Datenschutz-Newsletter Nr. 4

Juni 2015

Sehr geehrte Schulleiterinnen,

sehr geehrte Schulleiter,

obwohl der Datenschutz in Deutschland in letzter Zeit vermehrt in der Kritik steht und damit oftmals als hinderlich realitätsfern wahrgenommen wird, möchte ich weiterhin für den Datenschutz werben und Sie mit meinem vierten Newsletter weiter sensibilisieren.

Gerade die Nachrichten der letzten Woche und Monate mit Enthüllungen über Cyberangriffe auf den Bundestag, Ausspähungen unter Freunden und sogar einem Angriff auf das Netzwerk eines der größten Softwareschmieden für Antivirus-Software haben gezeigt, wie wichtig es ist, persönliche Daten zu sichern und zu schützen. Deshalb gebe ich der Thematik der „Risiken im Internet“ und wie man sich davor schützen kann, heute etwas mehr Raum im Newsletter.

Da jetzt bald wieder die Abschlussbälle an den Schulen stattfinden werden, möchte ich Sie auch noch mal auf den hinsichtlich der Anwesenheit externer bzw. professioneller Fotografen sensibilisieren und habe Ihnen dazu die Aussagen des Bayerischen Landesbeauftragten für Datenschutz zusammengefasst.

Weitere Kurznotizen betreffen die Löschungsfristen von Schülerdaten, die Anschaffung von Smart-TVs oder auch Streaming-Boxen für Unterrichtsräume, die Behandlung sensibler Daten auf Datenträgern, Smartphones und Tablets.

Mit freundlichen Grüßen

Norbert Raith, L und DSB

Datenschutzbeauftragter des Schulamtsbezirks Neumarkt i.d. OPf.

Norbert Raith, L
Mittelschule Dietfurt
Mallerstetter Str. 25
92345 Dietfurt
☎ 08464-381
Raith-DSB-NM@gmx.de

Hilfen und Vorschriften

Datenschutz in der Schule: http://www.km.bayern.de/download/4837_lfd_broschuere_schule.pdf

http://www.km.bayern.de/ministerium/recht/datenschutz.html

Rechtliche Grundlagen: https://www.mebis.bayern.de/service/recht/datenschutz/grundlagen/

Vorlagen: https://www.mebis.bayern.de/service/recht/datenschutz/muster-vorlagen/

Kurznotizen:

• Vernichtung von sensiblen Daten bzw. Datenträgern:

Der folgende Link soll Sie darüber informieren, wie bei der Vernichtung von sensiblen Daten in Ihrer Dienststelle umgegangen werden soll. Unter dem Begriff „Sichere Vernichtung“ versteht man das Vernichten von schutzwürdigen Informationen auf Datenträgern in der Art, dass ihre Reproduktion der auf ihnen wiedergegebenen Informationen unmöglich ist oder weitgehend erschwert wird.

https://www.datenschutz-bayern.de/technik/orient/oh_datentraegerentsorgung.pdf

• Smart-TVs und Streaming-Boxen an Schulen

Bei der Anschaffung neuer TV-Geräte für Unterrichtsräume sollte darauf geachtet werden, dass, wenn es überhaupt ein Smart-TV sein muss, Kamera und Sprachsteuerung leicht abzuschalten sind!

Smart-TV-Geräte und Streaming-Boxen sammeln Nutzerdaten auf Basis von Nutzerdaten (welche Apps und welche Filme werden wie und wann genutzt), Sprachbefehlen, etc. und reichen diese an die Hersteller weiter, um Werbung besser personalisieren zu können und um „Anwendungen zu verbessern“…..

Hinzu kommt die Gefahr, dass Smart-TVs nicht unbedingt besonders gegen Angriffe gesichert sind.

Ein Beispiel hierfür bietet die Sendung Plusminus http://www.daserste.de/information/wirtschaft-boerse/plusminus/videos/smart-tv-sicherheitsluecken-bei-internet-betrieb-100.html

Deshalb: Schalten Sie bei Smart-TVs Kamera und Sprachsteuerung ab oder erlauben Sie den Geräten keinen Zugriff auf das Internet.

Externe Fotografen

Die Schule kann jederzeit für die Erstellung von Schülerfotos einen externen Fotografen dafür beauftragen. In diesem Falle sind allerdings die gesetzlichen Vorgaben des **Art. 6 BayDSG** über die Auftragsdatenverarbeitung zu beachten und einen schriftlichen Vertrag mit dem Auftragnehmer abzuschließen.

Die Verantwortung in Sachen Datenschutz obliegt aber immer noch dem Auftraggeber, also der Schule und damit insbesondere dem Schulleiter/ der Schulleiterin.

Deshalb sollte bei der Auswahl des Auftragnehmers besonders darauf geachtet werden, dass dieser auch dazu geeignet ist.

Zu beachten ist auch, dass die erhobenen Daten (Foto und Adressen der Schüler) nicht zu anderen Zwecken benutzt werden dürfen.

Natürlich ist auch darauf zu achten, dass eine datenschutzkonforme Einwilligungserklärung der Erziehungsberechtigten bzw. der Schüler an der Schule vorliegt.

Auch die Weitergabe von personenbezogenen Daten an den externen Partner ist nur mit o. g. Erklärung zulässig.

Ebenso ist eine Weitergabe aller Fotos, zum Beispiel auf einem Datenträger, an alle Schüler nur mit einer Einwilligungserklärung rechtens.

Dies gilt auch für die Werbung auf der Internetseite des Auftragnehmers o.ä. mit den Fotos oder sogar Videos.

Auf der Schul-Homepage darf nicht für den Fotografen geworben werden!

Youtube-Filme mit Schülern

Laden Sie keine Filme, die Ihre Schüler zeigen, auf Server außerhalb der europäischen Union bzw. des EWG-Raumes. Nutzen Sie deutsche bzw. europäische Server, die den deutschen Datenschutzbestimmungen entsprechen!

http://dozenten.alp.dillingen.de/mp/recht/kmbek-medienbildung2012.pdf

Kurznotizen:

• Löschungsfristen:

· Wollen Sie WORD-, EXCEL-, oder ähnliche Dateien, wie z.B. Mitteilungen, Verweise, Sportfestergebnisse, usw.. abspeichern, so müssen personenbezogene oder personenbeziehbare Daten anonymisiert werden. D.h., diese Daten müssen so verändert werden, dass die Angaben keiner bestimmten Person zugeordnet werden können.
· Art. 12 Abs. 1 Nr. 2 BayDSG verlangt eine umgehende Löschung der Daten, sobald diese für die Aufgabenerfüllung nicht mehr erforderlich sind.
· Wenn keine Rechtsgrundlage mehr besteht, sind Daten ebenfalls zu löschen.
· Schülerdaten (Unterrichts- oder Leistungsdaten) sind nach Ablauf des nachfolgenden Schuljahres zu löschen.

• Notenverwaltung:

Bei Schülernoten handelt es sich um sensible personenbezogene Daten, auf die Lehrkräfte nur in dem sachlichen und zeitlichen Umfang zugreifen dürfen, der für die Erfüllung ihrer jeweiligen Aufgabe tatsächlich erforderlich ist. Im Rahmen dieser Erforderlichkeitsprüfung ist abzuwägen zwischen dem Informationsinteresse der Lehrkräfte einerseits und dem Persönlichkeitsrecht der Schülerinnen und Schüler andererseits. Die Schülerinnen und Schüler haben einen Anspruch darauf, nicht befürchten zu müssen, dass schlechte Zensuren einer Lehrkraft in einem Fach bei den übrigen Lehrkräften - wenn auch nur unbewusst - zu einem negativen Eindruck oder gar zu einer Voreingenommenheit führen. Somit muss das Informationsinteresse der Lehrkräfte zumindest teilweise hinter dem Persönlichkeitsrecht der Schülerinnen und Schüler zurücktreten. Aus datenschutzrechtlicher Sicht ist es daher nicht zulässig, allen Lehrkräften jederzeit und anlasslos einen fächerübergreifenden Einblick in die Leistungsdaten ihrer Schülerinnen und Schüler einzuräumen.

https://www.datenschutz-bayern.de/tbs/tb26/k10.html#10.1

• Private Smartphones und Tablets als Dienstgeräte:

Auf die Nutzung von Apps, die Schülerdaten speichern und verwalten, sollte verzichtet werden, da diese Daten im Regelfall automatisch in der Cloud gespeichert werden und oftmals zusätzlich Nutzerdaten erhoben werden.
Googles Clouddienste „GoogleDocs“, „G-Mail“ etc. verarbeiten und „lesen“ automatisiert Dateien, die damit verschickt oder bearbeitet werden. Für dienstliche Belange ist dies nicht zulässig!
Ebenso ist eine Verarbeitung und Speicherung von dienstlichen Daten auf dem privaten Notebook, Tablet, Smartphone oder USB-Sticks mit äußerster Vorsicht zu betrachten. Verschlüsseln Sie!
https://www.datenschutz.de/news/detail/?nid=7260
Siehe den 25. Tätigkeitsbericht des Landesbeauftragten für Datenschutz Nr. 2.1.3
https://www.datenschutz-bayern.de/tbs/tb25/tb25.pdf

Links

Datenschutz in der Schule: http://www.km.bayern.de/download/4837_lfd_broschuere_schule.pdf

Rechtliche Grundlagen: https://www.mebis.bayern.de/service/recht/datenschutz/grundlagen/

Vorlagen: https://www.mebis.bayern.de/service/recht/datenschutz/muster-vorlagen/

FAQ Datenschutz: https://www.mebis.bayern.de/service/recht/datenschutz/fragen-und-antworten-3/

Weitere Hilfen : Fachberatung Informatik oder DSB im Schulamtsbezirk NM

Wichtige Grundsätze, die das Surfen im Internet sicherer machen

1. Betriebssysteme wie Windows 8.1, Windows 7, OSX weisen immer wieder Sicherheitslücken auf. Nutzen Sie deshalb unbedingt die automatische Updatefunktion des Betriebssystems. Überprüfen Sie auch regelmäßig Browser wie Firefox oder Chrome und Programme wie Java oder Flash auf Updates!
2. Windows XP auf PCs mit Internetzugang ist ein Sicherheitsrisiko – Ersetzen Sie es!
3. Surfen oder mailen Sie niemals als administrativer Benutzer. Legen Sie sich zum Surfen und Mailen ein eigenes Benutzerkonto ohne „administrativen Berechtigungen“ an.
4. Verwenden Sie eine Antiviren-Software auf Ihrem PC, die sich täglich mehrmals selbstständig aktualisiert. Wenn Sie MS Outlook nutzen, achten Sie darauf, dass ihre Antiviren-Software auch den Posteingang wirklich überprüft. Nicht jede kostenlose Antiviren-Software kann dies!
5. Verschlüsseln Sie Ihr WLAN zuhause ausschließlich mit WPA2. Für die missbräuchliche Nutzung Ihres heimischen WLANS können Sie oftmals haftbar gemacht werden.
6. Bedenken Sie, dass E-Mail-Absender-Adressen gefälscht werden können. Öffnen Sie E-Mail-Anlagen nur dann, wenn Sie absolut sicher sind, dass sie tatsächlich vom angegebenen Absender stammen. Auch vermeintlich „sichere Dokumententypen“ wie Office– und PDF-Dokumente können für Angriffe verwendet werden.
7. Untersuchen Sie USB-Sticks und andere externe Datenträger erst mit einer Antivirensoftware, bevor Sie darauf zugreifen.
8. Setzen Sie zumindest die Firewall ein, die Windows 8.1 mitbringt und überprüfen Sie regelmäßig deren Einstellungen. Besser noch wären Sicherheitslösungen von z.B. Kaspersky, Norton, F-Secure. Aktuelle Tests finden Sie hier: http://www.av-test.org/de/antivirus/privat-windows/
9. Vermeiden Sie die Nutzung der PIN/TAN-Liste beim Online-Banking, nutzen Sie c’tBankix oder HBCI. http://www.heise.de/ct/projekte/Sicheres-Online-Banking-mit-Bankix-284099.html
10. Nutzen Sie für sichere Passörter mind. 12 Zeichen, Groß- und Kleinbuchstaben und Sonderzeichen - oder nutzen Sie ein Programm wie Keepass, das sich all Ihre Passwörter merkt und verschlüsselt ablegt.
11. Setzen Sie auf Mail-Provider, die Mails grundsätzlich – „end-to-end“(also beim Absenden bzw. beim Empfänger) und nicht erst beim Provider ver- und entschlüsseln. https://www.test.de/E-Mail-Provider-Mail-Dienste-sehen-alles-4806144-0/
12. Achten Sie darauf, die Browser-Chronik regelmäßig zu löschen – Sie wollen doch nicht, dass Google, Facebook, Amazon oder auch andere Firmen wissen, welche Seiten Sie in den letzten drei Wochen besucht haben?
13. Sichern Sie Ihre Daten regelmäßig, verschlüsseln Sie diesen Datenträger, v.a. wenn dienstliche Daten darauf ausgelagert werden und bewahren Sie den Datenträger an einem sicheren Ort auf. Hier kann ihnen TrueCrypt 7.1 immer noch gute Dienste erweisen.
14. Wenn Sie Ihre Daten in einer Cloud sichern, dann achten Sie darauf, dass dienstliche Daten nur verschlüsselt und keinesfalls auf Servern außerhalb der EWG gespeichert werden.
15. Überprüfen sie auf jeden Fall die Datenschutz-Bestimmungen, die bei Zahlung mit Kreditkarten gelten. Achten Sie darauf, dass eine verschlüsselte Verbindung (https://..) besteht, wenn Sie die sensiblen Daten eingeben.
16. Lassen Sie sich nicht entmutigen oder von Ihrem Computer nerven.