an österreichischen Schulen eingesetzt waren, um mittels Audio- und Videostreaming Kommunikationsanforderungen des Schulalltags abzuwickeln, wie etwa

- Erstellen und Bereitstellen von Online-Lernunterlagen sowie Live-Unterricht per Video,
- Stellen und Einsammeln von Aufgaben und Feedback an Schülerinnen und Schüler geben,
- Kommunikation unter Schüler/innen und soziale Präsenz in der Lerngruppe fördern,
- Festigen des Gelernten und Erheben des Lernstands der Schülerinnen und Schüler und
- Kommunikation mit Erziehungsberechtigten (elektronisches Mitteilungsheft).

Zu § 15 (Festlegung von Verpflichtungen der Verantwortlichen):

Bereits seit Längerem ist für Bundesschulen eine Festlegung der Verpflichtungen bezüglich der datenschutzrechtlichen Verantwortung von Schulleitungen und dem BMBWF als Schulerhalter definiert (https://www.bmbwf.gv.at/Themen/schule/schulrecht/ds.html#02). Auf dieser im Schulalltag bewährten Regelung aufbauend werden allgemeinere Zuständigkeitsregelungen zur datenschutzrechtlichen Verantwortlichkeit festgelegt. Dabei wird in § 15 Z 1 der Verordnung die Verantwortlichkeit für die Einhaltung der Rechtmäßigkeit sowie Zweckbindung der Verarbeitungstätigkeiten weitgehend den Schulleitungen zugeordnet. Dies ergibt sich insbesondere aus den einschlägigen gesetzlichen Vorgaben in den § 56 SchUG sowie den §§ 4 und 5 BilDokG, die im Wesentlichen die Zwecke der schulischen Verarbeitungstätigkeiten gesetzlich vorgeben.

Die Legaldefinition des Verantwortlichen in Art. 4 DSGVO stellt aber nicht nur auf Zwecke, sondern auch auf die Entscheidung über Mittel ab, wobei hier die Lehre (DatKomm Praxiskommentar zum Datenschutzrecht zu Art. 4 Rz 84) ausführt: „Als Mittel sind nicht nur die technischen und organisatorischen Methoden gemeint, sondern das „Wie“ der Verarbeitung“.

Die Verantwortlichkeit für die eingesetzten Mittel bei Verarbeitungstätigkeiten wird daher in § 15 Z 2 der Verordnung derjenigen Stelle zugeordnet, die als Maßnahme bezüglich der IT-Ausstattung an Schulen die Entscheidung darüber trifft, welche IT-Systeme und Dienste (etwa für Schulverwaltung, Lernplattform oder Mailservice) eingesetzt werden. Diese sind in der schulischen IT-Landschaft, wie sie auch die Verordnung grundsätzlich technisch beschreibt, weitgehend keine Server, die nur von einem Schulstandort betrieben werden, sondern webbasierte IT-Services, die für eine große Zahl an Schulen (etwa alle Bundesschulen, alle Pflichtschulen eines Bundeslandes, alle Schulen eines privaten Schulerhalters) einheitlich technisch festgelegt, beauftragt, gehostet und gewartet werden.

Es ist aber nicht Regelungsgegenstand der Verordnung, festzulegen, welche Stelle Entscheidungen über den IT-Einsatz an Nicht-Bundes-Schulen trifft, da dies in den sachlichen Geltungsbereich insbesondere des Pflichtschulerhaltungs-Grundsatzgesetzes und des Privatschulgesetzes und den darauf beruhenden Ausführungsgesetzen fällt. De lege lata ist hier aber keine ausdrückliche Regelung zur IT-Ausstattung der Pflichtschulen enthalten. In der Praxis treffen Entscheidung über IT-Mitteleinsatz für Bundesschulen der Bund, für öffentlich-rechtliche Pflichtschulen das Land bzw die Gemeinden, sowie für Privatschulen der jeweilige privatrechtliche Schulerhalter. Das BMBWF ist sich dieser Thematik bewusst und strebt grundsätzlich eine diesbezügliche föderale weitere Erörterung der Thematik an.

Für die Auslegung der von der Verordnung verwendeten Wendung „jene Stelle, die als Maßnahme bezüglich der IT-Ausstattung an Schulen die Entscheidung darüber (über IT-Einsatz, Produktauswahl etc) trifft“, wäre insbesondere Folgendes zu berücksichtigen:

- Für Bundesschulen sowie Privatschulen ist der Schulerhalter als diese Stelle anzusehen.
- Bei Lizenzen für Mobile Device Management-Software wird grundsätzlich darauf abgestellt, dass Produkte zum Einsatz kommen, die bereits in der Rahmenvereinbarung der BBG mit Microsoft (Microsoft Dachvertrag) bzw. den bestehenden MS-Verträgen der Länder für alle öffentlich-rechtlichen Schulerhalter umfasst sind. Weiters wird für das Mobile Device Management für Chromebooks ein Lizenzvertrag seitens des BMBWF geschlossen. Soweit hier konkrete Konfigurationsanleitungen für ein MDM-Produkt durch das BMBWF erstellt und allen Schulen bereitgestellt wurden, wurde diesbezüglich durch das BMBWF auch die Datenschutzkonformität berücksichtigt.
- Nach einer Erhebung der Abt. Präs/11 werden Schulverwaltungsprogramme sowie Iso/Ideal für Pflichtschulen grundsätzlich in allen Bundesländern durch die Landesregierung bzw die Bildungsdirektion zur Verfügung gestellt. Ausnahmen bestehen teilweise bei Pflichtschulen in größeren Städten.

- Bei den Lernplattformen (etwa: Schooly, LMS und edu.vidual) bestehen weitgehend Angebote der Länder bzw. Bildungsdirektionen.

Diese Verantwortlichkeit für Entscheidungen bzgl. der eingesetzten Mittel berührt nicht die jeweiligen Rechtsgrundlagen, die festlegen, wer für welche Zwecke Daten verarbeitet. Grundsätzlich sieht das Schulrecht hier (weiterhin) vor, dass personenbezogene Schülerdaten (insbes. gem. § 5 BilDokG 2020) nur am Schulstandort für Zwecke des Schulrechtsvollzuges verarbeitet werden.

Aus den obigen Überlegungen ergibt sich daher folgende Zuständigkeitsaufteilung, die sich im Bereich der Bundesschulen unter Berücksichtigung der schulrechtlich grundsätzlich definierten Rollen von Schulleitung, Schulerhaltung (sowie Schulaufsicht) in der Praxis seit Einführung der DSGVO bewährt hat:

Sphäre der Schulleitung nach § 15 Z 1:

1. lokale Datenverarbeitung und dabei insbesondere die Sicherstellung der Rechtmäßigkeit, Vertraulichkeit und Richtigkeit der Erhebung gemäß Art. 5 bis 9 DSGVO,
2. Einholung der Einwilligung der Betroffenen für alle Datenverarbeitungen, die nicht auf gesetzlicher bzw. dienstrechtlicher Grundlage oder auf der Wahrnehmung einer Aufgabe im öffentlichen Interesse beruhen,
3. Beantwortung von Betroffenenrechtsanfragen, wie zum Beispiel Auskunfts-, Richtigstellung- und Löschungsanfragen gemäß Art. 15 bis 23 DSGVO,
4. Meldung von gegebenenfalls auftretenden Datenschutzverletzungen gemäß Art. 33 und 34 DSGVO, soweit es die lokale Verarbeitung von personenbezogenen Daten betrifft un
5. Erteilung einer Datenschutzinformation gemäß Art. 12 bis 14 DSGVO, wobei auf den lokalen Schul-Webseiten auf die allgemeine Datenschutzinformation im Rahmen der Schulverwaltung an österreichischen Schulen auf der Webseite des Bundesministeriums für Bildung, Wissenschaft und Forschung verlinkt werden kann.

Sphäre der Stelle nach § 15 Z 2:

1. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gemäß Art. 25 DSGVO,
2. Abschluss von Auftragsverarbeitervereinbarungen mit allen Auftragsverarbeitern gemäß Art. 28 DSGVO,
3. Führung eines Verarbeitungsverzeichnisses gemäß Art. 30 DSGVO, sofern dies nicht durch die zuständige Bundesministerin zu erfüllen ist (§ 4 Abs. 2 Z 1 BilDokG 2020),
4. Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 DSGVO,
5. Meldung von gegebenenfalls auftretenden Datenschutzverletzungen gemäß Art. 33 und 34 DSGVO, soweit es das zentrale Hosting oder Softwarefehler betrifft,
6. Durchführung einer Datenschutzfolgeabschätzung gemäß Art. 35 f DSGVO, sofern dies nicht durch die zuständige Bundesministerin oder durch den zuständigen Bundesminister zu erfüllen ist (§ 4 Abs. 2 Z 1 BilDokG 2020) und
7. Benennung eines Datenschutzbeauftragten für die Aufgaben gemäß Z 1 bis 6.

Eine ausführliche Liste der Datenschutzbeauftragten im Bildungsbereich sowie deren Zuständigkeit ist auf der Webseite des BMBWF veröffentlicht.

Zu §§ 16 bis 18 (Übergangsbestimmungen, Verweise auf Bundesgesetze, Inkrafttreten):

Die Übergangsbestimmung des § 16 legt fest, ab welchem Zeitpunkt die Teilnahme am Bildungsstammportal für Bundesschulen und für andere Schulen als Bundesschulen realisiert sein muss.

§ 17 stellt klar, dass Bundesgesetze, auf die im Rahmen dieser Verordnung verwiesen wird, immer in der mit dem Inkrafttreten der jeweils letzten Novelle dieser Verordnung geltenden Fassung anzuwenden sind.

Das Inkrafttreten dieser Verordnung wird in § 18 mit 1. September 2021 festgelegt.