Datenschutz
an der Primarschule Weinfelden

Peter Keller, Primarschule Weinfelden
Genehmigt durch die Primarschulbehörde: 22.02.2021 / 31.05.2021
Version 1.0

Verwendete Abkürzungen

MA = Mitarbeiter / Verwaltung **SuS** = Schülerinnen und Schüler **EB** = Erziehungsberechtigte

Inhaltsverzeichnis

Verwendete Abkürzungen 2
1 Ausgangslage 3
2 Datenklassifizierung 3
3 Kommunikation 4
3.1 E-Mail 4
3.1.1 Aktuelle Situation 4
3.1.2 Primärer Handlungsbedarf ("Hochrisiko" eliminieren) 4
3.1.3 Sekundärer Handlungsbedarf 4
3.2 Messenger 4
3.2.1 Aktuelle Situation 4
3.2.2 Primärer Handlungsbedarf ("Hochrisiko" eliminieren) 5
3.2.3 Sekundärer Handlungsbedarf 5
3.3 Videokonferenz-Tools 5
3.3.1 Aktuelle Situation 5
3.3.2 Primärer Handlungsbedarf ("Hochrisiko" eliminieren) 5
3.3.3 Sekundärer Handlungsbedarf 5
4 Datenspeicherung & Kollaboration 6
4.1 Datenspeicherung 6
4.1.1 Aktuelle Situation 6
4.1.2 Primärer Handlungsbedarf ("Hochrisiko" eliminieren) 6
4.1.3 Sekundärer Handlungsbedarf 7
4.2 Kollaboration 7
4.2.1 Aktuelle Situation 7
4.2.2 Primärer Handlungsbedarf ("Hochrisiko" eliminieren) 7
4.2.3 Sekundärer Handlungsbedarf 7
5 Weitere Bereiche 8
5.1 Foto-, Film- und Tonaufnahmen 8
5.1.1 Aktuelle Situation 8
5.1.2 Primärer Handlungsbedarf ("Hochrisiko" eliminieren) 8
5.1.3 Sekundärer Handlungsbedarf 8
5.2 Kennwörter 8
5.2.1 Aktuelle Situation 8
5.2.2 Primärer Handlungsbedarf ("Hochrisiko" eliminieren) 8
6 Zusammenfassung 9
7 Weiteres Vorgehen 10
8 Anhang 11

1 Ausgangslage

Die Datenschutzgesetzgebung ist veraltet, so stammt das aktuelle Bundesgesetz über den Datenschutz vom 01.07.1993. Das kantonale Datenschutzgesetz des Thurgaus ist seit dem 01.01.1989 in Kraft. Beide Gesetze stammen also aus der Zeit, wo die digitale Welt noch in den Anfängen war und niemand z.B. von Cloud-Speichern gesprochen hat. Diese Gesetze werden deshalb revidiert. Das revidierte Schweizer Datenschutzgesetz steht kurz vor dem Abschluss – es stehen nur noch die Verordnungen aus.

Aufgrund der immensen digitalen Entwicklung kann aber nicht mehr länger zugewartet werden, zumal auch die veralteten Gesetze anzuwenden sind. Der Datenschutz an unserer Schule muss deshalb überprüft und angepasst werden, nicht zuletzt auch, weil seit dem Mai 2018 die Europäische Datenschutz-Grundverordnung in Kraft ist, welche auch Auswirkungen auf die Schweiz hat (siehe Anhang). Die digitale Welt kennt eben keine Grenzen. Da die öffentliche Schule zudem dem "Öffentlichen Recht" unterliegt, gelten andere – strengere – Regeln als im "Privatrecht", dem z.B. die Privatwirtschaft unterliegt. Bezüglich detaillierterer rechtlicher Grundlagen / Begründungen sei auf die kantonalen Dokumente (Anhang) verwiesen.

2 Datenklassifizierung

Um einen sinnvollen Datenschutz definieren zu können, ist es nötig, die Daten zu klassifizieren. Hilfreich ist die Datenschutz-Ampel der PHTG. Bei der folgenden Darstellung handelt es sich um diejenige für Lehrpersonen. Auf tg.ch finden sich auch die Datenschutz-Ampeln für Schulleitungen, Schulpersonal und SuS (siehe Anhang), die sich aber von der untenstehenden nicht wesentlich unterscheiden.

Besonders schützenswerte Personendaten:

- Zeugnisse, Notenlisten und andere Leistungsbeurteilungen wie Lernpass-, Lernlupe- oder Stellwerkresultate
- Lebensläufe und Bewerbungsschreiben
- Ärztliche Untersuchungen
- **Sensible** Foto-, Video- oder Audiodateien von bestimmbaren Personen[1]
- **Sensible** Texte (z.B. persönliche Ansichten zu Religion oder Politik) mit Namensbezug
- Massnahmen (Therapien, Disziplin, Notizen etc.)
- **Sensible** Informationen über die Eltern

⇨ hohe Restriktionen bezüglich Datenschutz

Personendaten:

- Arbeits- und Übungsblätter mit Namensbezug (d.h. auf einem Dokument steht der Vorname oder Nachname des Autors)
- Foto-, Video- oder Audiodateien von bestimmbaren Personen[1]
- Nicht sensible Texte mit Namensbezug (d.h. im Text steht der Vorname oder Nachname des Autors)
- Informationen über die beruflichen, finanziellen und sozialen Verhältnisse der Eltern

⇨ Restriktionen bezüglich Datenschutz

Sachdaten:

- Arbeits- und Übungsblätter ohne Namensbezug (d.h. auf einem Dokument steht nirgends ein Vorname oder Nachname)
- Foto-, Video- oder Audiodateien (sofern keine Person bestimmbar ist) ohne Namensbezug
- Nicht sensible und sensible Texte (z.B. persönliche Ansichten zu Religion oder Politik) ohne Namensbezug (d.h. im Text steht nirgends der Vorname oder Nachname des Autors)

⇨ keine Restriktionen bezüglich Datenschutz

3 Kommunikation

3.1 E-Mail

3.1.1 Aktuelle Situation

Alle MA haben eine Mailadresse @primarweinfelden.ch. Diese wird durch einen eigenen Mailserver (Standort Paul-Reinhart) gehostet. Das heisst, dass Mails innerhalb der Primarschule unseren Server nie verlassen und deshalb bezüglich Datenschutz unbedenklich sind.

Viele MA leiten die Mails allerdings an ihre privaten Mailadressen weiter. Viele dieser privaten Adressen werden im Ausland gehostet (gmail.ch, gmx.net u.a.), weshalb das bezüglich Datenschutz problematisch ist.

Die SuS ab der 3. Klasse haben eine Mailadresse von Microsoft365. Dies ist gemäss kantonalem Datenschutzbeauftragten nicht tolerierbar, wenn Personendaten im Spiel sind. E-Mail-Kommunikation spielt aber bei SuS der Primarschule eine marginale Rolle, zudem beschränken sich die Inhalte solcher Mails in der Regel auf Sachdaten, was unproblematisch ist (mit Ausnahme der eigentlichen Mailadresse, welche den echten Nachnamen enthält).

E-Mail-Kommunikation zwischen LP und EB ist hingegen wieder problematischer, da es häufig um Personendaten geht und die Mailprovider der EB häufig im Ausland domiziliert sind (siehe oben).

3.1.2 Primärer Handlungsbedarf ("Hochrisiko" eliminieren)

Die Mail-Weiterleitungen von MA an private Mailadressen werden aufgehoben. Alle MA sollen ihre Geschäftsmails (@primarweinfelden.ch) über ein zusätzliches Konto in einem Mailclient oder per Webmail über remote.primarweinfelden.ch empfangen und senden.

Im E-Mail-Verkehr von MA nach aussen (EB, SuS) ist auf Personendaten, insbesondere auf besonders schützenswerte Personendaten zu verzichten. Wenn dies nicht möglich ist, müssen die Informationen innerhalb eines verschlüsselten Dokumentes (passwortgeschützt) versendet werden, wobei das Kennwort dann über einen anderen Kanal mitgeteilt werden muss (Telefon, Messenger u.a.).

Heikel ist auch die Registrierung mit der Schul-Mailadresse bei Webdiensten, deren Server im Ausland sind. Es ist deshalb bezüglich Datenschutz besser, schweizerische Webdienste zu verwenden (LMVZ, Schabi u.a.).

Im Weiteren sollen die MA bezüglich datenschutz-konformer Verwendung des E-Mailings geschult werden, dazu gehört z.B. die Verwendung des Bcc-Adressfeldes bei Mails an mehrere Empfänger.

3.1.3 Sekundärer Handlungsbedarf

Um den Datenschutz zu erhöhen, werden Inhalte mit besonders schützenswerten Personendaten innerhalb eines verschlüsselten Dokumentes (passwortgeschützt) versendet.

Die SuS könnten einen Mailaccount auf unserem eigenen Mailserver erhalten. Dies ist aber kostenintensiv (ca. Fr. 15.— pro SuS jährlich). Alternativ könnten die Konten der SuS pseudonymisiert oder anonymisiert werden (siehe 4.1.3)

3.2 Messenger

3.2.1 Aktuelle Situation

Allgegenwärtig ist der WhatsApp-Messenger, sowohl in der Kommunikation unter den MA, zwischen MA und EB und auch zwischen MA und SuS, obwohl der Dienst eigentlich erst ab 16 Jahren erlaubt wäre, und die SuS der Primarschule allesamt jünger sind. Zudem benötigt WhatsApp Zugriff auf alle Kontaktdaten des Users, was datenschutzrechtlich nicht zumutbar ist.

3.2.2 Primärer Handlungsbedarf ("Hochrisiko" eliminieren)

Da WhatsApp für die Kommunikation im Schulbereich aufgrund der Datenschutzproblematik ausscheidet, wird eine Alternative benötigt. Dafür bietet sich die App "Signal" an. Diese wurde vom kantonalen Datenschutzbeauftragten bezüglich Datenschutz positiv beurteilt (OpenSource, Ende-zu-Ende-Verschlüsselung, keine Kontaktfreigabe-Pflicht). Sie ist wie WhatsApp ebenfalls gratis und bietet ungefähr die gleiche Funktionalität. Deshalb ist es zumutbar, dass auch die EB (und evt. die SuS) diese App installieren. Ein weiterer Vorteil besteht darin, dass auf diese Weise private (WhatsApp) und schulische (Signal) Chats sauber getrennt werden können. Aus Sicht des Datenschutzes können mittels Signal auch jegliche Personendaten übermittelt werden.

Aufgrund dieser Überlegungen nutzt die Primarschule Weinfelden zukünftig für schulisches Messaging ausschliesslich Signal. Soll auch mit SuS gechattet werden, muss eine Einwilligung der Eltern vorliegen, da auch Signal ein Mindestalter kennt (13 Jahre).

3.2.3 Sekundärer Handlungsbedarf

Die MA könnten mit einem Dienst-Handy ausgerüstet werden, damit für die Kommunikation mit den EB nicht die private Mobilnummer preisgegeben werden muss. Private und schulische Kommunikation könnte so noch optimaler getrennt werden. Hier stellt sich die Frage, ob dies nicht sogar dem primären Handlungsbedarf zuzuordnen wäre.

3.3 Videokonferenz-Tools

3.3.1 Aktuelle Situation

Während der Schulschliessungen infolge der Corona-Pandemie kamen erstmals Videokonferenz-Tools regelmässig zum Einsatz und zwar sowohl für den Fernunterricht als auch für die Zusammenarbeit unter den MA. Eingesetzt wurde in erster Linie das Besprechungstool von Microsoft Teams.

3.3.2 Primärer Handlungsbedarf ("Hochrisiko" eliminieren)

Wie auch unter 4.1.2 und 4.2.2 erwähnt, sollte aus Sicht des Datenschutzes zum jetzigen Zeitpunkt eigentlich auf die Verwendung von Microsoft365-Tools verzichtet werden. Zurzeit gibt es aber keine wettbewerbsfähigen und brauchbaren Alternativen mit besserem Datenschutz. Da auch für die Kollaboration (siehe nächstes Kapitel) Teams verwendet wird, drängt sich dieses Tool natürlich auf.

Um Videokonferenzen so datenschutzkonform wie möglich zu gestalten, sind aber folgende Rahmenbedingungen einzuhalten:
Es wird die Einwilligung der beteiligten MA und/oder SuS, respektive ihrer Erziehungsberechtigten benötigt. Es dürfen keine Konferenz-Aufzeichnungen ohne vorgängige Einwilligung und Mitteilung über den Verwendungszweck gemacht werden. Auf die Verwendung von Personendaten sollte wenn immer möglich verzichtet werden. Zudem hat jeder hat das Recht, ohne die Freigabe der Kamera teilzunehmen.

3.3.3 Sekundärer Handlungsbedarf

Die Entwicklung wird sorgfältig verfolgt. Vielleicht verbessert Microsoft die datenschutzrelevanten Rahmenbedingungen oder es entstehen alternative Tools, welche die nötige Funktionalität mitbringen und datenschutzrechtlich problemloser sind.

4 Datenspeicherung & Kollaboration

4.1 Datenspeicherung

4.1.1 Aktuelle Situation

Standardmässig werden Daten von MA und SuS auf dem lokalen Server gespeichert werden (Standort: Paul-Reinhart). Dieser ist bezüglich Zugriff von aussen geschützt. Ordner-Berechtigungen stellen sicher, dass innerhalb der Primarschule nur berechtigte Personen auf entsprechende Dokumente zugreifen können.

MA könnten zudem mittels einer VPN-Verbindung (Virtual Private Network = verschlüsselte sichere Verbindung) auch von ausserhalb des Schulnetzwerkes auf ihre Daten zugreifen.

Vermehrt werden die Daten aber auch in der Cloud gespeichert. Seit den Homeoffice-Zeiten im Zusammenhang mit der Corona-Pandemie hat dies zugenommen. Als Cloudspeicher wird in erster Linie OneDrive von Microsoft verwendet, da dieser Dienst eng mit den Diensten auf unserem eigenen Server gekoppelt ist (z.B. Benutzeraccount-Synchronisierung).

Die LehrerOffice-Daten liegen ebenfalls in einer Cloud, nämlich in Form einer Citrix-Anbindung beim Kanton, was datenschutzrechtlich keine Probleme verursacht.

Die Datenspeicherung auf Plattformen, die den datenschutzrechtlichen Anforderungen genügen und eine personalisierte Zugangsberechtigung verlangen, wie das genutzte Backslash-DMS, sind auch für Personendaten geeignet.

Auf den Webseiten der Primarschulzentren sind praktisch ausschliesslich Sachdaten gespeichert. Bezüglich Fotoaufnahmen von LP und Klassen wird auf Kapitel 5.1 verwiesen. Vereinzelt werden auch Personendaten veröffentlich, so z.B. die Namen der MA oder auch private Telefonnummern/Mailadressen (z.B. im PRS ⇨ Forum Eltern Schule).

4.1.2 Primärer Handlungsbedarf ("Hochrisiko" eliminieren)

Die Datenablage (insbesondere von Personendaten) auf den Microsoft-Servern ist bezüglich Datenschutz aus Sicht des kantonalen Datenschützers äusserst problematisch, obwohl die Standorte der Microsoft-Server in Europa und zukünftig sogar in der Schweiz liegen. So werden die USA niemals darauf verzichten, im Bedarfsfall auf alle von US-Firmen verwalteten Daten zuzugreifen, auch wenn die Daten nicht in den USA lagern.

Ähnliche Probleme bestehen auch bei anderen weitverbreiteten Clouddiensten, wie Dropbox, Google Drive oder iCloud, weshalb auch hier keinerlei Personendaten abgelegt werden sollten.

Da wir mit einem eigenen Server, der zudem dank VPN-Technologie auch von extern erreichbar ist, eine datenschutzkonforme Datenspeicherungslösung haben, sind alle MA zu sensibilisieren, alle Dokumente mit Personendaten auf diesem zu speichern und in der Cloud nur Dokumente mit reinen Sachdaten (z.B. Unterrichtsvorbereitungen). Möchte man Dokumente mit Personendaten in der Cloud speichern, müssen diese zwingend verschlüsselt (mit Passwort versehen) werden.

Die Einrichtung einer VPN-Verbindung ist eher kompliziert, weshalb es nicht in Frage kommt, dass auch SuS von aussen auf unseren Server zugreifen können. Da es bei Dokumenten der SuS aber in der Regel um Sachdaten geht (z.B. Arbeitsblätter), können diese vorderhand weiterhin in der Cloud gespeichert werden. Nehmen die SuS Schulgeräte mit nach Hause, ist das Problem dank "Offline-Dateien" gelöst ⇨ SuS können so ausserhalb des Schulnetzwerkes ihre Dokumente auf die gleiche Weise wie innerhalb des Schulnetzwerkes speichern. Sobald sich dann die Geräte wieder mit dem Server verbinden, werden die Daten automatisch mit diesem synchronisiert.

Bei jeglicher Veröffentlichung von Personendaten auf den Webseiten muss vorgängig das Einverständnis der Betroffenen eingeholt werden.

4.1.3 Sekundärer Handlungsbedarf

Datenschutzrechtlich problematisch bei Microsoft365 (OneDrive-Cloud, Mail, Teams usw.) sind u.a. die Benutzeranmeldedaten, welche nach dem Schema "v.nachname" erstellt werden. Solange nur Sachdaten abgespeichert werden, ist das halbwegs okay. Diese Grenze ist aber schnell überschritten, so ist z.B. bereits eine Audioaufnahme eines Schülers den Personendaten zuzuordnen.

Um auch Personendaten (ausgenommen besonders schützenswerte) abspeichern zu können, müssten diese Anmeldedaten zukünftig anonymisiert (z.B. nur eine Zahl wie "schueler3145", was in den Schulen des BBZ so gehandhabt wird) oder pseudonymisiert (z.B. NaVor11 = 2 Buchstaben des Nachnamens, 3 Buchstaben des Vornamens, Jahreszahl des Schuleintritts) werden. Letzteres würde trotzdem noch eine mehr oder weniger problemlose Identifizierung durch die MA (insb. durch die Lehrpersonen) ermöglichen. Um einem korrekten Datenschutz Rechnung zu tragen, müssten dann aber auch in allen Dokumenten (z.B. Arbeitsblätter, Schülertexte) und in allen Microsoft365-Tools (Teams, OneNote etc.) konsequent diese Pseudonyme verwendet werden.

Für MA sind anonymisierte oder pseudonymisierte Logins zwar auch denkbar, da trotz eines solchen pseudonymisierten Logins die bisherige E-Mail-Adresse beibehalten werden könnte und somit die Mailadresse weiterhin - so wie üblich - aus dem korrekten Namen gebildet würde. Es würde aber der grosse Vorteil der Synchronisierung des Benutzerlogins zwischen lokalem Server und Microsoft365 entfallen. Die MA hätten somit zwei unterschiedliche Logins.

Um den Datenschutz weiter zu erhöhen, könnte verfügt werden, dass Dokumente mit besonders schützenswerten Personendaten auch auf dem lokalen Server verschlüsselt abgelegt werden müssen.

Eine weitere Möglichkeit wäre, dass man sich einen Cloud-Anbieter in der Schweiz sucht (z.B. Swisscom). Dadurch werden allerdings die Vorteile der Kombination von Cloud und Kollaboration (siehe nächster Punkt) bei Microsoft365 preisgegeben.

4.2 Kollaboration

4.2.1 Aktuelle Situation

Der Einsatz von Kollaborationstools (Tools zur Zusammenarbeit) hat während der Coronakrise/Home-Schooling enorm zugenommen. Eingesetzt wurden v.a. Tools von Microsoft365 (Microsoft Teams, Microsoft OneNote).

4.2.2 Primärer Handlungsbedarf ("Hochrisiko" eliminieren)

Da die Datenablage auf den Microsoft-Servern aus Sicht des Datenschutzes wie im letzten Kapitel erwähnt problematisch ist, sollte eigentlich auf diese Dienste verzichtet werden. Momentan gibt es aber leider keine Alternative, welche bezüglich Funktionalität und Kosten die Dienste von Microsoft365 (Teams, OneNote, Sway, Forms u.a.) übernehmen könnte.

Setzt man Microsoft365-Tools ein, sollte zumindest aber darauf geachtet werden, dass möglichst keine Personendaten verwendet oder abgelegt werden, und wenn, dann nur verschlüsselt.

4.2.3 Sekundärer Handlungsbedarf

Werden die Benutzerkonten anonymisiert oder pseudonymisiert (siehe 4.1.3), würde die Datenschutzproblematik "entschärft". Es bleibt aber das Problem der MA-Accounts, deren Pseudonymisierung nicht sehr praktikabel ist. Evt. müssten für MA, welche Kollaborationstools verwenden, halt doch ein zusätzlicher pseudonymisierter Account eröffnet werden.

Die Entwicklung wird sorgfältig verfolgt. Vielleicht verbessert Microsoft die datenschutzrelevanten Rahmenbedingungen oder es entstehen alternative Tools, welche die nötige Funktionalität mitbringen und datenschutzrechtlich problemloser sind.

5 Weitere Bereiche

5.1 Foto-, Film- und Tonaufnahmen

5.1.1 Aktuelle Situation

Bezüglich Foto-, Film- und Tonaufnahmen im Internet gibt es zurzeit ein Informationsdokument "Datenschutz auf den Webseiten der Weinfelder Primarschulzentren", welches den EB beim Eintritt von Kindern in unsere Schule ausgehändigt wird. Darin wird darauf hingewiesen, dass Fotos von SuS – in der Regel Gruppenbilder – auf den Webseiten publiziert werden können, allerdings ohne Namen und andere persönlichen Informationen, und dass vom Einverständnis der EB ausgegangen wird, solange kein Einwand erfolgt. Es ist also eine Art "stille" Einverständniserklärung.
(https://www.schuleweinfelden.ch/downloads.html?file=files/Inhalte%20Verwaltung/Dokumente/Allgemeine%20Dokumente%2C%20Schulverwaltung/Datenschutz%20auf%20Websites.pdf oder https://bit.ly/3of6GdM)

5.1.2 Primärer Handlungsbedarf ("Hochrisiko" eliminieren)

Jegliche Aufnahmen von personenbezogenen Inhalten (Bild und Ton), auch wenn sie nur dem Unterricht dienen und weder im Internet noch sonst wo publiziert werden, sind nur erlaubt, wenn eine schriftliche Einwilligung von den betroffenen Personen (sowie den EB) vorliegt. Wenn diese Inhalte dann gar noch veröffentlicht werden (z.B. Internet), ist dies noch wichtiger.

Neu wird beim Eintritt in die Primarschule und in der Folge alle 2 Jahre (also Eintritt KG, 1./3./5. Klasse) eine entsprechende schriftliche Einwilligung (mit einem Hinweis auf das Widerrufsrecht) oder allenfalls halt auch Nicht-Einwilligung eingeholt und dem Personaldossier beigefügt. Diese Einwilligungserklärung beinhaltet auch das Publizieren von Fotos bei Schulanlässen, Klassenfotos und MA-Fotos auf den Webseiten. Dies gilt auch für alle MA.

Sobald die SuS bezüglich dieser Thematik genügend sensibilisiert sind, wird diese Einwilligung zusätzlich von den SuS unterschrieben.

5.1.3 Sekundärer Handlungsbedarf

Im Weiteren gilt es, die LP im Umgang mit dem Datenschutz von Foto-, Film- und Tonaufnahmen zu schulen. Dazu wird eine Liste erstellt mit konkreten Situationen (Unterricht, Schulanlass, Besuchstag u.a.) und was bezüglich Foto-, Film- und Tonaufnahmen jeweils erlaubt resp. nicht erlaubt ist. Ausgangspunkt ist dabei das kantonale Dokument "Konkretisierung für die Praxis" (https://av.tg.ch/public/upload/assets/82118/Leitfaden_Foto-Film-Ton.pdf oder https://bit.ly/3kmW8XS).

5.2 Kennwörter

5.2.1 Aktuelle Situation

Ein wichtiger Aspekt bezüglich Datenschutz sind Kennwörter, welche für das Login auf unsere Server (Datenserver, Mailserver), fürs Login auf diverse Online-Dienste (LehrerOffice, Microsoft365, Cloud u.a.) oder fürs Verschlüsseln von Dokumenten eine zentrale Rolle spielen, auch bei den SuS. Leider ist gemäss meiner Erfahrung der sorgfältige Umgang mit Kennwörtern noch nicht bei allen selbstverständlich. Kennwörter sind oft noch zu einfach, werden irgendwo aufgeschrieben und manchmal gar für alle sichtbar abgelegt oder aufgehängt.

5.2.2 Primärer Handlungsbedarf ("Hochrisiko" eliminieren)

Hier gilt es, die MA und SuS immer wieder zu sensibilisieren, zu schulen und den korrekten Umgang einzufordern.

6 Zusammenfassung

Die unter "primär" aufgeführten Massnahmen sollen baldmöglichst, resp. spätestens auf Beginn des Schuljahres 2021/22 umgesetzt werden. Die sekundären Massnahmen sind Ermessenssache.

	primär	Terminierung	sekundäre mögliche Massnahm.	Terminierung
E-Mail	• MA-Weiterleitung aufheben • Mail nach extern mit besonders schützenswerten Personendaten: Dateianhänge verschlüsseln • w.m. CH-Webdienste verwenden • Massenmails mit Bcc	sofort	• SuS-Konten pseudonymisieren • Schülermails auf eigenem Mailserver (hohe Kosten)	z.B. per SJ 21/22 einlaufend (neue 3. Klassen)
Messenger	• Wechsel auf Signal • Einverständniserklärung EB für SuS, falls verwendet	sofort	• Anschaffung Diensthandys	Budget 2022
Videokonferenz - Tools	• Einwilligungserklärungen einholen • Rahmenbedingungen bezüglich Aufzeichnungen, Personendaten und Kamerafreigabe einhalten	sofort	• SuS-Konten pseudonymisieren • zusätzliche pseudonymisierte MA-Konten	z.B. per SJ 21/22 einlaufend (neue 3. Klassen)
Datenspeicherung	• Datenschutzampel beachten u. Sensibilisierung für passenden Speicherort • keine Personendaten ohne Verschlüsselung in Cloud • Einwilligung für Speicherung von Personendaten auf den Webseiten (MA und SuS)	sofort per SJ 21/22	• SuS-Konten pseudonymisieren • pseudonymisierte MA-Konten • CH-Cloud /digitale Plattform in CH verwenden • konsequentes Verschlüsseln von Dokumenten mit besonders schützenswerten Personendaten	z.B. per SJ 21/22 einlaufend (neue 3. Klassen)
Kollaboration	• keine Personendaten	sofort	• SuS-Konten pseudonymisieren • zusätzliche pseudonymisierte MA-Konten	z.B. per SJ 21/22 einlaufend (neue 3. Klassen)
Foto-, Film- und Tonaufnahmen Webseiten	• Einwilligungserklärungen einholen	per SJ 21/22	• Konkretisierung in der Praxis	sobald verfügbar
Umgang mit Kennwörtern	• Sensibilisierung und Schulung	permanent		
LP / SuS	• Information und Schulung	sofort		

Nach Umsetzung der primären Massnahmen könnten folgende "Kanäle" für Daten gemäss Klassifizierung (siehe Kap. 2) eingesetzt werden:

	• interne Mails • Signal-Messenger • Speicherung lokaler Server • Mails mit verschlüsselten Dateianhängen an Externe (z.B. EB) • verschlüsselte Speicherung Cloud / Kollaborationstools • Online Datenablage bei Backslash
	zusätzlich: • Webseiteninhalte (Namen und vereinzelt andere Daten der MA / Fotos)
	zusätzlich: • Mails an EB und SuS • unverschlüsselte Speicherung Cloud / Kollaborationstools

7 Weiteres Vorgehen

Verantwortlich für die Einhaltung des Datenschutzes ist die Schulbehörde, weshalb es entsprechende Diskussionen und Beschlüsse bedarf. Die Schulbehörde trägt auch die Konsequenzen bei Nichteinhaltung. Das Risiko einer Klage ist aber sehr klein und das einer allfällig zu erwartenden Strafe ebenfalls.

Um zu entscheiden, welche Massnahmen umgesetzt werden, gilt es, einen zeitgemässen Unterricht im Auge zu behalten. Erwünscht wäre ein pragmatisches Vorgehen, das einerseits einem massvollen Datenschutz Rechnung trägt, das andererseits die neuen digitalen methodisch-didaktischen Möglichkeiten nicht allzu stark einschränkt. Ein "Restrisiko" sollte also in Kauf genommen werden. Wird die eine oder andere Datenschutzmassnahme umgesetzt und wenn immer möglich auch im Unterricht thematisiert, ist das ein wertvolles Signal gegenüber den EB, welche in der Folge allfälligen datenschutzrechtlichen "Vergehen" die nötige Toleranz entgegenbringen könnten. **All dies sollte insbesondere bei der Entscheidung, ob überhaupt (resp. welche) sekundären Massnahmen umgesetzt werden, in Erwägung gezogen werden.**

Sobald die nötigen Entscheide gefällt sind, müssen diese in geeigneter Weise den LP kommuniziert werden. Eine rein schriftliche Information ist dabei meiner Meinung nach wenig zielführend. Zusätzlich ist eine Thematisierung / Schulung an einem Teamtag (oder notfalls an einem – evt. gemeinsamen – Konvent) angezeigt, evt. mit einem Referat von einem Mitautor der kantonalen Datenschutz-Leitfäden. Das könnte auch gekoppelt werden mit der Thematik "Urheberrecht".

Zudem muss der Datenschutz auch im M+I – Unterricht mit der nötigen Sorgfalt behandelt werden.

Die "Richtlinien und Weisungen für die Lehrpersonen", sowie das Informatikreglement müssen im Anschluss noch angepasst werden. Dabei können Beschlüsse bezüglich Datenschutz in die bisherigen Reglemente integriert werden, oder es wird darin auf eine neues "Datenschutz-Reglement" verwiesen. Die Nutzungsvereinbarung, welche den Erhalt und das Verständnis dieser beiden Dokumente bestätigt, wird mit einer Einwilligung betreffend Veröffentlichung von Personendaten ergänzt.

Wertvoll wäre möglicherweise auch, wenn Richtlinien – eine Art Kommunikationskonzept – geschaffen würden, worin dargelegt wäre, welche Kommunikationskanäle (Papier, Mail, Messenger, Webseite, Gruppenchats, Push-Nachrichten...) für welche Art Dokumente (Elternbrief, Schulinformationen, Planungen...) und welche Zielgruppe (MA, SuS, EB...) eingesetzt werden sollen. Es könnte, um die allgemeine

Informationsflut etwas zu minimieren, auch definiert werden, was überhaupt kommuniziert werden muss und insbesondere auch, was nicht.

Aufgrund der rasanten digitalen Entwicklung, sowie der baldigen Gesetzesanpassungen im Datenschutzbereich müssen alle Bestimmungen in regelmässigen Abständen überprüft und bei Bedarf angepasst werden. Zudem sind vom Kanton weitere Leitfäden in Vorbereitung, deren Erkenntnisse dann auch in den Weinfelder Bestimmungen aufgenommen werden müssen.

8 Anhang

Alle kantonalen Dokumente zum Datenschutz an Thurgauer Volksschulen findet man hier:

https://av.tg.ch/angebote-und-beratung/angebote-zu-unterrichtsthemen/ict/datenschutz.html/10049# oder https://bit.ly/2HmZKLh u.a.:

- Modul Cloud-Dienste (u.a. Datenschutzampeln, Microsoft365, Pseudonymisierung)
- Modul Digitale Kommunikation (u.a. Datenschutzkonforme Messenger)
- Modul Foto-, Film-, Tonaufnahmen (u.a. Formular Einwilligungserklärung)

Datenschutz-Grundverordnung der Europäischen Union:

- https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/datenschutz/Datenschutz%20-%20International/DSGVO.html
  oder https://bit.ly/3dJUDR3
- Auswirkungen auf die Schweiz:
  https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2018/Die_EU_DSGVO_und_ihre_Auswirkungen_auf_die_Schweiz_DE_Nov18.pdf.
  oder https://bit.ly/3oeF2xR