Mit klarem Kopf in der Cloud

13 Mit klarem Kopf in der Cloud

14 Apple, Google, Microsoft & Co.

15 Vielfalt digitaler Tools in den Schulen

17 Ja zu digitalen Lehrmitteln und Lernfördersystemen

18 Eindeutiger Identifikator für den Bildungsraum Schweiz

19 Plagiate mit einer Software erkennen

20 Office 365 für die Verwaltung

21 Elektronischer Zugriff auf Personaldossiers

Mit klarem Kopf in der Cloud

Cloud Computing vereinfacht viele Prozesse. Im Vergleich mit der herkömmlichen Auslagerung eröffnet Cloud Computing neue Welten der Datenbearbeitung. Auch die Verwaltung möchte davon profitieren, allen voran der Bildungsbereich.

Im Berichtsjahr erhielt der Datenschutzbeauftragte eine grosse Anzahl Anfragen zum Thema Cloud Computing. Die zur Prüfung vorgelegte Produktepalette ist riesig, betrifft unterschiedliche Anbieter und alle Bereiche der Verwaltung. Einige Überlegungen sind jedoch gleich, unabhängig davon, ob es sich um das Produkt eines grossen Anbieters oder einer kleinen Spezialfirma handelt.

Zuerst stellt sich die Frage nach der Art der Daten und nach den Geheimnispflichten, denen die Daten unterliegen. Hier entscheidet sich, welche Massnahmen durch den Anbieter und das öffentliche Organ umgesetzt werden müssen. Dazu gehören technische Massnahmen wie die Verschlüsselung, die Trennung von Mandanten in der Cloud oder die Portabilität der Daten und organisatorische Massnahmen wie ein Back-up oder ein Passwortkonzept. Mit diesen Massnahmen lässt sich der Transparenz- und Kontrollverlust minimieren, der mit dem Cloud Computing einhergeht. Der Datenschutzbeauftragte hat auf seiner Website detaillierte Dokumente veröffentlicht, die bei der Bestimmung der notwendigen Massnahmen helfen.

In der Praxis scheitern viele Projekte daran, dass die Massnahmen zur Informationssicherheit gar nicht umgesetzt werden können. Die Verschlüsselung der Daten während des Transports und in der Cloud selber erhöht die Sicherheit umfassend. Oft ist sie möglich, verhindert jedoch, dass alle Funktionalitäten eines Produkts ausgeschöpft werden können. Weiter stellt sich die Frage, ob der Schlüssel für die verschlüsselten Daten beim öffentlichen Organ liegt. Ist dies beispielsweise aus technischen Gründen nicht möglich, dürfen etwa Berufsgeheimnisdaten nicht durch Anbieter bearbeitet werden, die dem US-amerikanischen CLOUD Act unterliegen.

Oft verhindert die mangelnde Flexibilität von Anbietern, dass ein Produkt genutzt werden kann, etwa wenn sie sich weigern, ihre Verträge datenschutzkonform auszugestalten. Für öffentliche Organe gilt aber, dass beim Auslagern von Personendaten schweizerisches Recht anzuwenden und ein schweizerischer Gerichtsstand zu vereinbaren ist.

Die öffentlichen Organe müssen unter Abwägung aller relevanten Faktoren im Rahmen einer sorgfältigen Risikoanalyse entscheiden, ob bezüglich einer spezifischen Datenbearbeitung Cloud Computing in Anspruch genommen werden kann. Der Datenschutzbeauftragte bietet ihnen seine Unterstützung an.

Apple, Google, Microsoft & Co.

Der Datenschutzbeauftragte hat mit den grossen Anbietern Kontakt aufgenommen, um allen Schulen die gleichen datenschutzkonformen Bedingungen zu ermöglichen bei der Nutzung der marktbeherrschenden Produkte. Google G Suite for Education wird 2020 von den Schulen datenschutzkonform genutzt werden können. Dies trifft ebenfalls für das Produkt School Manager von Apple zu. Die Rahmenverträge für den Einsatz von Office 365 werden durch Educa.ch und Switch neu verhandelt.

Für die Nutzung dieser Dienstleistungen werden durch den Datenschutzbeauftragten neue Leitfäden erarbeitet. Die Schulen erfahren daraus, welche Verträge unterzeichnet werden müssen, welche Vorarbeiten zu tätigen und welche Massnahmen während der Nutzung des Produkts umzusetzen sind.

Der Datenschutzbeauftragte beantwortet weiterhin offene Fragen bei der Umsetzung und informiert regelmässig, wenn neue Dokumente zu diesen Themen publiziert werden.

Vielfalt digitaler Tools in den Schulen

Im Schulbereich werden zunehmend digitale Produkte und Cloud-Dienste eingesetzt. Eltern und Lehrpersonen aus verschiedensten Schulstufen melden sich beim Datenschutzbeauftragten und fragen nach Hilfestellungen. Die datenschutzrechtliche Prüfung dieser Produkte ist oft äusserst komplex.

Eine Schule darf Daten nur für die Zwecke bearbeiten, die zur Aufgabenerfüllung notwendig sind. Dies gilt auch, wenn mehr Daten als notwendig vorhanden sind und Auswertungen für andere Zwecke möglich wären. Der Datenschutzbeauftragte hat in seiner Beratungstätigkeit darauf aufmerksam gemacht, dass mit einem unkontrollierten Einsatz von digitalen Produkten Persönlichkeitsprofile entstehen. Persönlichkeitsprofile beinhalten ein hohes Missbrauchspotenzial. Eine Lehrperson kann beispielsweise mithilfe von eingesetzten Produkten feststellen, zu welcher Uhrzeit eine lernende Person welche Aufgaben gemacht hat oder wie lange sie für welche Aufgaben gebraucht hat. Sie kann daraus ableiten, ob eine Person die ganze Nacht wach war. Diese Auswertung der vorhandenen Daten ist nicht erlaubt.

Schultablets zu Hause nutzen

Ein Vater wandte sich an den Datenschutzbeauftragten, da in der Primarschule seiner Töchter Tablets eingeführt wurden. Mit den Tablets stieg auch die Zahl der benutzten digitalen Unterrichtswerkzeuge, wie Internetplattformen zum Vokabellernen oder zum Protokollieren der Hausaufgaben. Der Datenschutzbeauftragte hatte einige der fraglichen Produkte schon geprüft und befunden, dass sie datenschutzkonform genutzt werden können. Dafür muss die Schule Rahmenbedingungen definieren. Die Auswertung von Protokollen und Analysen der Daten muss immer der Zweckerfüllung der Schule dienen. Mit der Abgabe von Tablets stellen sich in der Praxis allerdings Fragen zu den Benutzerrechten, etwa dazu, wer welche Daten löschen darf. Wann darf die Schülerin oder der Schüler welche Daten löschen? Welche Daten darf die Lehrperson löschen? Bei den Eltern herrscht oft Unsicherheit oder ein unbehagliches Gefühl. Die Eltern sind einzubeziehen und über die Regeln beim Einsatz der Instrumente zu informieren.

Risikoanalyse bei Cloud-Diensten

Der Datenschutzbeauftragte prüfte einzelne schulrelevante Cloud-Dienste. Für die Prüfung von Verträgen mit Dienstleistern stellt der Datenschutzbeauftragte auf seiner Website den Leitfaden Bearbeiten im Auftrag zur Verfügung. Oft stellen die Anbieter den Schulen nicht einmal die notwendigen Informationen und Unterlagen zur Verfügung, um die Online-Dienste datenschutzrechtlich beurteilen zu können. Bei jedem Produkt muss zunächst festgestellt werden, welche Daten zu welchem Zweck ausgelagert werden. Die Schule muss den Gerichtsstand und das anzuwendende Recht abklären. Der Datenschutzbeauftragte rät anhand einer Risikoanalyse, die zu protokollierenden Informationen zu definieren, die Protokollierung von Änderungen zu regeln und angemessene Aufbewahrungsfristen festzulegen.

Lernplattformen, Umfragetools und Blogs

Auf der Stufe der Berufsschulen behandelte der Datenschutzbeauftragte Anfragen zum Einsatz von Produkten wie digitale Lernplattformen, Umfragetools oder Blogs. Die Schulen wünschten digitale Gruppenarbeitsräume.

Wenn Lernplattformen von den Schulen selbst betrieben werden, müssen diese die Informationssicherheit gewährleisten können. Werden für den Betrieb Dritte beauftragt, müssen die Voraussetzungen für eine Auslagerung erfüllt sein. Dazu müssen der Gerichtsstand, anwendbares Recht, Informationssicherheitsmassnahmen inklusive Informationen zur Speicherung und Löschung der Daten geprüft werden.

Vor der Nutzung ist in einem Konzept festzulegen, wer wann was macht. Der Datenschutzbeauftragte rät dazu, die Plattformen wenn möglich anonymisiert oder pseudonymisiert zu nutzen. Die Lernenden sind über mögliche Auswertungen zu informieren. Der Umfang der Datenbearbeitung bei der Nutzung von Lernplattformen oder Blogs ergibt sich durch den schulischen Auftrag. Schulen dürfen nur die Daten erheben und bearbeiten, die für die Aufgabenerfüllung der Schule erforderlich sind.

Bring Your Own Device

Für den Berufsfachschulunterricht hielt der Datenschutzbeauftragte fest, dass die Schülerinnen und Schüler auf freiwilliger Basis private Geräte verwenden dürfen. Dafür müssen die minimalen Schutzmassnahmen eingehalten werden. Diese umfassen die Einrichtung eines Passwortschutzes, die Installation eines Virenschutzprogramms, eine aktuelle Firewall sowie die Durchführung regelmässiger System-Updates und die Verschlüsselung sensitiver Daten bei der Speicherung und Übermittlung. Unter diesen Voraussetzungen hiess der Datenschutzbeauftragte auch die lokale Installation von Programmen wie Teams oder Onenote gut.

Ja zu digitalen Lehrmitteln und Lernfördersystemen

Lehr- und Lernprozesse mit digitalen Lehrmitteln und digitalen Lernfördersystemen gewinnen in der Volksschule an Bedeutung. Das Volksschulamt (VSA) und der Lehrmittelverlag Zürich (LMVZ) richteten diverse Fragen zu digitalen Lehrmitteln und Lernfördersystemen an den kantonalen Datenschutzbeauftragten.

Der Datenschutzbeauftragte analysierte mit den Verantwortlichen von VSA und LMVZ die Ausgangslage und mögliche Szenarien in Bezug auf die Datensicherheit, den Schutz der Privatsphäre sowie die Profilbildung. Die organisatorischen Rahmenbedingungen zum datenschutzkonformen Einsatz von digitalen Lehrmitteln wurden ebenso erörtert wie Fragen zu problematischen Datensammlungen. Besonderes Augenmerk fiel auf die technischen Möglichkeiten, vorhandene Datenbestände zu aggregieren, diese Verbindungen zu analysieren und daraus Schlussfolgerungen zu ziehen. Ähnliche Auswertungen wären vor der Digitalisierung zwar schon möglich gewesen, wurden aber aufgrund des manuellen und personellen Aufwands nicht umgesetzt.

In gedruckten Lehrmitteln erarbeiteten Schülerinnen und Schüler Aufgaben, die von den Lehrpersonen korrigiert und beurteilt wurden. Digitale Lehrmittel sollen in gleichem Masse genutzt werden können. Dazu benötigen die Lehrpersonen Einblick in die Nutzungsdaten der Lernenden. Die bisherige strikte Trennung von Nutzer- und Nutzungsdaten bei digitalen Lehrmitteln soll dafür aufgeweicht werden. Der Paradigmenwechsel führt zu zusätzlichen Datenbearbeitungen, insbesondere durch die Lehrpersonen in Bezug auf die Schülerinnen und Schüler.

Digital fallen oft mehr Daten an als bei einer Datenbearbeitung in analoger Form. Bei der analogen Hausarbeit hat die Lehrperson in der Regel keine genauen Informationen über Tag und Uhrzeit oder Dauer der Aufgabenbearbeitung, ebenso wenig darüber, wie oft eine Schülerin oder ein Schüler die Arbeiten unterbrochen hat. Bei digitalen Lehrmitteln werden diese Randdaten protokolliert. Die Schule muss sich vor dem Einsatz Gedanken machen über die Art und Weise der Nutzung digitaler Instrumente. Daten, die für den Lehrauftrag nicht notwendig sind, müssen in den Systemeinstellungen ausgeblendet oder sofort gelöscht werden. Der permanente Zugriff auf die Lernergebnisse durch die Lehrperson ist nicht erlaubt. Eltern, Schülerinnen und Schüler sowie Lehrpersonen sind vor dem Einsatz der digitalen Lehrmittel über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung der Daten zu informieren.

Eindeutiger Identifikator für den Bildungsraum Schweiz

Die Bildungsdirektion bat den Datenschutzbeauftragten, die von der Schweizerischen Konferenz der kantonalen Erziehungsdirektoren (EDK) vorgeschlagene Föderation von Identitätsdiensten für den Bildungsraum Schweiz (FIDES) zu prüfen. Die Identifizierungs- und Zugangsmanagement-Lösung für das Schweizer Bildungssystem ist heute unter dem Namen Edulog bekannt und wird durch Educa.ch angeboten.

Edulog soll den sicheren und transparenten Zugang der Volksschulen und der Sekundarstufe II zu verschiedenen Dienstleistern gewährleisten, beispielsweise dem Lehrmittelverlag. Die zentrale Föderationsplattform soll zukünftig die einzelnen Schulen als Identitätsanbieterinnen einbinden und ihnen die Verantwortung und Kontrolle über ihre Daten belassen. Der Datenschutzbeauftragte beurteilte die Plattform in einer Vorabkontrolle.

Die Verantwortlichen stützten die Datenbearbeitungen im Rahmen des Projekts auf das Konkordat über die Schulkoordination sowie auf ein spezifisches Organisationsreglement. Das Projekt erwies sich als komplex. Die Datenbearbeitungen durch die Föderationsplattform mussten von denjenigen durch die Schule und durch die Dienstleister unterschieden werden. Die Vorabkontrolle ergab, dass die geplante Datenbearbeitung keine genügende Rechtsgrundlage hatte. Die Datenbearbeitungen waren ungenügend beschrieben und es war nicht klar ersichtlich, bei wem die datenschutzrechtliche Verantwortung für welche Daten und ihre Bearbeitung liegen würde.

Aufgrund des Resultats der Vorabkontrolle wurde das Organisationsreglement angepasst, etwa betreffend die Zweckbindung und die Klarheit der Bestimmungen. Das Verhältnismässigkeitsprinzip wurde stärker berücksichtigt und nicht notwendige Datenbearbeitungen eliminiert. Edulog genügt damit den datenschutzrechtlichen Anforderungen, auch im Sinne einer Übergangslösung bis zu einer Revision des Konkordats.

Die Datenschutz- und Informationssicherheits-Managementsysteme von Edulog sollen zukünftig nach ISO 27001 und Good Privacy zertifiziert werden. Dadurch sind die generellen Informationssicherheitsanforderungen sichergestellt. Im organisatorisch-technischen Bereich gibt es Optimierungsbedarf bei den Prozessen für die Generierung, Erstverwendung, Änderung und Löschung einer Identität. Der Datenschutzbeauftragte wies darauf hin, dass bestehende Standards für die Föderation von Identitäten zu verwenden sind.

Der intensive Dialog und der aktive Miteinbezug von Educa.ch in die Beurteilung ermöglichte, das Projekt datenschutzkonform umzusetzen.

Plagiate mit einer Software erkennen

Eine Hochschule möchte eine Software einsetzen, um Abschlussarbeiten auf Plagiate zu überprüfen. Sie legte das Projekt dem Datenschutzbeauftragten zur Vorabkontrolle vor.

Zur Nutzung dieser Software müssten die Studierenden beim Softwareanbieter ein Benutzerkonto mit Name, Vorname und E-Mail-Adresse einrichten. Die Arbeiten würden beim Anbieter gespeichert. Die Nutzung der Software wäre freiwillig und würde auf der Einwilligung der Studierenden basieren.

Der Datenschutzbeauftragte kam in der Vorabkontrolle zum Schluss, dass ein solches Vorhaben einer Hochschule nicht freiwillig sein kann. Die Hochschule muss über eine gesetzliche Grundlage verfügen. Die Nutzung der Software gestützt auf eine Einwilligung ist nicht möglich. Das IDG sieht ein Bearbeiten von Personendaten mit Einwilligung nicht vor. Beim Einsatz dieser Software handelt es sich um eine Auftragsdatenbearbeitung. Die Hochschule bleibt für die Datenbearbeitung durch den Software-Anbieter verantwortlich.

Der Software-Anbieter war dem Swiss-US Privacy Shield beigetreten und die Standardvertragsklauseln waren Bestandteil des Vertragspakets. Dadurch verfügt er über ein angemessenes Datenschutzniveau. In den Verträgen waren auch die Datenkategorien, die Zweckbindung, die Rechte der Betroffenen, die Kontrollmöglichkeit der Hochschule, die Anwendbarkeit von schweizerischem Recht und ein schweizerischer Gerichtsstand festgehalten.

Der Datenschutzbeauftragte riet der Hochschule, nur die für eine Plagiatsüberprüfung notwendigen Personendaten an den Anbieter zu übermitteln. Dafür sollte nur ein Benutzerkonto durch die Hochschule eröffnet werden, über das die Arbeiten geprüft werden könnten. Weiter ist durch die Hochschule zu prüfen, wie die Arbeiten der Studierenden anonymisiert oder pseudonymisiert werden können.

Office 365 für die Verwaltung

Der Datenschutzbeauftragte wurde von Anfragen überhäuft, ob Office 365 nicht nur in Schulen, sondern auch in der Verwaltung eingesetzt werden könne. Ein Amt fragte an, wie eine Ausschreibung für die neue Ausstattung von Arbeitsplätzen zu gestalten sei.

Das öffentliche Organ bleibt immer verantwortlich für seine Daten, auch wenn es Produkte mit Cloudnutzung einsetzt, beispielsweise Office 365. Dies ist die Ausgangslage für alle Überlegungen. Wie kann diese Verantwortung wahrgenommen werden? Erstens muss der Vertrag datenschutzkonform sein. Er muss die gesetzlichen Anforderungen erfüllen, schweizerisches Recht für anwendbar erklären sowie einen schweizerischen Gerichtsstand festhalten. Zweitens müssen die Sicherheitsmassnahmen vorgesehen sein, die der Art und dem Umfang der Datenbearbeitung entsprechen. Drittens muss das öffentliche Organ beispielsweise ein Konzept erarbeiten, aus dem hervorgeht, wie welche Dienste mit welcher Art von Daten zu welchem Zweck genutzt werden. Bei der Nutzung sind teilweise Speicherorte und Verschlüsselungsmechanismen auszuwählen oder Lösch- und Protokollierungsfunktionen einzustellen.

Mit einer Gesamtrisikoanalyse ist zu bestimmen, ob ein Produkt in Anspruch genommen werden kann. Sind beispielsweise Berufsgeheimnisdaten betroffen, kann eine Auslagerung aufgrund hoher Risiken für die Persönlichkeitsrechte eingeschränkt werden. Eine Übersicht über diese Problematik stellt der Datenschutzbeauftragte auf seiner Website im Leitfaden Auslagerung: Berücksichtigung des CLOUD Act detailliert dar.

Zum Einsatz von Office 365 in der Verwaltung hat der Datenschutzbeauftragte versucht, sich mit Microsoft in datenschutzrechtlichen Belangen auf Schweizer Recht und einen schweizerischen Gerichtsstand zu einigen. Diese Faktoren wären bei Vertragsabschluss einzufordern. Microsoft hat sich nicht auf die vorgeschlagene Formulierung festgelegt.

In seiner Antwort auf die Anfrage eines Amtes zu den Bedingungen für die Ausschreibung einer neuen Arbeitsplatzumgebung schrieb der Datenschutzbeauftragte, dass die Anbieter begründet darzulegen haben, falls sie gewisse datenschutzrechtliche Anforderungen nicht erfüllen können. Das öffentliche Organ kann dann einen Entscheid für oder gegen Cloud Computing fällen, bei dem alle Aspekte berücksichtigt wurden.

Elektronischer Zugriff auf Personaldossiers

Nach Einführung des E-Personaldossiers in der kantonalen Verwaltung können Führungskräfte über ein Portal auf Informationen in den Personaldossiers der Mitarbeitenden elektronisch zugreifen. Der Datenschutzbeauftragte ging Anfragen nach, in denen kritisiert wurde, dass Führungskräfte über das Portal auf zu wenige Hierarchiestufen ihrer Organisation zugreifen können.

Das Personalamt ist für die Webanwendung verantwortlich. Abklärungen des Datenschutzbeauftragten ergaben, dass der Zugriff auf die Personaldossiers auf zwei Arten beschränkt ist. Einerseits werden der Führungskraft nicht alle im Personaldossier enthaltenen Dokumente angezeigt. Die Führungskraft kann etwa Administrativunterlagen wie Adressänderungen nicht einsehen. Auch sensible Angaben, die die oder der Vorgesetzte nicht zur Erfüllung der Aufgaben braucht, werden nicht angezeigt, beispielsweise Unterlagen eines Case Management oder Lohnabrechnungen. Andererseits erhalten Führungskräfte nur ständigen Zugriff auf die Dossiers von Mitarbeitenden, die maximal zwei Hierarchiestufen tiefer stehen. Auf Anfrage kann die HR-Abteilung dem Vorgesetzten weitere Dossiers zeitlich beschränkt elektronisch freischalten oder die Führungskraft kann direkt bei der HR-Abteilung in die Dossiers Einsicht nehmen.

Der Datenschutzbeauftragte kam zum Schluss, dass die Praxis dem Verhältnismässigkeitsprinzip entspricht. Er merkte an, dass alle Zugriffe auf die Dokumente zu protokollieren sind. Dies betrifft besonders die direkte Einsichtnahme der Führungskraft bei der HR-Abteilung. Die technische Protokollierung erfasst in diesem Fall den HR-Zugriff auf das E-Dossier. Der Zugriff durch die Führungskraft muss zusätzlich protokolliert werden.