SACHSEN-ANHALT
Landesbeauftragter
für den Datenschutz

Hinweise zur Ausstattung der Schulen mit digitalen Endgeräten unter Nutzung von Produkten wie Microsoft Office 365

I.
Die Umsetzung des Digital Pakts Schule schreitet mit großen Schritten voran. Digitale Endgeräte für Lehrkräfte und Schülerinnen und Schüler stehen in erheblichem Umfang zur Verfügung und sind vielfach bereits verteilt bzw. werden kurzfristig zur Verfügung gestellt. Dabei sollte der Eindruck vermieden werden, dass gegen die Nutzung der Endgeräte mit gängiger außereuropäischer Software, insbesondere Microsoft Office 365, keine Bedenken bestünden. Dies könnte bewirken, dass sich Schulen ohne die gebotene Prüfung für die Nutzung von Microsoft Office 365 nebst zugehörigen Produkten für den Schulbetrieb entscheiden. Damit würden sich Schulen als datenschutzrechtlich Verantwortliche ggf. Verantwortungslasten aufbürden, die sie zu Tragen kaum in der Lage wären. Es ist daher auf Folgendes hinzuweisen:

II.
Die Schule trägt für die Verarbeitung der Daten der Schülerinnen und Schüler die Verantwortung, sie muss die datenschutzrechtlichen Vorgaben einhalten. Bei Schülerinnen und Schülern handelt es sich vielfach um Minderjährige, die eines besonderen Schutzes bedürfen. Die DS-GVO betont diesen Schutzbedarf u. a. in den Erwägungsgründen 38, 58, 65, 71 und 75 DS-GVO sowie Art. 8, 12 Abs. 1, 57 Abs. 1 lit. b) DS-GVO.

III.
Grundsätzlich ist die Schule befugt, Daten der Schülerinnen und Schüler und Eltern auf Basis des Schulgesetzes insoweit zu verarbeiten, wie dies für die Erfüllung des Bildungs- und Erziehungsauftrags erforderlich ist. Dabei ist es möglich, sich automatisierter Verarbeitung, auch in Auftragsverarbeitung bei einem Dienstleister, zu bedienen. Die Anforderungen der Datenschutz-Grundverordnung müssen eingehalten werden. Dabei sind insbesondere die Grundsätze der Datenverarbeitung nach Art. 5 DS-GVO (Transparenz, Vertraulichkeit, Datenminimierung, Erforderlichkeit und Zweckbindung) sowie die Anforderungen an technische und organisatorische Vorgaben (Art. 5 Abs. 1 lit. f), 25 Abs. 1, 32 DS-GVO) zu beachten. Dies muss die Schule in eigener Verantwortung prüfen und die Einbindung von geeigneten IT-Dienstleistern datenschutzkonform gewährleisten. Bei einer Umsetzung ist auch zu beachten, dass Softwareprodukte im Auslieferungszustand oft nicht umfassend den Geboten der datenschutzfreundlichen Voreinstellungen (Art. 25 Abs. 2 DS-GVO) entsprechen, sodass insoweit eine Nachjustierung erforderlich werden kann.

Bei einer Verlagerung von personenbezogenen Daten zu einem Dienstleister bedarf es einer Rechtsgrundlage. Wäre eine Übermittlung angedacht, wäre grundsätzlich die Regelung des

§ 84a SchulG LSA einschlägig. Die Übermittlung von personenbezogenen Daten an nichtöffentliche Stellen ist aber sehr stark eingeschränkt (§ 84a Abs. 8 Satz 2 SchulG LSA) und dürfte zudem an der fehlenden Erforderlichkeit scheitern. Übermittlungen von Schülerdaten an nichtöffentliche IT-Dienstleister kommen daher grundsätzlich nicht in Betracht. Es verbleibt daher in der Regel nur die Möglichkeit, eine derartige Inanspruchnahme eines Dienstleisters als Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO vertraglich auszugestalten.

Vor dem Hintergrund der regelmäßigen Unzulässigkeit der Datenübermittlung an einen privaten Dritten nach § 84a Abs. 8 S. 2 SchulG LSA ist auch stets zu prüfen, ob über die inhaltliche Nutzung der Softwareprodukte hinaus auf andere Weise Daten übermittelt werden, sei es durch Nutzung anfallender Daten durch den Dienstanbieter für eigene Zwecke oder durch die Notwendigkeit einer persönlichen Anmeldung der Nutzer. Zu betrachten ist weiter, welche der verschiedenen cloudbasierten Online Dienste von Microsoft Verwendung finden sollen, bei denen personenbezogene Datenflüsse entstehen können, wie Azure Active Directory, Exchange Online, SharePoint Online, OneDrive, Teams/Skype for Business, Mobile Device Management, Power BI, Click-to-Run Bereitstellung, Office Security & Threat Intelligence usw. Auch bei Standardanwendungen wie Word und Outlook kommt die Sammlung personenbeziehbarer Daten durch Microsoft in Betracht, die über Inhalte hinausgehen (z. B. bezüglich der Verwendung der Rücktaste oder der Worte vor und nach dem in der Rechtschreibüberprüfung geprüften Wort). Durch eine Vielzahl von erfassten Ereignissen können Profile entstehen. Unter anderem können Daten über das genutzte Endgerät, die Adresse des Internet-Zugangs und Standortdaten personalisiert werden. Dabei ist zu berücksichtigen, dass von einem Personenbezug einer Information bereits ausgegangen werden muss, wenn eine Identifizierbarkeit gegeben ist (siehe dazu Erwägungsgrund 26 DS-GVO). Einfache Pseudonymisierungen als Sicherungsmaßnahmen wären daher ggf. nicht ausreichend, soweit die Information durch eine Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden können.

Schulen sind bei der Nutzung von Microsoft Office 365 grundsätzlich datenschutzrechtlich Verantwortliche (Art. 4 Nr. 7 DS-GVO), Microsoft in der Regel Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO). Der Schule obliegt es daher, neben der Einhaltung der bereichsspezifischen Vorschriften (§ 84a ff SchulG LSA) die europarechtlichen Grundsätze (Art. 5 DS-GVO) und Vorgaben, insbesondere in technischer und organisatorischer Hinsicht (Art. 5 Abs. 1 lit. f), Art. 25, Art. 32 DS-GVO) einzuhalten und die Einhaltung auch nachzuweisen (Art. 5 Abs. 2 DS-GVO). Sie muss daher gem. Art. 32 Abs. 1 DS-GVO Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Kategorien personenbezogener Daten feststellen und basierend darauf die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener natürlicher Personen beurteilen. Sodann sind geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Für die Auftragsverarbeitung sind weiter die Voraussetzungen nach Art. 28 DS-GVO zu beachten. Der Verantwortliche hat danach bei der Auswahl eines Auftragsverarbeiters zu beachten, dass dieser hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen getroffen wurden und so durchgeführt werden, dass die Verarbeitung dauerhaft im Einklang mit den Anforderungen der DS-GVO erfolgt und damit der Schutz der Rechte der betroffenen Personen gewährleistet ist.

IV.
Es bestehen sehr erhebliche Bedenken dahingehend, dass es Schulen nicht gelingen dürfte, eine datenschutzrechtskonforme und damit zulässige Verarbeitung von Schülerdaten nachzuweisen. Nach langjährigen Beratungen mit Microsoft kam die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder im September 2020 nach Auswertung der Allgemeinen Bedingungen und der Datenschutzbestimmungen von Microsoft mit knapper Mehrheit zu dem Ergebnis, dass auf Basis der genannten Unterlagen kein datenschutzgerechter Einsatz von Office 365 möglich ist. Datenschutzbeauftragte anderer EU-Länder und auch der Europäische Datenschutzbeauftragte sehen noch verschiedene offene Punkte, die mit der DS-GVO in Einklang zu bringen sind und noch Änderungen von Produkt und Vertragsbedingungen durch Microsoft erfordern. Abschließende Einschätzungen werden darüber hinaus dadurch erschwert, dass das Produkt unangekündigt geändert werden kann und auch die Vertragsbedingungen möglichen Änderungen unterliegen. Das Thüringer Bildungsministerium hat daher die Nutzung von Microsoft Office 365 bereits untersagt („Datenschutz in Schulen“, Nr. 7.5, https://bildung.thueringen.de/schule/medien/datenschutz-in-schulen). Auch die auf dem Landesbildungsserver veröffentlichte Handreichung des Ministeriums für Bildung Sachsen-Anhalt „Datenschutz an Schulen“, Nr. 26, gibt vor, dass auf die Nutzung von Office 365 verzichtet werden sollte.

Microsoft selbst vertritt nach hiesiger Erkenntnis, dass Office 365 DS-GVO-konform nutzbar sei. Dies erscheint jedoch aus einer Reihe von vorgetragenen Gründen (mangelnder Transparenz, fehlenden Konfigurationsmöglichkeiten und auch rechtlichen Defiziten) zu bezweifeln. Dazu erscheint Folgendes beachtenswert:

1. Schwierigkeiten ergeben sich im Hinblick auf die Stellung von Microsoft als Auftragsverarbeiter. Die Vertragsgestaltung muss den Anforderungen des Art. 28 DS-GVO entsprechen. So darf der Auftragsverarbeiter u. a. nur nach Weisung handeln (Art. 28 Abs. 3 lit. a) DS-GVO) und muss die erforderlichen Maßnahmen nach Art. 32 DS-GVO treffen (lit. c). Der Vertrag muss die Verarbeitung präzisieren, insbesondere bezüglich Art und Zweck sowie Art und Umfang der Daten. Unterauftragnehmer dürfen nur nach vorheriger Genehmigung des Verantwortlichen beauftragt werden.

   Microsoft stellt dem Verantwortlichen in der Regel Online Service Terms (OST, Allgemeine Bedingungen) und Data Processing Addenda (DPA, Datenschutzbestimmungen) als Vertragsbestandteile zur Verfügung. Die Dokumente enthalten wohl nur unzureichende Informationen über Unterauftragnehmer, einschließlich deren Aktualisierung gemäß Art. 28 Abs. 2 DS-GVO. Nach hiesiger Erkenntnis wird vor der Beauftragung von Subauftragnehmern nicht, wie geboten, die Genehmigung eingeholt, sondern es erfolgt nur eine Veröffentlichung auf einer Liste. Es fehlen wohl auch differenzierte Beschreibungen der Umsetzungen risikoangemessener technischer und organisatorischer Maßnahmen gem. Art. 32 DS-GVO. Die Risikoangemessenheit technischer und organisatorischer Maßnahmen dürfte durch den Verantwortlichen nur schwer überprüfbar sein. Auch sind, soweit hier bekannt, Beschreibungen zu Arten und Zwecken der Datenverarbeitungen und den betroffenen personenbezogenen Daten unpräzise. Insbesondere Verarbeitungen personenbezogener Daten für eigene Geschäftszwecke (ggf. Verbesserung der Produktqualität, Erhöhung der Sicherheit, Werbezwecke etc.)

werden unzureichend transparent beschrieben (insoweit stellt sich auch die weitere Frage nach der ausreichenden Rechtsgrundlage der Verarbeitung).

2. Das niederländische Justizministerium hat in einer Studie (https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office/DPIA+Microsoft+Office+2016+and+365+-+20191105.pdf) nachweisen können, dass Microsoft über die Basisfunktionalitäten von Office 365 ProPlus eine umfangreiche Erhebung des Nutzerverhaltens durch Telemetriedaten durchführt. Sollte keine ausreichende Rechtsgrundlage für die Übermittlung von Beschäftigten- bzw. Nutzerdaten an Microsoft gefunden werden können, so müssen konkrete Maßnahmen benannt und umgesetzt werden, die eine derartige Telemetriedatenübermittlung verhindern oder zumindest stark einschränken können.

3. Klärungsbedürftig ist weiter, ob auszuschließen ist, dass cloudbasierte Sicherheitsprodukte Einsicht in die verarbeiteten Inhalte (Dokumente, E-Mails, Tabellen) nehmen und serverseitig Kopien davon anlegen, um potentielle Bedrohungen aufzudecken. Damit könnten personenbezogene Inhalte ggf. ohne Rechtsgrundlage übermittelt werden.

4. Soweit nicht auszuschließen ist, dass personenbeziehbare Daten an Microsoft als Anbieter in den USA fließen, ist von einer Übertragung von Daten in ein sog. Drittland auszugehen. Dann wären neben den grundsätzlichen Voraussetzungen auch die Voraussetzungen der Kapitels V (Art. 44 ff) der DS-GVO zu berücksichtigen. Zweck der Regelungen ist, auch für Verarbeitungen außerhalb der Geltung der DS-GVO ein entsprechendes Schutzniveau (z. B. in Bezug auf Betroffenenrechte) zu wahren. Der Verantwortliche hat daher im Zusammenwirken mit dem Datenempfänger ein entsprechendes Schutzniveau sicherzustellen. Dabei ist zu beachten, dass zwar noch die europäischen Standardvertragsklauseln Verwendung finden können, das sog. Privacy Shield der EU-Kommission jedoch infolge der Entscheidung des Europäischen Gerichtshofs vom 16. Juli 2020 („Schrems II“, Rechtssache C 311/18) nicht mehr gilt. Hierzu verweise ich auf die aktuellen Informationen zum Datenexport in Drittländer infolge des "Schrems II"-Urteils des EuGH auf meiner Homepage u. a. mit Verweis auf Empfehlungen des Europäischen Datenschutzausschusses (https://datenschutz.sachsen-anhalt.de/informationen/infopakete/infopaket-drittstaatentransfer/). Ein Einfluss einzelner Schulen auf Microsoft dahingehend, dass die vertraglichen Gestaltungen diesen Anforderungen angepasst werden, erscheint sehr fraglich.

5. Im Rahmen der Sicherstellung des Grundsatzes der Vertraulichkeit (Art. 5 Abs. 1 lit. f) DS-GVO) und des Rechts auf wirksamen gerichtlichen Rechtsbehelf (Art. 79 DS-GVO) ist auch zu prüfen, ob dies angesichts von Regelungen wie des US Cloud Act oder der Section 702 des Foreign Intelligence Surveillance Acts bzw. weiterer Sicherheitsvorschriften in den USA gewährleistet ist. Derartige Regelungen können die Diensteanbieter zur Herausgabe von Informationen verpflichten, z. T. auch, wenn die Daten auf Servern außerhalb der USA liegen. Zudem ist es auch möglich, dass die Unternehmen angehalten werden, den Abruf der Daten gegenüber den Betroffenen zu verheimlichen. Vielfach bestehen keine bzw. eingeschränkte Rechtsbehelfe. Eine Offenlegung personenbezogener Daten an Sicherheitsbehörden eines Drittlandes kommt in der Regel wohl nur in Betracht, wenn eine internationale Übereinkunft (Rechtshilfeabkommen)

dies stützt (Art. 48 DS-GVO). Ergänzend verweise ich auf das Infopaket Drittstaatentransfer auf meiner Homepage (https://datenschutz.sachsen-anhalt.de/informationen/infopakete/infopaket-drittstaatentransfer/).

6. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg hatte infolge der o. g. Entscheidung der Datenschutzkonferenz im Zusammenwirken mit dem dortigen Kultusministerium und Microsoft einen Praxistest unter erheblichem sachlichen und personellen Einsatz durchgeführt. Unter anderem ging es um Abhilfemaßnahmen zur Minimierung der Risiken der Microsoft Software sowie darum, ob unerwünschte bzw. nicht angeforderte Datenverarbeitungen, beispielsweise von Telemetrie-, Diagnose- (oder anders bezeichneten) Daten, erkennbar waren und inwieweit die Verarbeitung personenbezogener Daten von Lehrern und Schülern zu eigenen Zwecken Microsofts festzustellen waren. Im Rahmen dieser Prüfung wurde zudem untersucht, ob Daten in Drittstaaten außerhalb des Geltungsbereichs der DS-GVO fließen und ob durch eine sichere verschlüsselte Kommunikation die Möglichkeiten eines Zugriffs seitens des Anbieters oder Dritter wirksam eingeschränkt werden konnten. Im Ergebnis bewertete der Landesbeauftragte die Risiken beim Einsatz der erprobten Microsoft-Dienste im Schulbereich als inakzeptabel hoch und riet davon ab, diese dort zu nutzen. Verantwortliche können nach der Bewertung des Landesbeauftragten derzeit nicht ausreichend nachvollziehen, welche personenbezogenen Daten wie und zu welchen Zwecken verarbeitet werden und sie können nicht nachweisen, dass die Verarbeitung auf das für diesen Zweck notwendige Minimum reduziert ist (siehe dazu die Veröffentlichung auf der Homepage, https://www.baden-wuerttemberg.datenschutz.de/lfdi-raet-aufgrund-hoher-datenschutzrechtlicher-risiken-von-der-nutzung-der-geprueften-version-von-microsoft-office-365-an-schulen-ab/). Das wäre aber erforderlich, um bei Beschwerden von besorgten Eltern gegenüber der Datenschutzaufsichtsbehörde die datenschutzkonforme Verarbeitung nachzuweisen (Rechenschaftspflicht, Art. 5 Abs. 2 DS-GVO).

7. Schließlich ist auch zu bedenken, dass mit der Nutzung von Microsoft Office 365 zumeist die Nutzung des Betriebssystems Windows 10 einhergeht. Auch in Bezug auf die Nutzung dieses Systems bestehen einige Bedenken, die ggf. einer gesonderten Betrachtung bedürften. Dazu weise ich deshalb lediglich auf den Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 26. 11. 2020, „Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise“ hin (https://www.datenschutzkonferenz-online.de/media/dskb/TOP_30_Beschluss_Windows_10_mit_Anlagen.pdf).

VI.

Bisher ist im Rahmen der Beratung in der Regel vornehmlich auf die Verantwortlichkeit der jeweiligen Schule hingewiesen worden, die die notwendigen Prüfungen in eigener Verantwortung durchführen müsste. Auch war zu berücksichtigen, dass zunächst ein digitalisierter Betrieb von Schulorganisation und Unterricht mangels flächendeckender Angebote nur bedingt möglich war und gerade in der besonderen Situation der Corona-Pandemie besondere Anforderungen gestellt wurden. Ob angesichts der in den o. g. Landtagsdrucksachen beschriebenen positiven Entwicklung noch länger davon ausgegangen werden kann, dass eine Nutzung

von bedenklichen Softwareprogrammen aus dem außereuropäischen Raum zur Sicherung des Schulwesens als alternativlos und damit noch vertretbar anzusehen ist, erscheint fraglich.

Demgemäß wäre zielführend, wenn verstärkt auf die mit der Auswahl außereuropäischer IT-Diensteanbieter verbundene Problematik hingewiesen wird. Im Interesse digitaler Souveränität (siehe dazu die Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 22.09.2020, „Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen“, https://datenschutzkonferenz-online.de/media/en/TOP%208%20Entschlie%C3%9Fung%20digitale%20Souver%C3%A4nit%C3%A4t_final.pdf) sollte verstärkt für die Nutzung von Produkten europäischer Anbieter sowie insbesondere der öffentlichen (geförderten) Angebote (Bildungsserver, MUNDO) geworben werden.

Impressum

Herausgeber:
Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Leiterstraße 9
39104 Magdeburg

Tel.: (0391) 81803-0
poststelle@lfd.sachsen-anhalt.de
https://datenschutz.sachsen-anhalt.de

Stand: Oktober 2021