



Datenschutz im Bildungsbereich

Verein Smarter Thurgau

ENTWURF

Datenschutz im Bildungsbereich

Verein Smarter Thurgau

Derzeit laufen im Kanton Thurgau beim Amt für Volksschule, bei der Pädagogischen Hochschule Thurgau (PHTG), beim Verein Smarter Thurgau sowie beim Datenschutzbeauftragten des Kantons Thurgau aktive Bestrebungen, gemeinsam einen modularen Leitfaden zum Datenschutz an den Schulen herauszugeben. Die einzelnen Module sollen in regelmässigen Abständen den Schulen zur Verfügung gestellt werden. Da diverse Schulgemeinden derzeit bereits damit beschäftigt sind, die eigene Informatik an den aktuellen Stand der Technik anzupassen, wird dieser Bericht schon heute (als Entwurf) veröffentlicht. Dadurch soll verhindert werden, dass während der aktuellen Sommerferienzeit unnötige Bestellungen vorgenommen werden. Es ist zu erwarten, dass gegen Ende September 2019 bereits das erste Modul des gemeinsamen Leitfadens veröffentlicht werden kann.

Der Verein Smarter Thurgau ist eine Vereinigung, die sich für optimale Rahmenbedingungen einsetzt, damit die Chancen der Digitalisierung für das Leben, Wohnen und Arbeiten im Kanton Thurgau nachhaltig genutzt werden können. Im Bereich Bildung sollen smarte Technologien die Wissensvermittlung und das Anwendungswissen für Schüler, Lernende, Erwachsene, Menschen mit Behinderung und Angehörige der «Silver Society» unterstützen. Der Datenschutzbeauftragte des Kantons Thurgau hat deshalb in Absprache mit dem Verein Smarter Thurgau die folgenden Gedanken zusammengestellt.

Entwurf vom 16. Juli 2019

Zitiervorschlag: Entwurf Datenschutz Smarter Thurgau 07/2019

Inhaltsverzeichnis

1	Anwendbare Gesetze	1
2	Personendaten	1
3	Recht zur Datenbearbeitung	2
4	Einwilligung	2
5	Klassifizierte Daten	2
6	Personendaten in einer Cloud	2
6.1	Verantwortlichkeit	3
6.2	Cloud-Nutzung unerwünscht	3
6.3	Vertragliche Möglichkeiten	3
6.4	Verschlüsselte Daten	4
6.5	Office 365	4
7	E-Mail im Schulwesen	4
7.1	Eigene Mailserver	4
7.2	Behördliche Server	5
8	Log-Daten für Kontrollzwecke	5
9	Datenschutz auf Webseiten	5
9.1	Schutz direkt Betroffener	5
9.2	Schutz Webbenutzer	5
10	EU DSGVO	5
11	Messengerdienste	6
12	Weitere Informationen	6

lic. iur. Fritz Tanner, Rechtsanwalt

Datenschutz im Bildungsbereich

Stichworte: Bildung, Cloud, Schulen, Wissen

Smarte Technologien sollen im Bildungsbereich unterstützend wirken. Sowohl didaktisch als auch im administrativen Bereich sind dabei die Bestimmungen des Datenschutzes zu beachten.

1 Anwendbare Gesetze

Das Ziel des Datenschutzes besteht im Schutz der Persönlichkeit. Um dieses Ziel zu erreichen, finden wir in diversen Gesetzen verschiedene Bestimmungen zum Datenschutz. Neben diesen vielen Einzelbestimmungen haben sowohl der Bund als auch die Kantone explizite Datenschutzgesetze erlassen. Das Bundesgesetz zum Datenschutz und die kantonalen Datenschutzgesetze haben verschiedene Anwendungsbereiche. Falls eine Bundesbehörde oder eine Privatperson Personendaten bearbeitet, sind die Bestimmungen des Bundesgesetzes über den Datenschutz¹ zu beachten. Sofern aber Daten durch eine Behörde im Kanton Thurgau bearbeitet werden, kommt das Datenschutzgesetz des Kantons Thurgau² zur Anwendung.

Neben den Bestimmungen des Datenschutzgesetzes sind bei der Datenbearbeitung auch die strafrechtlichen Regelungen des Schweizerischen Strafgesetzbuches³ zu beachten. Bei der Bearbeitung von Personendaten kann es im Bildungsbereich sehr rasch zu Geheimnisverletzungen kommen, weshalb dem

Amts-⁴ oder allenfalls auch dem Berufsgeheimnis⁵ ein wichtiger Stellenwert zukommt.

2 Personendaten

Die Bestimmungen des Datenschutzes bezwecken, die Persönlichkeit der betroffenen Personen zu schützen. Der Datenschutz gilt somit vor allem bei der Bearbeitung von Personendaten. Neben den Personendaten gibt es aber auch noch die Kategorie der Sachdaten. Diese weisen keinen Bezug zu Personen auf. Reine Sachdaten sind datenschutzrechtlich nicht relevant, können aber bei unvorsichtigem Umgang zu einer Amts- oder Berufsgeheimnisverletzung führen. Ebenso können diese durch ungünstige Datenverknüpfungen doch noch datenschutzrechtlich relevant werden.

Es bedarf keiner weiterer Erklärung, dass es sich bei Personendaten um Daten von Personen handelt. Dennoch konkretisieren die Datenschutzgesetze, dass es sich bei Personendaten um Angaben über natürliche oder juristische Personen handelt, sofern diese bestimmt oder bestimmbar sind⁶. Bestimmt ist eine Person bereits dann, wenn sie durch ihren Namen bezeichnet wird. Bestimmbar bedeutet, dass die Person erst durch weitere Umstände erkennbar wird. Ist dies der Fall, sind die Bestimmungen des Datenschutzes in beiden Fällen zu beachten, damit es zu keinen Persönlichkeitsverletzungen kommt. Die Bestimmun-

¹ DSG (SR 235.1)

² TG DSG (RB 170.7)

³ StGB (SR 311.0)

⁴ Amtsgeheimnis: Art. 320 StGB

⁵ Berufsgeheimnis: Art. 321 StGB

⁶ § 3 TG DSG

gen des Datenschutzes gelten also nicht nur bei der Bearbeitung von konkreten Namenslisten, sondern bereits bei der Bearbeitung von Daten, welche nur einen geringen Bezug zu Personen aufweisen.

3 Recht zur Datenbearbeitung

Personendaten dürfen grundsätzlich nur bearbeitet werden, wenn dies entweder durch ein Gesetz oder durch die betroffene Person erlaubt wird⁷. Bei der Bearbeitung von besonders schützenswerten Personendaten⁸ gelten besondere Bestimmungen, weshalb mit solchen Daten dementsprechend vorsichtig umzugehen ist.

4 Einwilligung

Für den Fall, dass keine gesetzliche Grundlage für die Bearbeitung von Personendaten besteht, wird häufig versucht, die Bearbeitung mit einer Einwilligung zu rechtfertigen. An die Gültigkeit von Einwilligungen werden aber immer mehr Anforderungen gestellt. Sobald mit Einwilligungen gearbeitet wird, ist beispielsweise sicherzustellen, dass diese aufgeklärt erfolgt sind. Das bedeutet, dass eine Einwilligung zur Datenbearbeitung nur dann gültig ist, wenn die einwilligende Person vorgängig über die Folgen einer Einwilligung umfassend und in verständlichen, einfachen Worten auf die möglichen Folgen einer Einwilligung hingewiesen wurde. Vermehrt ist es auch der Hinweis erforderlich, dass die Einwilligung jederzeit widerrufen werden kann und an welche Adresse der ein entsprechender Widerruf rechtsgenügend erklärt werden müsste. Im Weiteren ist sicher zu stellen, dass die richtige Person die Einwilligung erklärt hat. Alle diese Voraussetzungen sollten schriftlich festgehalten werden, da-

mit die entsprechenden Dokumente bei allfälligen Rechtsstreitigkeiten beweisbar vorgelegt werden können.

5 Klassifizierte Daten

Im Schulbereich gelten Personendaten grundsätzlich als vertraulich. Mit diesen ist deshalb vorsichtig umzugehen. Sobald jedoch nur einfache Sachdaten, welche keinem Geheimnis unterliegen, bearbeitet werden, gelten die strengen Datenschutzvorgaben nicht mehr. Es ist deshalb zulässig, nicht vertrauliche Sachdaten mit Dritten auszutauschen. So kann beispielsweise eine neue Schulbroschüre durchaus in einer Cloudumgebung oder über unsichere Mail-systeme realisiert werden, solange dadurch keine sicherheitsrelevanten Nachteile entstehen. Es ist deshalb sinnvoll, die jeweiligen Daten vor der Verwendung zu kategorisierten bzw. zu klassifizieren. Dadurch kann erreicht werden, dass bei der Datenbearbeitung einheitliche Regelungen verwendet werden und Fehler vermindert werden.

6 Personendaten in einer Cloud

Bei der Datenbearbeitung in einer Cloud, werden Daten auf einem fremden Server bearbeitet. Die Daten, seien es Sach- oder Personendaten bzw. sogar besonders schützenswerte Personendaten, müssen dazu auf die Systeme von Dritten gebracht werden bzw. diesen zur Verfügung gestellt werden. Sobald die Daten zu Dritten gelangen oder von diesen abgerufen werden können, soll hier von Clouddiensten gesprochen werden.

⁷ § 4 TG DSG

⁸ Das Datenschutzgesetz des Kantons Thurgau hält in § 4 fest, dass es sich bei Angaben über die religiöse, weltanschauliche oder politische Ansicht oder Betätigung, bei Daten zum persönlichen Geheimbereich, zum seelischen, geistigen oder körperlichen Zustand, bei Massnahmen der sozialen Hilfe oder der fürsorgerischen Betreuung und bei Daten zu Straftaten und die dafür verhängten Strafen oder Massnahmen um besonders schützenswerte Personendaten handelt, welche nur ausnahmsweise bearbeitet werden dürfen. Diese Liste ist aber nicht abschliessend.

6.1 Verantwortlichkeit

Paragraph 6 TG DSG bestimmt, dass das öffentliche Organ bei der Bearbeitung von Personendaten dafür verantwortlich ist, dass diese datenschutzkonform bearbeitet werden. Das gilt selbstverständlich auch, wenn diese Personendaten zur Bearbeitung an Dritte ausgelagert werden.

6.2 Cloud-Nutzung unerwünscht

Es ist vom Grundsatz auszugehen, dass Personendaten nicht in eine fremde Cloud gelangen dürfen. Sobald Daten auf fremde Systeme gelangen, können diese Daten grundsätzlich von externen Systemanbietern eingesehen werden. Damit werden Personendaten an Dritte bekannt gegeben, was nur zulässig ist, wenn dies entweder in einem Gesetz erlaubt wird oder die Einwilligung der betroffenen Personen vorliegt. Im Strafgesetzbuch wird ähnlich erwähnt, dass es verboten sei, Geheimnisse zu «offenbaren». Um das Gesetz zu verletzen, genügt es auch hier bereits, wenn das Geheimnis in den «Herrschaftsbereich» eines Dritte gelangt. Ab diesem Zeitpunkt gelten die Geheimnisse als offenbart bzw. als dem Dritten bekannt gegeben. Konkret besteht somit eine Gesetzesverletzung, wenn ein einzelner Administrator des Cloud-Anbieters die Möglichkeit hätte, in die bei ihm gespeicherten Daten Einblick zu nehmen⁹.

6.3 Vertragliche Möglichkeiten

Neben den allgemeinen Risiken bei der Auftragsbearbeitung durch Dritte sind vor dem Einsatz einer Cloud-Lösung weitere Aspekte zu beachten. Soweit also eine Cloud-Lösung datenschutzrechtlich möglich ist, muss mit dem

Anbieter ein Vertrag abgeschlossen werden, damit die Einhaltung mindestens der folgenden Punkte sichergestellt werden kann:

- Es muss klar erkennbar sein, wo die Standorte der Server liegen.
- Es muss das Recht eingeräumt werden, dass beim Cloud-Anbieter unangemeldete Kontrollen durchgeführt werden dürfen. Dies ist aber nur möglich, wenn sich die Server in der Schweiz befinden. Im Ausland können Kontrollen höchstens rechtshilfweise durchgeführt werden, wodurch unsere Daten unweigerlich an andere Staaten bekannt gegeben werden, was nicht erlaubt ist.
- Es ist klarzustellen, dass für die Verträge Schweizer Recht anwendbar ist und ein Schweizer Gerichtsstand gegeben ist.
- Datenschutzrechtliche Ansprüche müssen auch beim Serverbetreiber umgehend durchgesetzt werden können. So muss dieser Lösungs- und Berichtigungsrechte in jedem Fall umgehend beachten. Die Daten dürfen aber erst nach Rücksprache mit der verantwortlichen Behörde gelöscht werden.
- Die Daten müssen gemäss jeweiligem Stand der Technik bestmöglichst geschützt werden.
- Der Serveranbieter hat sich zu verpflichten, dass die erhaltenen Daten vertraulich behandelt werden und nicht an Dritte herausgegeben werden, bzw. diesen offenbart werden. Allenfalls sind die Anforderungen an die Verschlüsselung und

⁹ Das Bundesgericht stellt im Entscheid 6B_1403/2017 vom 8. August 2018 entgegen der früheren Meinung von BGE 142 IV 65 fest, dass die Tat bei Verletzung des Fabrikations- oder Geschäftsgeheimnisses vollendet sei, sobald ein Aussenstehender dank dem Verhalten des Täters Kenntnis vom betreffenden Geheimnis erhält. Solange der Dritte aber die Geheimnisse nicht zur Kenntnis genommen habe, handle es sich erst um einen Versuch. Diese Feinheit ist vorliegend aber als Nebensächlich zu werten, da auch der Versuch einer Amtsgeheimnisverletzung strafrechtlich geahndet wird. Es soll somit alles unterlassen werden, dass Daten an unberechtigte Dritte offenbart werden.

an den Geheimnisschutz vertraglich klar zu fixieren, wobei der Cloudanbieter und weitere Dritte keinen Zugriff auf die Schlüssel erhalten darf. Hier sei auf die obigen Ausführungen verwiesen, wonach US-Unternehmen derzeit aufgrund des Cloud Acts rechtlich nicht in der Lage sind, Geheimhaltungsbestimmungen einzuhalten.

- Bei Datenverlust oder Datenmissbrauch hat der Anbieter den Auftraggeber unaufgefordert, sofort und vollumfänglich zu informieren.
- Drittanbieter dürfen nicht ohne Zustimmung des Auftraggebers beigezogen werden.
- Es ist sicherzustellen, dass nach Auflösung des Vertragsverhältnisses die Datenportabilität zum Auftraggeber gewährleistet ist und die Daten beim Anbieter sicher gelöscht werden.
- Insbesondere die Pflicht zur Verschwiegenheit ist durch eine genügend starke Konventionalstrafe zu sichern.

6.4 Verschlüsselte Daten

Sofern Personendaten verschlüsselt auf Cloud-Diensten oder auf andere Art bei Dritten gespeichert werden, ist zu beachten, dass die gewählte Verschlüsselung jede Einsichtnahme durch den Anbieter verhindert. Es ist sicher zu stellen, dass der Anbieter keinen Zugriff auf die Schlüssel erhält.

6.5 Office 365

Bei der Verwendung von Office 365 werden Daten bei Dritten bearbeitet. Es sind deshalb die Bestimmungen zu den Clouddiensten zu beachten. Da es sich bei Microsoft um eine US-Unternehmung handelt, ist diese gehalten, die US-Gesetze einzuhalten. Dazu gehört leider auch der «Clarifying Lawful Overseas Use of Data Act» (Cloud Act) vom 23. März

2018, welcher amerikanische Anbieter elektronischer Kommunikationsdienste wie Microsoft ausdrücklich verpflichtet, auch die im amerikanischen Ausland gelegenen Daten an die Behörden der USA auszuliefern. Somit kann sich ein amerikanischer Cloudanbieter rechtlich gar nicht verpflichten, unsere Cloudbestimmungen zu akzeptieren. Es ist deshalb rechtlich nicht zulässig, Personendaten und weitere vertrauliche Daten mit der Cloudlösung von Office 365 zu bearbeiten. Microsoft versucht, eine allfällige Datenschutzkonformität damit zu erreichen, dass die Daten nur verschlüsselt gespeichert würden. Dazu benötigt Microsoft aber den möglichen Zugang auf den Schlüssel, wodurch die Verschlüsselung nicht mehr gegeben ist und die Cloudvorgaben nicht eingehalten werden können. Mit der Applikation Office 365 dürfen deshalb weder Personendaten noch vertrauliche Daten bearbeitet werden.

7 E-Mail im Schulwesen

7.1 Eigene Mailserver

Bei Verwendung von E-Mails können sich Probleme ergeben, weil die Daten im Internet oft an Dritte bekannt gegeben werden. Sobald Maildaten zu einem externen Mailanbieter wie beispielsweise xy@gmail.com oder xy@gmx.ch etc. gelangen, können diese von den Providern mitgelesen und ausgewertet werden. Da die Eltern jeweils eigene Mailanbieter verwenden, ist es nicht angebracht, dass Lehrpersonen mit den Eltern über Mail kommunizieren. Anders kann es bei der Kommunikation mit den eigenen Schülerinnen und Schülern sein, da diesen eine eigene Mailadresse der Schule zugeteilt werden könnte. Sobald dann der Mailverkehr zwischen den Lehrpersonen und den Schülerinnen und Schülern nur noch über den eigenen Mailserver verläuft - und somit nicht mehr bei Drittanbietern wie gmail oder gmx etc. durchgeführt wird - werden die Daten nur noch intern ausgetauscht. Bei einer gut verschlüsselten Leitung kann dadurch erreicht werden, dass sowohl der Weg als auch der Speicherort der E-Mails ver-

traulich ist, weshalb gegen den Mailversand auf eigenen Mailservern nichts einzuwenden ist.

7.2 Behördliche Server

Es ist verständlich, dass nicht alle Schulen im Kanton Thurgau die Möglichkeit haben, eigene Mailserver für die Kommunikation mit den Schülerinnen und Schülern aufzusetzen. Deshalb bieten sich hier zwei weitere Lösungsmöglichkeiten an:

- Entweder wird für den Betrieb der Mailserver eine Drittperson beigezogen, welche sich verpflichtet die Cloudvorgaben einzuhalten (Daten in der Schweiz, Vertraulichkeitserklärung, Kontrollmöglichkeit, Datenschutzdurchsetzung etc.)
- oder es wird versucht, mit dem Amt für Informatik des Kantons Thurgau eine entsprechende Lösung anzustreben.

Die zweitgenannte Lösung hätte den Vorteil, dass der Mailverkehr nun behördenintern erfolgt, da das Amt für Informatik auch an das Amtsgeheimnis gebunden ist.

8 Log-Daten für Kontrollzwecke

Wird zur Bearbeitung von Personendaten eine neue Software evaluiert, ist zu beachten, dass diese die Möglichkeit bietet, die Bearbeitung von Personendaten zu kontrollieren. Entsprechende Applikationen müssen deshalb die Möglichkeit bieten, die Zugriffe auf Personendaten vollständig zu protokollieren. Soweit eine Bearbeitung nicht immer der gleichen Person zugeordnet werden kann, ist also mit automatischen Log-Dateien sicherzustellen, wer zu welchem Zeitpunkt die betreffenden Personendaten bearbeitet hat.

9 Datenschutz auf Webseiten

9.1 Schutz direkt Betroffener

Im Kanton Thurgau besteht keine gesetzliche Grundlage, welche es erlauben würde, Photos von Schülerinnen und Schülern oder von Lehrpersonen im Internet zu veröffentlichen. Dies

gilt auch für die Aufschaltung von Klassenfotos, da auf diesen Personen bestimmt oder bestimmbar sind. Deshalb dürfen Klassenfotos im Internet nur publiziert werden, wenn die aufgeklärte und beweisbare Einwilligung der Erziehungsberechtigten - und je nach Alter auch der betroffenen Personen selbst - vorliegt.

9.2 Schutz Webbenutzer

Beim Betrieb einer Webseite ist nicht nur zu beachten, dass die Persönlichkeitsrechte der Schüler und Lehrpersonen durch eine vorschnelle Datenbekanntgabe verletzt werden könnten. Es ist auch daran zu denken, dass beim Einsatz von Webseiten die Persönlichkeitsrechte der Seitenbenutzer verletzt werden können. So kann mit Analyseprogrammen wie Google-Analytics oder durch den Einsatz von weiteren Werkzeugen wie beispielsweise die Einbindung externer Schriften oder bei Dritten abzurufenden Symbolen durch Unberechtigte herausgefunden werden kann, welche Seiten ein Benutzer vorzugsweise besucht. Dadurch können nicht nur Rückschlüsse auf dessen Surfverhalten, sondern auch auf dessen Persönlichkeit getroffen werden. Dies ist datenschutzrechtlich nicht erlaubt.

10 EU DSGVO

Die am 25. Mai 2018 als anwendbar erklärte EU Datenschutz-Grundverordnung (EU-DSGVO) ist ausländisches Recht und müsste deshalb durch die Schulen des Kantons Thurgau gar nicht beachtet werden. Es empfiehlt sich jedoch, die EU-DSGVO dennoch zu beachten, da sonst im EU-Ausland gegen uns ein Urteil erwirkt werden könnte, welches dann in der Schweiz vollstreckbar wäre. Dieses neue ausländische Regelwerk sollte deshalb von den Schulen im Kanton Thurgau insbesondere beachtet dann werden,

- wenn die Dienste eines Auftragsdatenbearbeiters mit Sitz in der EU in Anspruch genommen wird (was beispielsweise beim Einsatz von Clouddiensten der Fall sein kann),

- falls das Verhalten von Personen in der EU beobachtet wird (was beim Einsatz von Trackingtools auf der Webseite erfolgen kann) oder
- falls an Personen mit Wohnsitz in der EU Waren oder Dienstleistungen angeboten werden, sei dies gegen Geld oder kostenlos.

Ausnahmen können sich ergeben, soweit die Schulen gestützt auf Art. 6 Abs. 1 lit. e EU-DSGVO Personendaten nur soweit bearbeitet, als dies «für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde». In diesen Fällen ist die Datenbearbeitung jeweils rechtmässig und erlaubt.

11 Messengerdienste

Bei Messengerdiensten sind die Bestimmungen betreffend der Cloud-Nutzung analog anwendbar. Bei Diensten, welche eine Ende-zu-Ende

Verschlüsselung anbieten, ist sicher zu stellen, dass im Programmcode keine Möglichkeit vorbehalten werden kann, die Daten dennoch unverschlüsselt dem Anbieter zu offenbaren¹⁰. Im Weiteren ist zu beachten, dass keine weiteren Personendaten, wie beispielsweise die eigenen Kontaktdaten, an den Anbieter freigeschaltet werden¹¹.

12 Weitere Informationen

Derzeit erarbeitet das Amt für Volksschule in Zusammenarbeit mit der Pädagogischen Hochschule Thurgau (PHTG), dem Verein Smarter Thurgau und dem Datenschutzbeauftragten des Kantons Thurgau einen Leitfaden zum Datenschutz an den Schulen. Darin wird neben weiteren Datenschutzthemen insbesondere die Nutzung von Messengerdiensten, der Einsatz von Office 365 sowie die Verwendung von Foto- und Filmaufnahmen näher thematisiert. Für weitere Informationen wird auf die kommende Publikation verwiesen.

Stand: 16. Juli 2019

¹⁰ Vorzugsweise Open Source Code.

¹¹ Der Zugriff auf die Kontakte ist bei WhatsApp nicht einschränkbar.

Erfasste Themenbereiche

