Bernhard Walz
Schybenstuckweg 27
4323 Wallbach
079 460 59 04
bernhard.walz@akkbl.ch
Vertreter GLK im AKK-Vorstand

BASEL LANDSCHAFT
BILDUNGS-, KULTUR- UND SPORTDIREKTION
AMTLICHE KANTONALKONFERENZ DER LEHRERINNEN UND LEHRER

Stellungnahme des GLK-Kernteams zum Entwurf

«VO Schulinformatik und der Benutzungsreglemente Schulinformatik»

Die GLK bedankt sich ausdrücklich für die Gelegenheit zum o.g. Entwurf Stellung nehmen zu können.

Generell unterstützt es die GLK, den Schutz sensibler Daten in Schulen auf einen Stand zu bringen, der den heutigen Anforderungen an den Datenschutz gerecht wird. Dies ist derzeit sicherlich nicht überall gegeben. Insofern sehen wir auch die sich für die BKSD ergebende Notwendigkeit, in dieser Sache aktiv zu werden.

Zwei Punkte sind aus Sicht der GLK hier vordringlich zu berücksichtigen:

1. Die in der Verordnung festgelegten Regeln im Umgang mit sensiblen Daten müssen praktikabel sein und dürfen die tägliche Arbeit nicht unnötig erschweren.

2. Der Zugang und der Umgang von und mit persönlichen und schulbezogenen Daten von Seite der IT.SBL muss klar geregelt werden. Eine beliebige Überwachung der Aktivitäten auf und mit IT-Geräten darf es nicht geben.

VO Schulinformatik

Sensible Daten werden heute im Wesentlichen im Schulnetz (SAL), durch Microsoft Office Software oder via Emails erzeugt und verwaltet.

§14 sieht die Nutzung des «Identitätsmanagement von IT.SBL.» für den Gebrauch solcher Standardanwendungen vor. In §28 ist dies konkretisiert und mit einer «Zweifaktorenauthentifizierung» bezeichnet.
An dieser Stelle muss darauf hingewiesen werden, dass gemäss §§9 und 10 der «Benutzungsreglemente Schulinformatik» bereits sichergestellt ist, dass der Zugang zum Schulnetz (SAL) nur über die Eingabe von 2 Passwörtern möglich ist («Der Zugang zu privaten Geräten muss in jedem Fall mit einem ausreichend komplexen Passwort gemäss den Vorgaben der SBL-Passwortrichtlinien gesichert werden.»). Die gemäss §28 vorgesehen «Zweifaktorenauthentifizierung» wäre also in der Praxis eine «DREI-faktorenauthentifizierung» und ist im Schulalltag nicht handhabbar. Einige Beispiele sollen dies verdeutlichen.
Beispiel 1: Zu Beginn einer Lektion sollen die Absenzen und Verspätungen im Schulnetz (SAL) eingeben werden. Die Lehrperson kann nicht ständig neben dem

Bernhard Walz
Schybenstuckweg 27
4323 Wallbach
079 460 59 04
bernhard.walz@akkbl.ch
Vertreter GLK im AKK-Vorstand

Computer stehen. Sollten also mehrere Lernende zu spät kommen, muss sich die Lehrperson nach jeder Eingabe wieder mit der «DREI-faktorenauthentifizierung» anmelden. Im Vergleich zur analogen Version ist dies ein gewaltiger Rückschritt. Es ist nicht nur umständlich, es geht auch wertvolle Unterrichtszeit verloren. Beispiel 2: Schüler:innen haben auf ihrem Gerät von IT.SBL personenbezogene Daten. Jedes Mal muss eine «Zweifaktorenauthentifizierung» oder sogar «DREI-faktorenauthentifizierung» beim Benutzen von Standardanwendungen erfolgen. Wer schon einmal unterrichtet hat, kann sich gut vorstellen, wie gut dies funktionieren würde. Auch würde der Unterricht in erheblichem Mass behindert. Beispiel 3: Planung von Prüfungsterminen oder andere administrative Tätigkeiten: Vorteilhafterweise erfolgen diese ohne die Nutzung von Papier interaktiv, wobei Schulnetz (SAL) nur zeitweise zum Einsatz kommt. Dabei sind «Totzeiten» von mehr als 10 Minuten durchaus möglich. Ein mehrfaches Anmelden (von einem notabene passwortgeschützten Gerät) durch eine «Zweifaktorenauthentifizierung» ist hier ein Arbeitshindernis, das zu keinem verbesserten Schutz der Daten führt.

Es kann festgestellt werden, dass im Umgang mit digitalen Daten ein ungleich höherer Massstab angelegt wird, als im Umgang mit analogen Daten. Was die Vorgabe für den Aufwand zur Verhinderung eines nicht-legitimierten Zugangs zu solchen Informationen betrifft sind diese beiden Massstäbe keinem Falle auch nur annähernd vergleichbar. So schreibt §6 der Benutzungsreglemente Schulinformatik «Die Mitarbeitenden haben sicherzustellen, dass ausgedruckte Dokumente mit besonderen Personendaten oder anderem schützenswertem Inhalt nicht von Unberechtigten eingesehen bzw. behändigt werden können.» Der aus dieser globalen Regelung ablesbare Vertrauensvorschuss für die Mitarbeitenden, dass im Umgang mit sensiblen Daten die angemessenen «Schutzmassnahmen» ergriffen werden, sollte auch für den digitalen Bereich gelten.

§17 sieht die Verwendung von «Pseudonymen» bei der Nutzung von «Webbasierte Unterrichtshilfen» vor. Elektronische Lehrmittel erlauben teilweise die Zuweisung von personalisierten Arbeitsblättern für die Lernenden via E-Mail. Die Verwendung von Pseudonymen bedeutet hier einen Mehraufwand, der durch die Sache nicht gerechtfertigt erscheint. Andererseits versetzt eine Weiterverwendung der genannten Funktion die Lehrperson in eine arbeitsrechtlich heikle Lage.

Bernhard Walz
Schybenstuckweg 27
4323 Wallbach
079 460 59 04
bernhard.walz@akkbl.ch
Vertreter GLK im AKK-Vorstand

§21 sieht vor, dass «Arbeitsergebnisse, wie beispielsweise Arbeitsblätter, Übungen und Unterrichtseinheiten gemäss den Vorgaben des Arbeitgebers zu speichern sind».

Es ist nicht nachvollziehbar, warum dies im Rahmen einer «VO Schulinformatik» geregelt werden soll. Der Umgang mit Arbeitsergebnissen ist in unserem Verständnis im Verhältnis Schulleitung-Lehrpersonen zu regeln, und sollte nicht Gegenstand dieser Verordnung sein. Wir schlagen vor allenfalls zu regeln, dass die IT.SBL auf Antrag der jeweiligen Schulleitung verpflichtet ist, genügend Speicherplatz zur Verfügung zu stellen.

Lt. §21 müssen bei der Verwendung des BYOD-Modells „nicht öffentliche oder zur Veröffentlichung bestimmte Daten" (schulische Daten), grundsätzlich auf der dafür vorgesehenen IT.SBL-Infrastruktur gespeichert werden.
Sollte das bedeuten, dass in zukünftig alle zur Unterrichtsvorbereitung und Durchführung erzeugten Daten zwingend zentral bei IT.SBL gespeichert werden müssen?
In diesem Falle wäre interessant zu verstehen, für welchen Zweck diese Zwangsspeicherung erfolgen soll. Eine Speicherung von Daten zum Zweck der Vorratshaltung ohne spezifizierten Verwendungszweck ist abzulehnen.

Einen Hinweis auf eine praktikable Lösung in dieser Sache gibt vielleicht eine Formulierung in § 24:
«Zugriffe auf und Auswertungen von … zweckgebunden sein. Sie gelten dann als zweckmässig, wenn sie entsprechend dem «need to know Prinzip» für die Erfüllung des … Auftrags notwendig sind.»

§ 28 sieht ein zentrales Identitätsmanagement vor. «Zum Empfangen des zweiten Faktors müssen bei Bedarf auch private Geräte eingesetzt werden.»
Generell sind wir der Ansicht, dass Arbeitsmittel vom Arbeitgeber zu stellen sind und nur dann, wenn keine Alternative besteht, auf private Arbeitsmittel zurückgegriffen werden sollte. Zudem gibt es Standorte, wo unter Umständen keine Mobilfunkabdeckung durch einzelne Provider besteht. Kann in diesen Fällen ein:e Mitarbeiter:in gezwungen werden, einen weiteren Mobilfunkvertag einzugehen?
Wir würden ein solches Vorgehen entschieden ablehnen und in dieser Folge auch generell diese Regelung. Sollte eine «Zweifaktorenauthentifizierung» für gewisse Zugänge als unumgänglich erachtet werden, so ist eine Lösung zu finden, die nicht auf private Geräte der Mitarbeitenden zurückgreift, insbesondere deshalb, weil solche Lösungen bereits existieren und kommerziell verfügbar sind.

Bernhard Walz
Schybenstuckweg 27
4323 Wallbach
079 460 59 04
bernhard.walz@akkbl.ch
Vertreter GLK im AKK-Vorstand

Benutzungsreglemente Schulinformatik

§ 13
Es besteht grosses Verständnis seitens der GLK, dass vertrauliche Daten in der Kommunikation mit Dritten (z.B. Eltern) sehr sensibel gehandhabt werden müssen. Einfach nur vorzuschreiben wie in §13 dass «Vertrauliche Daten, insbesondere Personendaten, nur verschlüsselt oder passwortgeschützt an E-Mail-Adressen ausserhalb des kantonalen Netzwerks versendet werden dürfen» ist aus unserer Sicht nicht sinnvoll. Wir gehen davon aus, dass auch die IT.SBL nicht den Weg zurück in die analoge Welt mit Papier und Kugelschreiber und der gelben Briefpost als Methode der Wahl empfehlen möchte.
Ziel der Verordnung sollte es doch sein, dass diese in der Praxis umgesetzt wird. Die Vorgabe von nicht praktikablen Vorgehensweisen unterstützt die Erreichung dieses Ziels nicht, sondern zwingt die handelnden Personen zur sinnvollen Ausführung ihrer Tätigkeit in einen legalen Graubereich.
Es braucht aus Sicht der GLK praktikable Lösungen, die dem Bedürfnis nach Schutz sensibler Daten gerecht werden.

§20 macht aus Sicht der GLK zu enge Vorgaben in Bezug auf die Speicherung von Daten. Die Vorgabe, dass «sonstige schulische Daten auf der durch die IT.SBL für diesen Zweck freigegebenen Cloud-Lösung zu speichern sind» und «es untersagt ist, schulische Daten auf privaten resp. nicht von IT.SBL zur Verfügung gestellten Datenträgern (z.B. externen Festplatten, USB-Sticks) … zu speichern» lässt viele Fragen offen.
Wie verhält es sich mit Back-up's von BYOD – Geräten? Sind diese zulässig?
Was passiert beim Wechsel einer Lehrperson in einen anderen Kanton? Verbleiben dann alle Dokumente zum Unterricht bei IT.SBL und das Anfertigen einer Kopie wäre ein Verstoss?
Unserer Ansicht nach wäre es notwendig, die Folgen einer solchen Regelung detailliert zu prüfen und dann eine angepasste Formulierung zu finden.

Ähnliches wird auch in §14 für die Lernenden geregelt. Hier sind die Regeln aus einer anderen Perspektive zu sehen, da es sich bei «schulischen Daten» teilweise um private Daten der Lernenden handelt. Es stellt sich die Frage, ob es gerichtlich haltbar wäre, Lernenden das Kopieren eigener «Erzeugnisse» auf externe Datenträger zu verbieten.
Für uns stellt sich die Frage, warum «Dateien, welche besondere Personendaten enthalten, dürfen ausschliesslich auf dem persönlichen Gerät gespeichert werden» dürfen. In den meisten Fällen wird es sich bei den Lernenden um ihre

Bernhard Walz
Schybenstuckweg 27
4323 Wallbach
079 460 59 04
bernhard.walz@akkbl.ch
Vertreter GLK im AKK-Vorstand

eigenen Personendaten handeln. Es ist nicht nachvollziehbar, warum der Umgang mit den eigenen Daten reguliert werden sollte.

§ 24 regelt die Protokollierung von Daten. «Protokolldaten dienen ausschliesslich der Datensicherheit und zur Sicherstellung eines ordnungsgemässen Betriebes, zu Zwecken der Datenschutzkontrolle und der IT-Revision. Sie werden nicht für eine präventive Verhaltens- oder Leistungsbewertung verwendet.»
Soweit könnten wir uns eigentlich einverstanden erklären, wenn nicht leider bereits mindestens ein Fall bekannt wäre, in dem diesem Grundsatz nicht entsprochen wurde.
Aus diesem Grund fordern wir, dass vor Verwendung der Daten eine Information an die betreffende Lehrperson dahingehend stattfinden muss, welche Daten zu welchem Zweck genutzt werden sollen, so dass diese über die Verwendung ihrer Daten in Kenntnis ist. Insbesondere ist uns wichtig, dass eine Verwendung von Daten zu disziplinarrechtlichen Zwecken der betroffenen Lehrperson vorgängig zur Kenntnis gegeben wird.

Eigentlich wäre diese Frage in §25 geregelt, wo festgestellt wird, dass «eine präventive personenbezogene Kontrolle nicht erlaubt ist» und «grundsätzlich die Mitarbeitenden im Voraus darüber informiert werden, wenn eine personen-bezogene Prüfung vorgenommen wird».

Aufgrund des besagten Vorkommnisses fehlt leider das Vertrauen in diesem Punkt. Wir fordern daher, dass jegliche vorsorgliche Sammlung von Daten, die der Überwachung dienen (Zugangsprotokolle mit z.B. IP-Adresse, Zeiten und Nutzungsdauern, Internetzugänge, Nutzung von Webseiten, o.ä.) unterlassen und nur bei einem begründeten Verdacht nach vorgängiger Information der betroffenen Person durchgeführt wird.
Gleiches sollte auch für den Zugriff auf Daten gelten, die von einer Lehrperson erstellt wurden. Ein Zugriff von IT.SBL, einer Schulleitung oder weiterer Personen sollte nur nach vorgängiger Begründung erfolgen dürfen. Hier sollte eine Rege-lung ähnlich §21 für den Fall einer «unvorhersehbaren Abwesenheit» gefunden werden.
Ein Weg, wie eine Regelung aussehen könnte zeigt § 27 der VO:
«Zugriffe auf und Auswertungen von … zweckgebunden sein. Sie gelten dann als zweckmässig, wenn sie entsprechend dem «need to know Prinzip» für die Erfüllung des … Auftrags notwendig sind», wobei hier die Details des «need to know Prinzips» zu detaillieren wären.
Wir sehen in einer Regelung, wie wir sie vorschlagen den Ausdruck eines gesunden Vertrauensverhältnisses zwischen Lehrpersonen und Direktionen.

Bernhard Walz
Schybenstuckweg 27
4323 Wallbach
079 460 59 04
bernhard.walz@akkbl.ch
Vertreter GLK im AKK-Vorstand

Wir möchten nochmals betonen, dass wir es sehr schätzen, zum Entwurf dieser Verordnung gehört zu werden und möchten festhalten, dass wir dem Anliegen der IT.SBL gegenüber, einen zeitgemässen Datenschutz in den Schulen zu realisieren, sehr aufgeschlossen sind.
Die zu treffenden Regelungen müssen aber auch wirksam, konsistent und praktikabel sein. Dies ist an vielen Stellen aus unserer Sicht nicht umgesetzt.

Besonders betonen möchten wir, dass der Datenschutz auch für die Lehrpersonen gelten muss. Regelungen, die den Verdacht nahelegen, dass Lehrpersonen systematisch «ausspioniert» werden, lehnen wir entschieden ab. Auch hier befürworten wir praktikable Lösungen, die im Sinne des gegenseitigen Respekts zwischen Lehrpersonen und Direktion getroffen werden.

Für das GLK-Kernteam

Bernhard Walz
Vertreter GLK im AKK Vorstand