AUTONOME PROVINZ BOZEN - SÜDTIROL

Generaldirektion
Organisationsamt

PROVINCIA AUTONOMA DI BOLZANO - ALTO ADIGE

Direzione generale
Ufficio Organizzazione

Datenschutzkodex und Schulen staatlicher Art

Abschlussbericht der Arbeitsgruppe

Generaldirektion
Organisationsamt

Autoren
Dr. Cristina Motti
Dr. Armin Haller
Dr. Andrea Bonani
Dr. Simonetta Maina

Projektkoordinierung: Christian Zelger

Redaktion der deutschen Fassung (Kapitel 1, 2, 5, 6 und Vorlagen)
Dr. Aron Mairhofer

Stand: Oktober 2013

Landhaus 1, Silvius-Magnago-Platz 1 • 39100 Bozen
Tel. 0471 41 49 50 • Fax 0471 41 49 69
http://www.provinz.bz.it/zentrale-dienste
organisation.organizzazione@pec.prov.bz.it
organisation@provinz.bz.it
Steuernr./Mwst.Nr. 00390090215

Palazzo 1, Piazza Silvius Magnago 1 • 39100 Bolzano
Tel. 0471 41 49 50 • Fax 0471 41 49 69
http://www.provincia.bz.it/servizi-centrali
organisation.organizzazione@pec.prov.bz.it
organizzazione@provincia.bz.it
Codice fiscale/Partita Iva 00390090215

Inhalt

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

Vorwort

Der vorliegende Leitfaden wurde erarbeitet aufgrund einer Anfrage des Verbandes der autonomen Schulen Südtirols (in Folge ASSA), die Aufgaben, Pflichten und Zuständigkeiten der einzelnen Personen, die im schulischen Bereich mit persönlichen Daten zu tun haben, zu klären. Die Anfrage des ASSA liegt dem Leitfaden bei.

Nach einem ersten Treffen von Vertretern des ASSA, der Informationstechnik und der Generaldirektion wurde die aktuelle Situation analysiert und anschließend der Beschluss gefasst, eine Arbeitsgruppe einzurichten, um eine angemessene Antwort auf die aufgeworfenen Fragen auszuarbeiten.

Mitglieder der Arbeitsgruppe:
Dr. Andrea Bonani (Lehrperson IC Europa 1, didaktisches Netz), Dr. Armin Haller (Abteilung Informationstechnik, didaktisches Netz), Dr. Christoph Kofler (ASSA), Frau Dr. Simonetta Maina (Abteilung Informationstechnik, Beauftragte für die informationstechnische Sicherheit), Frau Dr. Cristina Motti (Organisationsamt, Beauftragte für den Datenschutz), Johann Parigger (Deutsches Schulamt), Dr. Mauro Valer (ASSA).
Die Arbeitsgruppe hat ihre Tätigkeit am 9. Januar 2013 aufgenommen und diese mit 5. Juni 2013 abgeschlossen. Koordinator der Gruppe war Christian Zelger vom Organisationsamt.

Sich mit dem Thema „Privacy" auseinanderzusetzen bedeutet, sich über eine Fülle von informationstechnischen und juristischen Regelungen bis hin zu Fragen der Personalführung an die Thematik heranzutasten.

Aus diesem Blickwinkel betrachtet möchte das vorliegende Werk einen Akzent setzen auf die technisch-organisatorischen Maßnahmen, welche der Gesetzgeber zum Schutze der Daten vorsieht (Legislativdekret vom 30.6.2003, Nr. 196), um die Angleichung der Organisation der staatlichen schulischen Einrichtungen an die geltenden Normen zu gewährleisten.
Es wird eine Verwaltung der Datenschutzobliegenheiten aufgebaut, die nur dann effektive Wirksamkeit erreicht, wenn sie integrierender Bestandteil der Verwaltungsabläufe ist und eine dynamische Verwaltung der Tätigkeiten ermöglicht.

Die Analyse fokussiert drei Themenbereiche:

1) Definition der Rollen, Aufgaben und Verantwortlichkeiten von Rechtsinhabern, Verantwortlichen und Beauftragten für Datenverarbeitung im schulischen Bereich.

2) Die Vorbereitung von Werkzeugen zur Umsetzung der Aufgaben (Vordrucke für die Ernennung von Verantwortlichen und Beauftragten für die Bearbeitung, sowie des Systemadministrators, Checklist für die Schulleitung);

3) Die Ausarbeitung von Vorschlägen für die Realisierung eines Handbuches zur Verwaltung persönlicher Daten im didaktischen Schulverband.

Ein solcher Ansatz kann nicht getrennt werden von einer Analyse der wichtigsten Informationssysteme, die im Einsatz sind, einschließlich der Art der darin gespeicherten persönlichen Daten und die Personen, die in verschiedenen Rollen auf sie zugreifen.

Dies gilt insbesondere für schulische Einrichtungen, welche Dienste outsourcen, die von öffentlichen Betrieben (Autonome Provinz Bozen) und Privaten (Firmen) geleistet werden und folglich für die Handlungen, mit welchen die Rechtsinhaber der Datenverarbeitung jene als Verantwortliche für die Datenverarbeitung und die Maßnahmen festlegen, wie die Daten im Rahmen des Zuständigkeitsbereiches des Beauftragten rechtmäßig bearbeitet werden können.

Der Schlüsselfigur des Systemadministrators wurde eine wichtige Rolle zugewiesen; er kann sowohl an der eigenen Schule seine Rolle wahrnehmen, aber auch in anderen Institutionen, deren Aktivitäten im Bereich Datenverarbeitung mittels Computer detailliert definiert sein müssen mit den entsprechenden Ernennungen.

Der Nutzer dieser Anleitung hat die Aufgabe, die einzelnen Abschnitte dafür zu nutzen, einen Überblick zu bekommen, was das Thema „Regelung der Privacy" angeht, und die Herausforderung anzunehmen, die geltenden Regelungen und das vorgeschlagene Modell in „gelebtes Recht" umzusetzen durch Normen und Verhaltenskodices in der täglichen Schulrealität.

1. Klärung der Rollen, Kompetenzen und Verpflichtungen (Maßnahmen)

Die Schlüsselfiguren in der Verarbeitung von persönlichen Daten – Rollen, Aufgaben und Verantwortung

Rechtsinhaber der Datenverarbeitung – Art. 28 Legislativdekret 196/2003

Rechtsinhaber der Datenverarbeitung ist die **schulische Einrichtung**.
In der Mitteilung, welche den Interessierten gemäß Art. 13 des Kodex ausgehändigt werden muss, ist der Rechtsinhaber demnach die Institution als Ganzes[1]. Selbstredend wird stellvertretend für die Institution der Leiter/Direktor fungieren, welcher diese repräsentiert und für sie gemäß den internen Regelungen der einzelnen Institution die Entscheidungen trifft. Er ist verantwortlich für strategische Entscheidungen und interne Vorgangsweisen (er verfügt über autonome Befugnisse betreffend die Modalitäten für die Verarbeitung von Daten, die elektronischen Instrumente und die zum Zwecke der Sicherheit eingesetzten Mittel).
Der Rechtsinhaber der Datenverarbeitung ist verpflichtet, die Arbeit des Verantwortlichen für die Datenverarbeitung, den er selbst ernannt hat, zu überwachen und zu kontrollieren, und ist für die illegale Verarbeitung von Daten verantwortlich (*„per culpa in eligendo e vigilando*").
Bei der Ernennung des Verantwortlichen für die Datenverarbeitung ist es notwendig, explizit die Kontroll- und Überwachungskompetenzen der Institutsleitung vorzusehen: Anforderung von regelmäßigen Reports und die Möglichkeit der Durchführung von Inspektionen. Im Sinne von Art. 31 des Kodex zum Schutz persönlicher Daten ist der Rechtsinhaber verpflichtet, geeignete Sicherheitsmaßnahmen und Vorkehrungen zur Überwachung der Daten vorzusehen (siehe auch Abschnitt „Sicherheitsmaßnahmen[2]"). Deren Fehlen oder nicht ausreichende Prädisposition kann sowohl zivil- als auch strafrechtliche Konsequenzen nach sich ziehen (Art. 15 und 169 des Kodex).

[1] Siehe Pressemitteilung der Datenschutzbehörde, 11.12.1997, Bollettino, 1997.

"Quando la raccolta, l'elaborazione, l'utilizzazione, la conservazione e in genere tutte le operazioni relative al trattamento dei dati vengono effettuate nell'ambito di un'amministrazione pubblica, di una società o di un ente, il titolare del trattamento è la struttura nel suo complesso e cioè il soggetto al quale competono le scelte di fondo sulla raccolta e sull'utilizzazione dei dati. Non devono, quindi, essere considerati come "titolari" le singole persone fisiche che l'amministrano o che la rappresentano, quali ad esempio il ministro, l'amministratore delegato, il direttore generale, il presidente, il legale rappresentante.

Il Garante ha chiarito, peraltro, che se i "titolari" sono le imprese e le amministrazioni pubbliche, per esse opereranno, nelle diverse scelte che sia necessario assumere, i rispettivi amministratori, secondo le regole che disciplinano ciascuna struttura: di volta in volta, il ministro, l'amministratore delegato, il consiglio di amministrazione, i direttori generali e gli altri dirigenti. Ad esempio, la notificazione al Garante, se dovuta, dvrà essere sottoscritta dalla persona fisica che ha il potere di rappresentarla."

[2] Verarbeitete oder zu verarbeitende personenbezogene Daten müssen je nach Art und nach Verarbeitungsmethode so aufbewahrt und überwacht werden, dass durch geeignete vorsorgliche Schutzmaßnahmen die Gefahr einer Vernichtung oder eines Verlusts, auch wenn dies durch Zufall geschieht, eines unbefugten Zugriffs oder der unbefugten oder nicht dem Beschaffungszweck entsprechenden Verarbeitung auf ein Minimum reduziert wird.

Der Verantwortliche für die Verarbeitung der Daten
Art. 29[3]

Der Verantwortliche für die Verwaltung in der Einrichtung (Schulen staatlicher Art) ist in der Regel auch **verantwortlich für** die Datenverarbeitung. Er wird eingesetzt durch den Leiter/Direktor durch eine Ernennung (siehe beiliegendes Ernennungsschreiben in Anlage 1), wo schriftlich und in ausführlicher analytischer Form die zugewiesenen Aufgaben und die damit verbundenen Verantwortungen beschrieben sind.

Einige der Aufgaben sind:
- Ernennung der Beauftragten (mit entsprechendem Schreiben und Aufgabenbeschreibung)
- Instruktionen und Kontrolle derselben
- Rückmeldungen an die Interessierten im Falle von Rechtsansprüchen durch Betroffene
- Auflistung der durchgeführten Datenverarbeitungen im jeweiligen Kompetenzbereich
- Pflege der Umsetzung der Sicherheitsmaßnahmen

Er ist nicht nur zuständig für die Umsetzung der Maßnahmen, sondern arbeitet Hand in Hand als Berater des Rechtsinhabers, was die Wahl der Maßnahmen für die Durchführung der Datenverarbeitung angeht. Dies bedeutet, dass in der Regel auch er, so wie der Rechtsinhaber, zivil-, straf- und verwaltungsrechtlich haftbar gemacht werden kann, wenn die geltenden gesetzlichen Bestimmungen verletzt werden.

Der Verantwortliche für die Datenverarbeitung wird ausgewählt vom Rechtsinhaber aufgrund seiner Fähigkeiten, Erfahrungen und seiner Vertrauenswürdigkeit.

Wenn der Rechtsinhaber mehrere Verantwortliche ernennt, arbeiten diese grundsätzlich gleichberechtigt auf derselben Kompetenz-Ebene.

Der Verantwortliche für die Datenverarbeitung ist eine fakultative Figur. Wann immer dieser Figur an einer Schule nicht ernannt worden ist, ist automatisch der Schulleiter (Direktor) verantwortlich für die Ernennung der Beauftragten.

[3] Der Rechtsinhaber (welcher dafür sorgen muss, dass seine technische und organisatorische Struktur dem Kodex angepasst wird) stellt dem Verantwortlichen für die Verarbeitung der Daten – wenn es einen gibt – eine Vollmacht aus. Die Ernennung schränkt eigentlich nur die Befugnisse ein und definiert die einzelnen Aufgaben des Verantwortlichen.
Diese Vollmacht befreit den Rechtsinhaber nicht von der Pflicht, die vom Gesetz vorgeschriebenen Sicherheitsmaßnahmen, welche auf den technischen Vorschriften der Anlage B basieren, umzusetzen, und ebenso nicht von der Verpflichtung, die Akteure der Datenverarbeitung zu ernennen und den Verpflichtungen gegenüber der Datenschutzbehörde nachzukommen (Meldung der Datenverarbeitung).

Der Beauftragte für die Verarbeitung der Daten[4]
Art. 30

Es ist immer eine physische Person, welche im Auftrag des Inhabers oder des Verantwortlichen die Umsetzung der Aufgaben in Hinblick auf die Datenverarbeitung übernimmt. Beauftragte sind im schulischen Bereich die Verwaltungsangestellten (in der Regel Sekretariatsbedienstete, aber auch Hilfspersonal) und Dozenten.

Er wird durch eine schriftliche Beauftragung eingesetzt, wo schriftlich und in ausführlicher analytischer Form die zugewiesenen Aufgaben und die damit verbundenen Verantwortungen beschrieben sind („Was darf er tun?", „Wie muss er es tun?"). Als Ernennung gilt auch die schriftlich belegte Bestellung einer natürlichen Person zum Leiter einer Einheit, für deren Mitarbeiter der Verarbeitungsbereich bereits schriftlich festgelegt ist (siehe auch beiliegendes Schreiben und ausgewählte Richtlinien für Sekretariatsmitarbeiter und Hilfspersonal – Anlagen Nr. 2, 2a und 2b).

Der Verwaltungsleiter gemäß Landesgesetz 12/2000 ernennt, sobald er als Verantwortlicher für die Datenverarbeitung im Sinne von Art. 29 des Datenschutzkodexes eingesetzt wurde, mit entsprechendem Ernennungsakt das Verwaltungspersonal, welches mit der Verarbeitung der Daten betraut wird und somit die Verwaltungsaufgaben durchführt.

Die Dozenten hingegen werden vom Schulleiter als Datenbeauftragte ernannt, und zwar mit einem entsprechenden Ernennungsakt (Anlagen Nr. 3, 3a).

Verpflichtungen:
Im Falle der Auslagerung von Diensten lehnen sich die staatlichen Schulen an die Autonome Provinz Bozen an: an die Abteilung 9. Informationstechnik für die Verwaltung von IT-Systemen (Netze und Server) und Datenbanken (Popcorn, OBU). In diesem Falle müssen die Schulen (soweit sie Auftraggeber und Rechtsinhaber der Datenverarbeitung sind) die Ernennung der Autonomen Provinz Bozen (Outsourcer) vornehmen, und zwar mit entsprechendem Schreiben, in welchem festgehalten ist, dass diese als **externer Verantwortlicher für die Datenverarbeitung** beauftragt wird; im Schreiben müssen alle Anforderungen detailliert beschrieben werden.

Die Ernennung erfolgt aufgrund eines Outsourcing-Vertrages[5] oder der Durchführung von Diensten zwischen der Autonomen Provinz Bozen (im

[4] Der Verantwortliche stellt dem Beauftragtem eine **Vollmacht für die Durchführung der Aufgaben aus.**
[5] **Outsourcing-Vertrag**
Vermischung von Elementen der Ausschreibung von Dienstleistungen (Art. 1677 ff.) und Lieferverträgen. Vorrang haben die Ausschreibungen von Dienstleistungen, sofern es sich um die Leistung von echten Diensten handelt (Wartung, Assistance, Kommunikation mit den Nutzern, Call Center).
Verpflichtung zur Leistung: Der Dienstleister, welcher die Leistung erbringt (Outsourcer) verarbeitet in der Regel auch personenbezogene Daten, Rechtsinhaber der Daten bleibt immer der Auftraggeber (Outsourcee).

Folgetext kurz APB), Abteilung 9. Informationstechnik und einzelnen Schulen, wobei die Konditionen der Dienstleistung (Rechte, Pflichten und Verantwortungen) im Vertrag festgeschrieben sind.

Alle Systembetreuer der Abteilung Informationstechnik werden vom Abteilungsdirektor mit einem entsprechenden Akt als **Systemadministratoren ernannt** und sind dadurch **Beauftragte für die Datenverarbeitung** (Beschreibung Systemadministrator siehe entsprechenden Abschnitt).

Wenn sich die Abt. 9 der Zusammenarbeit mit anderen Firmen bedient (Privatunternehmen, SIAG, usw.) und diesen einen Teil der informationstechnischen Arbeiten übergibt, werden diese Formen der Zusammenarbeit formell definiert durch entsprechende **Dienstleistungsverträge**, welche ausgehandelt werden zwischen APB (Abteilung 9. Informationstechnik) und den einzelnen Unternehmen.

Zusammenfassend sehen die **Pflichten der Schulen** aus wie folgt:

1. Abschluss eines **Outsourcing-Vertrages** (bzw. eines **Dienstleistungs-Abkommens**) mit der APB (Abteilung 9. Informationstechnik).
2. **Ernennung** der APB zum **externen Verantwortlichen** für die **Datenverarbeitung** (bei Bedarf auch durch eine entsprechende Klausel im Vertrag (siehe Punkt 1). Eine Vorlage finden Sie als Anlage 4.
3. Die Instruktionen und Aufgaben, welche der APB übertragen werden, können auch nachträglich mittels verschiedener Akte definiert werden.

Gleichzeitig muss die **Abteilung 9. Informationstechnik**:

1. **Verträge mit den Firmen** abschließen, welche Dienstleistungen an die Schulen liefern (Wartung, Assistance, Call Center).
2. Die **Voraussetzungen** schaffen, dass die Schulen externe Firmen (oder SIAG) als externe Verantwortliche für die Datenverarbeitung ernennen können (Anlage 6).
3. **Ernennung der Mitarbeiter als Beauftragte für die Datenverarbeitung[6] bzw. als Systemadministratoren**; die Listen derselben und die Aufgabenbeschreibungen müssen an die Schulen weitergegeben werden.

Somit muss der Outsourcer als Verantwortlicher für die Datenverarbeitung ernannt werden (im Sinne des Art. 29 des Kodex) und er muss vom Rechtsinhaber die Vorgaben erhalten, nach welchen er sich zu verhalten hat; dies muss zudem vom Rechtsinhaber periodisch kontrolliert werden.
Der Datenaustausch zwischen Rechtsinhaber und Verantwortlichem wird vom Kodex nicht als Datenmitteilung berücksichtigt.

[6] Laut Kodex darf es sich nur um physische Personen handeln.

Im Handbuch „Privacy und Datenschutz" von Giusella Finocchiaro stellt die Autorin fest, dass der Rechtsinhaber der Datenverarbeitung die Ernennung der Unternehmen, an welche der Outsourcer Dienste ausgelagert hat, zu externen Datenverantwortlichen vornehmen muss; diese wiederum müssen ihre Mitarbeiter selbst zu Datenbeauftragten ernennen.

Der Rechtsanwalt Giovanni Guerra bestätigt dies in seiner Abhandlung „Privacy Compliance, novità, adempimenti, sanzioni, ispezioni", November 2011) auf S. 447: "il responsabile esterno del trattamento non può a sua volta designare un sub-fornitore responsabile per le operazioni di trattamento che gli demanda, ma dovrebbe più correttamente promuoverne la nomina da parte del titolare".
Dazu existiert auch eine Anfrage an das Büro für Beziehungen mit der Bevölkerung der Datenschutzbehörde in Rom (URP), welche diese Regelung sowohl schriftlich als auch mündlich am 21.02.2013 bestätigt hat.
(Auf der Website der Datenschutzbehörde finden sich zahlreiche Stellungnahmen zum Thema Outsourcing (Verwaltungsmaßnahmen vom 12.5.2011 und vom 15.6.2011).

Der Systemadministrator gemäß Datenschutzkodex

Grundlage für diese Figur ist eine Maßnahme der Datenschutzbehörde vom 27.11.2008 (abgeändert mit Maßnahme vom 25.6.2009) Doc web. Nr. 1577499: "Misure e accorgimenti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

Der Systemadministrator (hinkünftig kurz SA) hat eine äußerst verantwortungsvolle und sensible Rolle inne, da die Durchführung seiner Tätigkeiten, wenn er Verantwortlicher oder Beauftragter ernannt worden ist, mit sich bringt, dass er jederzeit kompletten Zugriff auf Informationssysteme und persönliche Daten hat, welche er nur und ausschließlich in seiner zugewiesenen Funktion und im Rahmen der ihm zugewiesenen Kompetenzen verarbeiten darf; entsprechend ist es notwendig, diese seine Tätigkeit(en) zu kontrollieren und zu überwachen.

Die Administratoren sorgen dafür, dass die Informationssysteme automatisch durch entsprechende Programme oder Geräte gewartet und verwaltet werden. Administratoren können sein: Datenbank-Administratoren, Netzwerk- und IT-Administratoren, Sicherheitsanlagen-Administratoren und Administratoren komplexer Softwaresysteme.

Auch wenn nicht vorgesehen ist, dass sie die Hintergrundinformationen verstehen (Bedeutung der Daten, Semantik der Funktionen und Format der Darstellungen), sind die Systemadministratoren konkret verantwortlich für die spezifischen Arbeitsabläufe, welche kritisch für den Schutz der Daten sein können.

Aktivitäten wie:

- **Datenspeicherung** (backup/recovery)
- **Organisation der Netzwerkflüsse**
- Verwaltung der **Datenspeicher**
- **Wartung Hardware**

sind einer Datenverarbeitung äquivalent. Umso mehr, wenn die Verwaltung die verschiedenen Informationen unverschlüsselt verwendet.
Im aktuellen Kodex ist die Figur des Systemadministrators nicht vorgesehen. Trotzdem werden die Aufgaben desselben größtenteils in der Anlage B des Kodexes beschrieben, vor allem in jenem Teil, wo festgestellt wird, dass die Schulen (Rechtsinhaber) verpflichtet sind, die Verwahrung zu gewährleisten, sowie die Verwaltung der eigenen Mittel für die Authentifizierung.

Aufgaben, vorgesehen in Anlage B, Besonderheiten des SA:

- **Realisierung Sicherheitskopien (backup/recovery)**
- **eventuelle Verwahrung der Mittel für die Authentifizierung**
- **Verwaltung der Authentifizierungs- und Bewilligungssysteme**

Pflichten des Rechtsinhabers

1. Bewertung der Eigenschaften

Die Identität der SA muss dokumentiert sein,
Zu bewertende Eigenschaften für die Ernennung durch den Rechtsinhaber:
1. Vertrauenswürdigkeit, 2. Fähigkeiten, 3. Erfahrung (siehe Art. 29 des Kodex bezüglich der vorgesehenen Eigenschaften für den Verantwortlichen für die Datenverarbeitung).

2. Individuelle Ernennungen

Wenn jemand als Beauftragter ernannt worden ist, muss er in jedem Falle die Voraussetzungen gemäß Art. 29 erfüllen.
Die Ernennung des SA muss individuell erfolgen und eine schriftliche analytische Auflistung der Aufgabenbereiche, geordnet nach Sektoren und Anwendungsbereichen enthalten, welche den zugewiesenen Benutzerberechtigungen entsprechen.

3. Liste der Systemadministratoren SA

Die persönlichen Daten der physischen Personen, welche als Systemadministratoren fungieren (Name und Nachname, Funktion, Arbeitsumfeld), mit der Auflistung der zugewiesenen Aufgabenbereiche müssen in einem internen Dokument festgehalten werden, dieses muss ständig aktualisiert werden und bei Bedarf von der Datenschutzbehörde eingesehen werden können.
Im Falle, dass die Aufgabe des Systemadministrators outgesourct wurde, müssen der Rechtsinhaber oder der Verantwortliche für die Datenverarbeitung die Liste mit den persönlichen Daten der SA aufbewahrt werden, die aktualisierte Version muss regelmäßig vom Outsourcer geliefert werden.

4. Überprüfung der Tätigkeiten

Der Rechtsinhaber oder der Verantwortliche muss mindestens einmal jährlich die Arbeit des AS kontrollieren (ausgeführte Arbeiten gemäß zugewiesenen Zuständigkeiten).

5. Protokollierung der Zugänge

Jeder Log-In (Zugang) eines AS muss protokolliert werden. Die Protokollierung der Zugänge (*access-log, log-in, log-out,* Zugangs-Fehler und alle Vorgänge, welche der SA durchgeführt hat und die sich auf seinen Username beziehen, mit Datum und Zeit), müssen vollständig, unveränderbar und verifizierbar sein; es muss also ersichtlich sein: wann hatte der SA Zugang? Beschreibung des durchgeführten Vorganges, ob es sich um einen *log-in*, einen l*og-out*, einen Zugangsfehler o.Ä. handelt, und welches Netz bzw. welcher Terminal verwendet wurde). Alle Protokollierungen müssen mindestens sechs Monate lang aufbewahrt werden.
Reine Anwenderzugänge müssen nicht protokolliert werden.

Mindestsicherheitsmaßnahmen

Art. 33 Datenschutzkodex[7]

Der Kodex verlangt die Veranlagung von ausgewählten Sicherheitsmaßnahmen, je nachdem, inwieweit die Datenverarbeitung mittels elektronischer Instrumente (IT) erfolgt.

Die Verarbeitung von personenbezogenen Daten **ohne den Einsatz von IT (Art. 35)** ist nur zugelassen, wenn folgende Mindestsicherheitsmaßnahmen erfüllt werden:

- Periodische Aktualisierung (mindestens einmal jährlich) der Festlegung des Verarbeitungsbereiches für die einzelnen Beauftragten und für die mit der Verwaltung oder Instandhaltung der elektronischen Mittel betrauten Personen; die Liste der Beauftragten kann auch nach homogenen Aufgabenbereichen und entsprechenden persönlichen Benutzungsberechtigungen erstellt werden;

- Vorsehen von Abläufen für eine angemessene Verwahrung von Akten und Dokumenten, die dem Beauftragten für die Durchführung diverser Aufgaben anvertraut worden sind; Übermittlung von schriftlichen Anweisungen für die Beauftragten, welche die notwendige Kontrolle und die Verwahrung definieren, und zwar für den gesamten Ablauf der Verarbeitung von Akten und Dokumenten, welche personenbezogene Daten enthalten;

- Vorsehen von Abläufen für die Konservierung bestimmter Akten in Archiven, zu denen nur ausgewählte Berechtigte Zugang haben und welche durch Zugangssysteme gesichert sind, welche eine eindeutige Identifizierung jedes einzelnen Zugangs ermöglichen, wenn es Situationen gibt, wo Personen, die außerhalb der Öffnungszeit, egal in wessen Auftrag einsteigen und nicht identifiziert und registriert werden, wenn die Archive nicht mit elektronischen Zugangssystemen oder Überwachungspersonal zur Kontrolle ausgestattet sind, und alle Zugangsberechtigten müssen vorab autorisiert sein.

[7] Dies sind die organisatorischen, physischen logischen und informationstechnischen Maßnahmen, welche die Grundlage für die minimalen Sicherheitsanforderungen zum Schutze der personenbezogenen Daten in schulischen Einrichtungen. Diese Maßnahmen werden teilweise auch in die Nominierungsakten eingefügt, welche die Personen betreffen, die befugt sind Daten zu verarbeiten, die in engem Zusammenhang mit den zugewiesenen Aufgaben stehen.

Die vorgesehenen Mindestsicherheitsmaßnahmen für die Datenverarbeitung mittels IT

Art. 34

Authentifizierung

In erster Linie muss für **die mit der Verarbeitung Beauftragten** eine elektronische Authentifizierung zur Verfügung gestellt werden; die Beauftragten müssen über einen Identifizierungscode verfügen (verbunden mit einem persönlichen Passwort), bzw. über ein eigenes Gerät, das zur Authentifizierung dient (eventuell mit Identifikations-Code oder Passwort).

Alternativ kann die Authentifizierung des Beauftragten durch die Verwendung von biometrischen Merkmalen (eventuell mit Identifikations-Code oder Passwort) erfolgen. Wo ein Identifizierungs-Code verwendet wird darf dieser nicht an andere Beauftragte weitergegeben werden, auch nicht für die Verwendung zu verschiedenen Zeiten.
Das Passwort muss, soweit es von der Authentifizierungsmethode vorgesehen ist, aus mindestens acht Zeichen bestehen, oder, wenn dies nicht möglich ist, aus der maximal möglichen Anzahl von Zeichen; es darf keine Rückschlüsse auf den Benutzer zulassen und wird beim ersten Gebrauch vom Nutzer personalisiert, in Folge mindestens alle sechs Monate.

Die Abläufe für die Verwaltung der Mittel zur Authentifizierung sind anzuwenden! Diese müssen deaktiviert werden, außer sie wurden vorab nur für die technische Verwaltung autorisiert, wenn sie für mindestens sechs Monate nicht eingesetzt worden sind oder wenn der Beauftragte die Voraussetzungen für den Zugang zu den Daten verliert. Zu den zugewiesenen Anweisungen für die Beauftragten gehören auch die Vorkehrungen, um die Geheimhaltung des persönlichen Teils des Identifikationsmittels und die sorgfältige Verwahrung der Vorrichtungen, in deren Besitz sie sind und die nur sie verwenden dürfen, zu gewährleisten.

Schließlich müssen geeignete und präventive schriftliche Anweisungen gegeben werden, welche die Modalitäten definieren, nach welchen der Rechtsinhaber garantieren kann, dass die Daten und die IT-Systeme auch im Falle einer längeren Abwesenheit oder einer Verhinderung des Beauftragten zur Verfügung stehen, wenn es unerlässlich und unaufschiebbare Notwendigkeit gibt, auf die Daten zuzugreifen.

Besondere Vorsicht gilt für die Verarbeitung von sensiblen Daten (das Passwort muss mindestens alle drei Monate geändert werden); hier müssen Chiffrierprogramme zum Einsatz kommen, Identifikationscodes oder andere Lösungen, welche die Daten zeitweilig unlesbar machen, auch für Berechtigte, und die zulassen, dass die Betroffenen nur im Bedarfsfalle identifiziert werden.
Bei der periodischen, mindestens jährlichen Aktualisierung der Festlegung des Verarbeitungsbereichs für die einzelnen Beauftragten und für die mit der Verwaltung oder Instandhaltung der elektronischen Mittel betrauten Personen

kann die Liste der Beauftragten auch nach homogenen Aufgabenbereichen und entsprechenden persönlichen Benutzungsberechtigungen erstellt werden.

Bewilligungen

Während die Zugangsberechtigung das Ziel hat, die Identität aller Personen zu verifizieren, die sich Zugang zum PC oder zum Netz zu verschaffen, ermöglicht die Authentifizierung dem Nutzer (bereits authentifiziert) die Bearbeitung all jener Daten, zu denen er aufgrund seiner zugewiesenen Benutzungsberechtigung Zugang hat. Die Benutzungsberechtigungen sind individuell und vor der Datenverarbeitung zu generieren, damit der Zugang auf all jene Daten beschränkt wird, welche der Nutzer gemäß seinem Profil bearbeiten darf. Mindestens einmal jährlich muss die Aktualität der Berechtigungen überprüft werden.

Speicherung und Sicherheitsmechanismen

Es ist sehr wichtig, den Schutz der Daten vor unrechtmäßigen bzw. unerlaubten Zugriffen und vor Viren zu schützen (gegen diese gibt es wirkungsvolle elektronische Instrumente, die mindestens alle sechs Monate zu aktualisieren sind). Zu diesem Zwecke müssen den Beauftragten entsprechende Instruktionen gegeben werden, damit die Computer nicht unbeaufsichtigt und frei zugänglich sind, wenn sie Daten verarbeiten, während der Bearbeiter sie geöffnet hat und beim Gebrauch von portablen Datenspeichern, auf welchen diese gesichert wurden.
Letztere müssen, wenn sie der Verarbeitung von sensiblen Daten dienen, bei Nichtgebrauch vernichtet oder unbrauchbar gemacht werden (zum Beispiel durch Software, die alle Daten sicher überschreibt). Diese Datenträger können aber auch von Nutzern, die nicht für den Gebrauch der sensiblen Daten autorisiert sind, benutzt werden, wenn die vorher auf dem Datenträger gespeicherten Daten nicht mehr lesbar sind und technisch nicht wiederhergestellt werden können.

Es muss schriftlich festgelegt werden, mittels welcher Abläufe Sicherheitskopien angefertigt werden können, aber auch, wie Daten und Systeme wiederhergestellt werden können. In jedem Falle müssen organisatorische und technische Instruktionen ausgearbeitet werden, welche die Speicherung der Daten mindestens einmal wöchentlich vorsehen.
Um dem Risiko einer Beschädigung der Daten vorzubeugen, ist angeraten, die Datenträger, auf welchen die Daten regelmäßig gesichert werden, regelmäßig zu erneuern; sie müssen sorgfältig aufbewahrt werden und es wäre wichtig, Kopien anzufertigen, die eine langfristige Sicherung an einem anderen Ort ermöglichen.

Wann immer die Mindestsicherheitsmaßnahmen darin bestehen, dass man sich der Zusammenarbeit mit einem externen Unternehmen bedient, muss der Rechtsinhaber von jener Person, welche die Programme installiert, eine schriftliche Beschreibung des erfolgten Eingriffes erhalten, aus der hervorgeht, dass die geltenden gesetzlichen Bestimmungen eingehalten worden sind.

Verwaltungsrechtliche Verantwortung

Art. 161-166 ff. Datenschutzkodex

Was das Verhalten der schulischen Einrichtungen angeht, sind die gravierendsten Verletzungen bei verwaltungsrechtlichen Handlungen die komplette oder teilweise Missachtung der Mitteilungspflichten gegenüber dem Betroffenen zu Beginn der Datenverarbeitung und die unrechtmäßige Weitervergabe der zu bearbeitenden Daten an Dritte. Ein weiterer relevanter Verstoß wäre die fehlende Zusammenarbeit mit der Datenschutzbehörde.

Im Detail:

1. Fehlende oder unzureichende Mitteilung im Sinne des Art. 13 an den Betroffenen: Verwaltungsstrafen von **6.000,00 bis 36.000,00** Euro.
2. Weitergabe der Daten an Dritte; Verstoß gegen Art. 16, Absatz 1, Buchstabe b oder Verstoß gegen andere Bestimmungen des Kodex: Verwaltungsstrafen von **10.000,00 bis 60.000,00** Euro.
3. Im Falle der Verletzung der Mindestsicherheitsmaßnahmen gemäß Art. 33 oder der Bestimmungen gemäß Art. 167: Verwaltungsstrafen von **10.000,00 bis 120.000,00** Euro.
4. Nichteinhaltung der Vorschriften bzw. Nichtbeachtung der notwendigen Maßnahmen und der von der Datenschutzbehörde ausgesprochenen Verbote (Art. 154, Absatz 1, Buchstaben c) und d) des Kodex): Verwaltungsstrafen von **30.000,00 bis 180.000,00** Euro.
5. Fehlende Meldung an die Datenschutzbehörde gemäß Art. 37 des Kodex: Verwaltungsstrafen von **20.000,00 bist 120.000,00** Euro.

Kontrollen, welche Sanktionen zur Folge haben können, werden vorrangig durch die Datenschutzbehörde oder durch die Finanzpolizei durchgeführt. Die Kontrollen werden vor Ort ausgeführt, wobei alle vorhandenen Unterlagen überprüft werden können (ausgehend vom Zeitpunkt der Kontrolle können alle Sicherheitspläne der vorangehenden fünf Jahre verlangt werden). Überprüft werden kann ebenso die Konformität der Unterlagen zu den Sicherheitsplänen.

Die Ausarbeitung eines <u>schriftlichen</u> Sicherheitsplanes ist nicht mehr obligatorisch, wird aber von der Datenschutzbehörde dringend empfohlen!

Strafrechtliche Verantwortung

Art. 167-172 ff. Datenschutzkodex

Strafrechtlich verantwortlich ist in der Regel der Rechtsinhaber der Datenverarbeitung, eventuell auch der Verantwortliche und der Beauftragte (Art. 167-172 ff Datenschutzkodex) in folgenden Fällen:

Wenn die Prinzipien, welche für die Verarbeitung von Daten angewandt werden müssen, verletzt werden: **Haftstrafe 6-8 Monate**, kann erhöht werden auf **6-24 Monate** im Falle der Weitergabe oder Veröffentlichung von personenbezogenen Daten.

Im Falle einer unrechtmäßigen Verarbeitung von sensiblen oder gerichtlichen Daten sind **Haftstrafen von 1-3 Jahren** vorgesehen.
Bevor eine Sanktion tatsächlich angewandt wird, müssen zwei wichtige Faktoren zusammentreffen: dem Täter muss die Absicht nachgewiesen werden, dass er für sich oder andere einen Vorteil zum Nachteil Dritter daraus ziehen wollte und dass durch sein Gebaren ein tatsächlicher Schaden verursacht wurde (*dolo specifico*).
Wenn das Vergehen schwerwiegender ist als jenes, für welches die Sanktion im Kodex vorgesehen ist, wird jeweils die Höchststrafe ausgestellt, vorbehaltlich der Möglichkeit, dass eine andere Gerichtsbehörde eine höhere Strafe vorsieht (z.B. strafrechtliche Folgen).

Mindestens eine Haftstrafe ist auch dann vorgesehen, wenn falsche Angaben an die Datenschutzbehörde gemacht oder Dokumente für diese gefälscht werden.
Ebenso bestraft wird der, der die Anordnung der Datenschutzbehörde missachtet, welche in vorsorgender Absicht die zeitweilige Einstellung der Verarbeitung der Daten oder die Unterbrechung einzelner Datenverarbeitungsschritte vorsieht, weil die Behörde festgestellt hat, dass die Verarbeitung selbst nicht rechtmäßig ist und daher einzustellen ist (siehe auch Punkt 4).

Zudem sind auch Geld- und Haftstrafen (bis zu 2 Jahren) vorgesehen, wenn der Rechtsinhaber, welcher dazu verpflichtet wäre, die Mindestsicherheitsmaßnahmen nicht anwendet (siehe auch Art. 162 und 169 des Datenschutzgesetzes).
In diesem Falle hat die Datenschutzbehörde die Befugnis, Vorschriften zu erlassen, um eine Richtigstellung der Tätigkeiten zu ermöglichen, wobei eine Frist von maximal sechs Monaten festzulegen ist (verlängerbar nur in begründeten komplexen Ausnahmefällen). Wenn der Täter die Beanstandungen der Datenschutzbehörde in Ordnung bringt, wird die Strafe in eine Geldstrafe umgewandelt (siehe auch Punkt 3).

Zivilrechtliche Verantwortung
Art. 15 Datenschutzkodex

1. Wer einen Schaden gegenüber Dritten durch die Verarbeitung von Daten verursacht, muss gemäß Art. 2050 des Zivilgesetzbuches Schadenersatz leisten.

2. Ein nicht materieller Schaden muss auch abgegolten werden, wenn die Grundsätze des Art. 11 verletzt worden sind:

Grundsatz der Notwendigkeit der Datenverarbeitung
Die Regelung hat zum Ziel die Sammlung und Verarbeitung von unnötigen Daten zu verhindern. Zu diesem Zwecke sehen die Bestimmungen (Art. 3 des gesetzesvertretenden Dekretes vom 30.6.2003 Nr. 196) vor, dass die IT-Systeme und die Programme so zu konfigurieren sind, dass ein Minimum von personenbezogenen und Identifizierungsdaten verwendet wird, um eine Verarbeitung auszuschließen, wenn die verfolgten Ziele in den einzelnen Fällen genauso mittels anonymer Daten oder durch andere adäquate Verfahren, welche die Identifikation des Betroffenen nur im Bedarfsfalle zulassen, erreicht werden können.
Demzufolge wird eine Regelung zur Einschränkung der Datensammlung eingeführt. Es werden nur notwendige Daten gesammelt, die für das zu erreichende Ziel unabdingbar sind.

Grundsatz der Zielsetzung
Die vorangehende Zielsetzung ist ein Grundsatz, welcher die Sammlung von Daten für den *zielgerichteten* Gebrauch begleiten muss.
In der Praxis bedeutet dies, dass die Schulen verpflichtet sind, wenn sie Daten der Schüler (oder Eltern) sammeln, die Betroffenen (Eltern oder Schüler) über den Zweck der Datensammlung aufzuklären; dieser Zweck muss legitim und eingegrenzt sein. Die Weitergabe der Daten an einen anderen Rechtsinhaber für inkompatible Zwecke – auch im Falle der Einstellung der Datenverarbeitung – ist illegal und der ursprüngliche Rechtsinhaber haftet dafür.

Grundsatz der Selbstbestimmung
Diese Regel bestimmt, dass die Eltern der Schüler grundsätzlich das Recht haben, zu bestimmen, in welchem Rahmen die schulische Institution Daten, die ihre Kinder betreffen, weitergeben darf. Demzufolge hat jeder Elternteil das Recht, festzusetzen, wie und in welchem Ausmaß Informationen, welche ihn selbst und das Kind betreffen, verbreitet und anderen zugänglich gemacht werden dürfen.

Grundsatz der Korrektheit
Der Grundsatz der Korrektheit ist ein Prinzip, das jeden betrifft, der personenbezogene Daten verarbeitet: in diesem Zusammenhang **muss die Schule** die **Rechtmäßigkeit und Korrektheit** der Datenverarbeitung sowohl

während der Sammlung als auch in der tatsächlichen Nutzung der Daten **garantieren**.
Die Verarbeitung ist **rechtmäßig**, wenn sie **gesetzeskonform** geht, sie ist korrekt, wenn die Datensammlung beim Betroffenen transparent erfolgt und nicht durch in betrügerischer Form.

Grundsatz der Vorsicht

Bei der Verwendung von personenbezogenen Daten ist es notwendig, jeder unrechtmäßigen Verwendung vorzubeugen, Nachlässigkeit und Unerfahrenheit entschuldigen kein Verfehlen. Jeder, der personenbezogene Daten verarbeitet muss größte Sorgfalt walten lassen, um zu vermeiden, dass er Daten erhält, deren Ursprung nicht zuverlässig ist oder deren Korrektheit nicht klar erkennbar ist.
Im Einklang mit diesen grundsätzlichen Prinzipien legen die Bestimmungen explizit einige klare Regelungen fest, was die Verarbeitung und die Eigenschaften von Daten angeht.
Dass die bisher behandelten Grundsätze eingehalten werden ist sehr wichtig, weil personenbezogene Daten, welche die wesentlichen Bestimmungen verletzend verarbeitet wurden, nicht verwendet werden dürfen.
Nur die Einhaltung der geltenden Bestimmungen beugt Sanktionen vor, welche die Verarbeitung der Daten blockieren können – **dies würde für eine Schule bedeuten, dass sie keine Schülerdaten mehr verwenden dürfte** -, aber auch der Anwendung von Verwaltungs- und strafrechtlichen Sanktionen (wie oben beschrieben).
Der Artikel 2050 des Zivilgesetzbuches geht von einer erschwerten Verantwortung aus, mit einhergehender Beweislastumkehrung, wenn:
Wenn es sich um eine gefährliche Aktivität handelt ist jener, welcher diese Aktivität ausführt, dafür verantwortlich nachzuweisen, dass er alle Vorkehrungen getroffen hat, um Schaden zu vermeiden. Der Geschädigte muss einen Beweis für seinen Schaden erbringen und dafür, dass ein Zusammenhang zwischen dem Schaden und dem Verhalten des Rechtsinhabers (aktiv oder passiv) besteht. Die Doktrin besagt, dass die Befreiung von der Schuld nur möglich ist, wenn es sich nachweislich um höhere Gewalt handelt.

Redaktion:

Dr.Cristina Motti – Organisationsamt

Szenario A : basierend auf der Analyseder Beziehungen zwischen Schulen und Abteilung Informationstechnik für die Wartung der IT-Systeme im didaktischen Umfeld.

1. Schulen = *Rechtsinhaber* der Datenverarbeitung (auch Auftraggeber)

a. ☐ ***Abschluss*** Outsourcing-Vertrag mit APB (Abt. Informationstechnik)

und

b. ☐ ***Ernennung***

2. APB – Abt. 9 Informationstechnik = *Externer Verantwortlicher für die Datenverarbeitung* (Art. **29** Kodex)

a. ☐ ***Ernennung***

Mitarbeiter der Abt. 9 Informationstechnik = Systemadministratoren und *Beauftragte der Datenverarbeitung* (Art. **30** des Kodex)

Fortsetzung: Outsourcing der Dienste

b. ☐ *Abschluss von Verträgen für die Weitervergabe von Diensten mit*

private Firmen, SIAG, usw.

3. Privatfirmen *Ernennung zu Datenverantwortlichen* (Art. 29) durch die Schule

a. ☐ *Ernennung*

eigene Mitarbeiter SA und Beauftragte für die Datenverarbeitung (Art. 30)

Um die Aufgaben der Überwachung und der Kontrolle, welche der Kodex den Rechtsinhabern der Datenverarbeitung durch Dritte vorschreibt, durchführen zu können, muss den Schulen die Liste der Namen der Beauftragten zugestellt werden. So ist es den Schulen möglich, in ihrer Eigenschaft als Rechtsinhaber, die Zugänge zu den Daten zu protokollieren, um die rechtmäßige Verarbeitung der Daten der Betroffenen zu belegen (im Falle einer Kontrolle durch die Datenschutzbehörde oder die Gerichtsbarkeit).

Redaktion: Dr. Cristina Motti – Organisationsamt

2. Optimierung der Abläufe für die Beauftragung von Personen zur Verarbeitung von personenbezogenen Daten

Schulinterne Ernennungen

Ausgehend davon, dass die staatlichen Schulen derzeit die Verantwortlichen und die Beauftragten für die Verarbeitung von personenbezogenen Daten auf der Plattform AXAM-S ernennen, und dass dieser Ernennungen zu allgemein sind, dem schulischen Umfeld kaum entsprechen, wurden Ernennungs-Modelle ausgearbeitet für den Verwaltungsverantwortlichen (Schulsekretär), für das Verwaltungs-/Hilfspersonal und für die Dozenten.
Zudem wurden Richtlinien zur Verfügung gestellt, die zum Ziel haben, das beauftragte Personal anzuleiten bei der korrekten Verarbeitung der Daten (siehe auch entsprechende Anlagen).

Vorlagen für die Ernennungen und Richtlinien

- Ernennung des Verwaltungsverantwortlichen
- Ernennung Sekretariatsmitarbeiter und Hilfspersonal
- Entwürfe Richtlinien Datenschutz für Sekretariatsmitarbeiter
- Entwürfe Richtlinien Datenschutz für Hilfspersonal
- Ernennung der Dozenten
- Entwürfe Richtlinien Datenschutz für Dozenten

Externe Ernennungen

Die Arbeitsgruppe hat sich auch mit der Thematik der Ernennungen von externen Verantwortlichen für die Verarbeitung im Falle einer externen Dienstleistung für die Schulen (Auslagerung) beschäftigt und entsprechende Vorlagen ausgearbeitet (siehe Anlagen).

Verzeichnis der Ernennungen:

Ernennung zum externen Verantwortlichen für die Datenverarbeitung – APB
Ernennung zum externen Verantwortlichen für die Datenverarbeitung - Unternehmen

Einbindung AXAM-S:

Es wird empfohlen, die vorhandenen Dokumente durch jene auszutauschen, welche die Arbeitsgruppe erarbeitet hat.

Dokument erstellt von:

Dr. Cristina Motti – Organisationsamt

3. Vorschläge für ein Regelwerk zum Schutz personenbezogener Daten im didaktischen Netzwerk

IT-Didaktik und Datenschutz - Handhabung und Regelung

Dieser Abschnitt beschreibt die möglichen Szenarien und leitet davon empfohlene Maßnahmen für die Handhabung und Regelung des Datenschutzes für die IT-Anlagen für didaktische Zwecke ab. Grundlage sind dabei genauso wie im Verwaltungsbereich die allgemeinen Datenschutzrichtlinien.

In Schulen existieren zwei aus Sicherheitsgründen komplett getrennte IT-Systeme bzw. IT-Netzwerke:

- jenes der Schulverwaltung als Teil des landesweiten Verwaltungsnetzes,
- jenes für didaktische Zwecke.

Das Didaktik-Netz ist in erster Linie für die didaktische Arbeit der Lehrkräfte und Schüler einschließlich der Nutzung des Internets gedacht, wobei in der Regel keine Daten im Sinne des Datenschutzkodex gespeichert und verarbeitet, sondern lediglich Übungen erstellt und bearbeitet werden.
Zur Arbeit der Lehrkräfte gehört jedoch auch der Umgang mit persönlichen Daten z.B. Bewertungen und sonstige Aufzeichnungen über Schüler, Korrespondenz mit Eltern usw. Da es sich dabei um zumindest persönliche Daten im Sinne der Datenschutzrichtlinie handelt, sollten diese folgerichtig im Verwaltungsnetz, das bereits den vorgesehenen Sicherheitskriterien entspricht, verarbeitet und gespeichert werden. Allerdings steht dieses in der Regel nicht in Außenstellen sondern nur in den Schulstellen mit Verwaltungssitz zur Verfügung oder PC-Arbeitsplätze des Verwaltungsnetzes sind nicht in ausreichender Anzahl für die Lehrkräfte vorhanden. Es kann deshalb nicht immer vermieden werden, dass Lehrkräfte persönliche Daten auf PCs der Didaktik verarbeiten und auf Servern der Didaktik abspeichern.

Neben den allgemeinen Prinzipien zur Verarbeitung von Daten[1] gibt der Datenschutzkodex *(Legislativdekret vom 30. Juni 2003, Nr. 196 insbesondere in Art. 33 - 34 – 36² und im Anhang B³)* Sicherheitskriterien für IT-Systeme vor, auf denen persönliche Daten verarbeitet oder gespeichert werden. Ist dies nicht der Fall, unterliegt das System nicht den Datenschutzbestimmungen und somit keinen besonderen Auflagen.
Ausgehend von diesen Vorgaben zur Handhabung persönlicher Daten einerseits und Bedürfnissen der didaktischen Realität anderseits werden für die IT-Systeme der Didaktik folgende Benutzerprofile und Regelungen vorgeschlagen. Sie können im Didaktik-Netz bei entsprechenden technischen Voraussetzungen auch nebeneinander bestehen und für verschiedene Benutzergruppen unterschiedliche Sicherheitskonzepte bereitstellen.
Da in der Didaktik bislang keine speziellen zentralen Datenbankanwendungen zur Verarbeitung zum Einsatz kommen, betreffen die Maßnahmen vor allem den Zugriff auf das Dateisystem.

Regelung des Zuganges zum IT-System

Um einerseits den Zugriff auf das Dateisystem und die dort abgelegten Daten zu regeln und Benutzeraktivitäten wie z.B. Internetzugang kontrollieren zu können, sind dem jeweiligen Bedarf bzw. den Aktivitäten der einzelnen Schule angepasste Benutzerprofile möglich.

Benutzer-Profil S (Sicher**) geeignet zur Verarbeitung persönlicher Daten**

- Persönlicher Benutzername *(siehe „Authentifizierungssysteme" unter Punkten 1 bis 4 der Anlage B des Datenschutzkodex)*
- Komplexes , „starkes" Passwort (Mindestlänge 8 Zeichen, nicht leicht zu erraten)
- Passwort beim ersten Einstieg und in regelmäßigen Abständen (mind. alle 6 Monate) durch den Benutzer zu ändern *(siehe Punkte 5 bis 11 des Anhangs B)*

Profil P (Persönlich**) nicht für Datenverarbeitung im Sinne des Datenschutzkodex geeignet**

- Persönlicher Benutzername
- Beliebige, auch „schwache", aber nur persönlich bekannte Passwörter
- Passwortänderung beim ersten Einstieg, danach nach Belieben des Benutzers

Profil G (**G**ruppe) **nicht für Datenverarbeitung im Sinne des Datenschutzkodex geeignet**

- Gruppen-Accounts (mehrere Benutzer, z.B. Schüler einer Klasse nutzen einen gemeinsamen Benutzernamen und Passwort)
- Beliebige feste, auch „schwache" Passwörter
- Keine Änderung des Passwortes durch Benutzer möglich

Profil A (**A**nonym) **nicht für Datenverarbeitung im Sinne des Datenschutzkodex geeignet**

- Nicht fest zugeordnete Gruppen- oder Einzel- Accounts (z.B. für Kurse)
- Sollten bei Nichtgebrauch gesperrt werden, um Missbrauch zu vermeiden

Profil E (extern**) nicht für die Verarbeitung von Daten der Schule geeignet.**

- Persönliche oder anonyme Accounts für externe Benutzer mit sicheren oder unsicheren Passwörtern
- Ohne Zugang zu Dateiablagen der Schule (Lehrkräfte/Schüler)

Auswahl und Zuordnung der einzelnen Benutzerprofile (Empfehlung)

Jede Schule legt auf Grund ihrer Bedürfnisse fest, wie der Zugang zum schuleigenen didaktischen Netz gehandhabt wird und sorgt in der Folge durch eine interne Benutzungsregelung dafür, dass zu schützende Daten nur in den dafür vorgesehenen Bereichen abgelegt werden.

Für <u>Lehrkräfte</u> wird unabhängig von der Schulstufe **Profil S** empfohlen.
Wenn Lehrkräfte persönliche Daten speichern, ist dieses Profil zwingend erforderlich. Zusätzlich zu einem persönlichen Datenverzeichnis, zu dem

ausschließlich der Benutzer selbst Zugriff hat, werden dem Account weitere gemeinsame Verzeichnisse mit auf bestimmte Gruppen beschränkten Zugriffsrechten zugeordnet. Der Benutzer sorgt in Eigenverantwortung dafür persönliche Daten so abzulegen, dass nur er selbst oder befugte Personen Zugriff haben. *(Siehe „Bewilligungssysteme" unter Punkten 12-13-14 der Anlage B)*
Anmerkung: Amtlich relevante Daten müssen so abgespeichert werden, dass sie im Bedarfsfall, z.B. bei längerer Abwesenheit durch vertretende Personen und durch die Schulführungskraft zugänglich, jedoch vor unbefugtem Zugriff geschützt sind. Mit Verfügbarkeit des digitalen Registers wird die korrekte Verarbeitung und Verfügbarkeit solcher Daten durch dieses geregelt.

Für **Schüler der Sekundarstufe** wird **Profil P** empfohlen.
Zusätzlich zu einem persönlichen Datenverzeichnis, werden dem Account weitere gemeinsame Verzeichnisse mit auf bestimmte Gruppen beschränkten Zugriffsrechten zugeordnet. Je nach Entscheidung der Schule haben Lehrkräfte Zugang zu den Datenverzeichnissen der Schüler. In diesem Fall müssen die Schüler und im Fall von Minderjährigen auch die Eltern über die Möglichkeit dieses Datenzugriffs schriftlich informiert werden.

Schüler der Primarstufe können je nach didaktischem Konzept der Schule vor allem Anfangs mit **Gruppenprofilen G** arbeiten. Empfohlen wird, z.B. ab Klasse 3 oder sobald eine umfangreichere Internetnutzung vorgesehen ist, die Schüler mit persönlichen Profilen P vertraut zu machen.

Für Kurse werden in der Regel **anonyme Profile A** temporär bestimmten Benutzern oder Benutzergruppen zugeordnet, abgelegte Übungen regelmäßig gelöscht. Evtl. wird schulintern protokolliert welche Benutzergruppe wann diese Zugänge verwendet hat (z.B. für Internetnutzung).

Externe Benutzer (z.B. externe Mitarbeiter einer Schulbibliothek oder nicht unterrichtendes Personal) die dauerhaft Zugang zu Teilen des Didaktik-Netzes benötigen, erhalten Benutzerprofile ohne Zugriff auf die Datenlaufwerke der Lehrkräfte und Schüler/innen.

Weitere Maßnahmen: Datensicherung gegen Datenverlust

(Siehe Art. 31 des Datenschutzkodex[4] unter besonderer Berücksichtigung der Punkte 16-17-18 der Anlage B).
Werden im didaktischen Netz persönliche Daten gespeichert, sind Vorkehrungen zu treffen, um den Verlust von Daten zu verhindern und unbefugte Zugriffe, Zerstörung von außen oder unkontrollierten Datenfluss nach außen zu unterbinden.
Für alle Datenverzeichnisse der Profile S ist eine regelmäßige systematische Datensicherung durchzuführen. Welche anderen Daten zusätzlich in welchen Zeitabständen gesichert werden entscheidet die Schule aufgrund ihrer didaktischen Erfordernisse und unter Berücksichtigung der jeweiligen technischen Möglichkeiten. Um die Funktion des IT-Systems sicherzustellen und unkontrollierbare Datenzugriffe durch Schadprogramme zu verhindern ist ein wirksamer aktueller Virenschutz notwendig.

Protokollierung der Internetaktivitäten

(Siehe Richtlinien der Datenschutzbehörde zum Gebrauch von Internet und Email vom 1. März 2007).

Auch wenn die gesetzliche Pflicht zur Protokollierung der Internetaktivitäten auf Benutzerseite nicht mehr besteht, ist es für die Schule von Interesse, diesen aus didaktischen Gründen zu regeln und im Problemfall Rückverfolgen zu können.

Soweit technisch möglich werden die Internetaktivitäten der Benutzer automatisch in einer Protokolldatei („log-Datei") mitgeschrieben, wobei mindestens Datum/ Uhrzeit/Benutzername und aufgerufene Zieladresse (Webseite) festgehalten werden. Diese Protokolle werden mindestens für 6 Monate archiviert und unterliegen dem Datenschutz (Privacy). Sie sind nur im Falle einer polizeilichen Ermittlung durch die Behörden einsehbar. Die Benutzer sind über die Protokollierung in Kenntnis zu setzen.

Hinweis: Eine direkte Rückverfolgung über die Protokollierung bis zum einzelnen Verursacher ist nur bei Verwendung von persönlichen Accounts (Profil S und P) möglich.

Information der Benutzer

Die Benutzer werden von der Schule durch eine Benutzerordnung (PUA) darüber informiert, welche Aktivitäten im Didaktik-Netz und im Internet unter welchen Bedingungen zulässig sind und welche Personen evtl. Zugriff auf ihre Daten haben (z.B. Lehrkräfte auf die Datenlaufwerke der Schüler).

Für minderjährige Schüler sind auch die Eltern zu informieren. Es empfiehlt sich bei dieser Gelegenheit auch die Erlaubnis der Eltern für die Internetnutzung für didaktische Zwecke und die interne Verwendung/Speicherung von Schülerarbeiten oder Fotos einzuholen bzw. eine entsprechende Regelung bekannt zu machen.

Beauftragungen der Netzwerkadministratoren und der Befugten für Datenverarbeitung

Die Schulführungskraft ermächtigt/beauftragt das Schulpersonal (Lehrkräfte) in jedem Fall zur Verarbeitung der Daten im Sinne des Datenschutzcodex *(vgl. Art. 30 des Datenschutzkodex)* und informiert gegebenenfalls darüber, unter welchen Bedingungen im Didaktik-Netz Daten verarbeitet werden dürfen.

Ebenso beauftragt die Schulführungskraft den Wartungsdienst für die Didaktik der Abteilung 9 die IT-Anlagen soweit technisch möglich und entsprechend der Wahl der Schule aus den oben angeführten Optionen zu konfigurieren und zu warten.

Die Abteilung 9 beauftragt ihrerseits die für die jeweilige Schule zuständigen Techniker/Administratoren, führt die entsprechenden Verzeichnisse und überprüft die Eignung und korrekte Abwicklung der Wartungsaufgaben.

Gibt es zusätzlich zu den Technikern des Wartungsdienstes noch schuleigenes Personal, das Teile des Didaktiknetzes verwaltet, etwa die Benutzerverwaltung oder sonstige administrative Aufgaben wahrnimmt, wird dieses von der Schulführungskraft direkt und namentlich dazu beauftragt/ermächtigt) beauftragt *siehe dazu auch Anlage – Modell Nr. 5 und Maßnahme der Datenschutzbehörde vom 27.11.2008 – Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema).*

Sofern im Didaktik-Netz persönliche Daten gespeichert werden, ist die Schule gesetzlich verpflichtet, zur Kontrolle der mit der Wartung beauftragten Administratoren ein System zu installieren, das alle An- und Abmeldungen der Administratoren protokolliert. Das Protokoll muss der Schulführungskraft als Vertreterin der Institution und/oder von ihr dazu beauftragen Personen zugänglich sein und darf von den Administratoren nicht beeinflussbar sein. Die Abteilung Informationstechnik schlägt dazu geeignete Systeme vor.
Wo die Einhaltung der Sicherheitskriterien zur Verarbeitung der Daten aus technischen Gründen (noch) nicht möglich ist, informiert der Wartungsdienst der Abt.9 die Schule darüber und schlägt auf Anfrage der Schule Alternativen bzw. einen Zeitplan zur Behebung vor.
Die Schule kann auch unabhängig von den technischen Möglichkeiten, z.B. aus didaktischen Überlegungen eine von der Empfehlung abweichende Regelung festlegen, wobei es der Schulführungskraft obliegt entsprechende interne Regelungen und Weisungen zu erlassen, bzw. die Benutzer gegeben Falls in Bezug auf die Datensicherheit zu sensibilisieren.

Die getroffenen Entscheidungen bzw. die getroffenen technischen Vorkehrungen oder eventuellen Grenzen werden in der Wartungsvereinbarung bzw. im Datenschutzbericht der Schule festgehalten.

Sensibilisierung der Benutzer

Die Schule sensibilisiert die Lehrkräfte, das Verwaltungspersonal[5] und die Schüler/innen in Bezug auf den Umgang mit persönlichen Daten. Abgesehen von den oben beschriebenen Aspekten und Regelungen wird auf die notwendige Sorgfalt und Eigenverantwortung bei der Verwendung von mobilen Datenträgern (USB-Stick, Speicherkarten, Festplatten) oder externen Netzwerkspeichern („Cloud"-Speicher) hingewiesen. *(Siehe Handbuch der Datenschutzbehörde: Privacy und Cloud-Computing).*

Fußnoten: Gesetzliche Grundlagen

[1] *Allgemeine Prinzipien zur Datenverarbeitung*

„Art. 3 des Datenschutzkodex „Grundsatz der Notwendigkeit bei der Datenverarbeitung":

Bei der Konfigurierung der Informationssysteme und Informatikprogramme ist die Verwendung von personenbezogenen und von Identifizierungsdaten auf ein Minimum zu beschränken, und zwar so, dass die Verarbeitung dieser Daten entfällt, wenn die im Einzelfall verfolgten Zwecke ebenso durch anonyme Daten erreicht werden können beziehungsweise durch Verfahren, bei denen die betroffene Person nur im Bedarfsfall identifiziert werden kann."

„Art. 11 des Datenschutzkodex „Verarbeitungsmodalitäten und Qualität der Daten":

1. Personenbezogene Daten, die Gegenstand einer Verarbeitung sind, müssen:

a) nach Treu und Glauben und korrekt verarbeitet werden;

b) für ausdrücklich festgelegte, rechtmäßige Zwecke erhoben und gespeichert werden und dürfen für andere Verarbeitungsvorgänge nur so weit verwendet werden, als dies mit diesen Zwecken vereinbar ist;

c) sachlich richtig sein und bei Bedarf aktualisiert werden;

d) in Bezug auf die Zwecke, für die sie erhoben oder später weiterverarbeitet werden, einschlägig und vollständig sein und dürfen nicht darüber hinausgehen;

e) so aufbewahrt werden, dass die betroffene Person nicht über den Zeitraum hinaus identifiziert werden kann, der für die Zwecke, wofür die Daten erhoben oder später weiterverarbeitet werden, erforderlich ist.

2. Personenbezogene Daten, bei deren Verarbeitung nicht die einschlägigen Vorschriften eingehalten wurden, dürfen nicht verwendet werden."

[2] ***„ Art. 34 Datenverarbeitung mit elektronischen Mitteln:***

1. Die Verarbeitung personenbezogener Daten

mit elektronischen Mitteln ist nur unter der Bedingung erlaubt, dass mit den in den technischen Vorschriften nach Anhang B angegebenen Modalitäten folgende Mindestsicherheitsmaßnahmen ergriffen werden:

a) Authentifizierung;

b) Festlegung von Verfahren zur Verwaltung der Mittel zur Authentifizierung;

c) Verwendung eines Bewilligungssystems;

d) periodische Aktualisierung der Festlegung des Verarbeitungsbereichs für die einzelnen Beauftragten und für die mit der Verwaltung oder Instandhaltung der elektronischen Mittel betrauten Personen;

e) Schutz der elektronischen Mittel und der Daten vor unrechtmäßiger Datenverarbeitung und vor unerlaubtem Zugriff sowie vor bestimmten Informatikprogrammen;

f) Festlegung von Verfahren zur Verwahrung von Sicherungskopien und zur Wiederherstellung von Daten und Systemen;

g) [aufgehoben];

h) Anwendung von Chiffriertechniken und Identifizierungscodes für bestimmte, von Gesundheitseinrichtungen durchgeführte Verarbeitungen von Daten, die Aufschluss über den Gesundheitszustand oder das Sexualleben geben können.

1bis. [aufgehoben]

1ter. Für die Anwendung der Datenschutzbestimmungen versteht man unter Verarbeitung zu Verwaltungs- und buchhalterischen Zwecken alle Verarbeitungsvorgänge, die unabhängig von der Art der zu verarbeitenden Daten mit Organisations-, Verwaltungs- Finanz und Buchhaltungstätigkeiten zusammenhängen.

Insbesondere betrifft dies Tätigkeiten zur internen Organisation, zur Erfüllung von Vertrags- oder vorvertraglichen Pflichten, zur Verwaltung aller Abschnitte eines Arbeitsverhältnisses, zur Buchhaltung sowie zur Anwendung von Rechtsvorschriften in den Bereichen Steuerwesen, Gewerkschaft, Für- und Vorsorge, Gesundheit, Hygiene und Arbeitssicherheit."

„Art. 36 Anpassung

1. Die technischen Vorschriften nach Anhang B über die in diesem Kapitel vorgesehenen Mindestsicherheitsmaßnahmen werden periodisch mit Dekret des Justizministers im Einvernehmen mit dem Minister für Innovation und Technologie und dem Minister für die Vereinfachung der Gesetzgebung dem neuesten Stand der Technik und den Erfahrungen in diesem Bereich angepasst."

[3] ***Anhang B: Technische Vorschriften im Bereich der Mindestsicherheits-maßnahmen,*** *insbesondere Datenverarbeitung mit elektronischen Mitteln (im Zusammenhang mit Art. 33 bis 36 des Datenschutzkodex)*

[4] ***„Art. 31 Sicherungspflicht***

1. Verarbeitete oder zu verarbeitende personenbezogene Daten müssen je nach Art und nach Verarbeitungsmethode so aufbewahrt und überwacht werden, dass durch geeignete vorsorgliche Schutzmaßnahmen die Gefahr einer Vernichtung oder eines Verlusts, auch wenn dies durch Zufall geschieht, eines unbefugten Zugriffs oder der unbefugten oder nicht dem Beschaffungszweck entsprechenden Verarbeitung auf ein Minimum reduziert wird; zu diesem Zweck werden die neuesten technischen Erkenntnisse in Betracht gezogen."

[5] ***„Art. 18 Grundsätze für jede Datenverarbeitung durch öffentliche Rechtsträger***

2. Öffentliche Rechtsträger dürfen personenbezogene Daten nur zu institutionellen Zweckenverarbeiten.

3. Bei der Datenverarbeitung haben öffentliche Rechtsträger die Bedingungen und Beschränkungen zu beachten, die in diesem Kodex, auch in Hinblick auf die Verschiedenartigkeit der Daten, sowie in Gesetzen und Verordnungen festgelegt sind.

4. Abgesehen von den im II. Teil festgelegten Vorschriften für Personen, die einen Gesundheitsberuf ausüben, sowie für öffentliche Gesundheitseinrichtungen, müssen öffentliche Rechtsträger nicht die Einwilligung der betroffenen Person einholen.

5. Es gelten die Bestimmungen über die Übermittlung und Verbreitung laut Artikel 25."

„Art. 35 Verarbeitung ohne elektronische Mittel

1. Die Verarbeitung personenbezogener Daten ohne elektronische Mittel ist nur unter der Bedingung erlaubt, dass mit den in den technischen Vorschriften nach Anhang B angegebenen Modalitäten folgende Mindestsicherheitsmaßnahmen ergriffen werden:

a) periodische Aktualisierung der Festlegung des Verarbeitungsbereichs für die einzelnen Beauftragten oder die Organisationseinheiten;

b) Festlegung von Verfahren zur angemessenen Verwahrung der Akte und Dokumente,die den Beauftragten zur Ausführung ihrer Aufgaben anvertraut sind;

c) Festlegung von Verfahren zur Aufbewahrung bestimmter Akte in beschränkt zugänglichen Archiven sowie Festlegung der Zugangsmodalitäten in Bezug auf die Identifizierung der Beauftragten."

Anlage B – Punkt 20 bis 29

IT-Didaktik und Datenschutz
Zusammenfassung

Der Gesetzgeber schreibt für die Datenverarbeitung mit elektronischen Mitteln genau definierte Sicherheitskriterien vor. „Daten" im Sinne des Gesetzes sind solche, die personenbezogene Informationen enthalten.
Im Unterschied zum Verwaltungs-Netz der Schulen („Lasis") ist im Didaktik-Netz die Einhaltung dieser Kriterien unter Umständen nicht durchgängig möglich oder gewünscht.
Z.B. kann es für Lehrkräfte notwendig sein, unter das Datenschutzgesetz fallende Daten (z.B. namentlich zugeordnete Informationen über Schüler) auf dem Didaktik-Netz zu speichern, während Schüler in der Regel lediglich anonymisierte Übungen erstellen und keine „Daten" im Sinne des Datenschutzgesetztes verarbeiten, anderseits aber eine flexible Arbeitsumgebung und einen der Altersstufe angemessen Zugang erhalten sollen.

Durch die Wahl entsprechender Benutzerprofile kann die Schule das Sicherheitsniveau für die einzelnen Benutzergruppen (z.B. Lehrkräfte, Schüler in verschiedenen Altersstufen, Kurse …) den Erfordernissen entsprechend wählen. Diese Entscheidung steht in direktem Zusammenhang damit, welche Art von Daten der Benutzer im Didaktik-Netz verarbeiten kann/darf und welche Benutzergruppen darauf Zugriff haben können.

Die Entscheidung der Schule für die einzelnen Benutzerprofile werden in der Wartungsvereinbarung als Auftrag für die technische Wartung festgehalten und von den dazu beauftragten Systemadministratoren umgesetzt. Diese sind für die korrekte Bereitstellung der vereinbarten Sicherheitskontexte verantwortlich. Die Verantwortung für die im jeweiligen Kontext korrekte Dateiablage oder Zugriffsmöglichkeit und die entsprechende Information/Einführung der Benutzer (z.B. durch entsprechende Hinweise in der Benutzerordnung) obliegt der Schule.
Prinzipiell können „sichere" und „unsichere" Benutzerprofile und entsprechend zugeordnete Dateiablagen im Didaktik-Netz nebeneinander existieren. Sobald im Didaktik-Netz einer Schule auch nur ein einziges zur Datenverarbeitung vorgesehenes Profil verwendet wird, sind sicherheitsrelevante Basisfunktionen für das Gesamtsystem einzuhalten.
Das kann einen administrativen Mehraufwand und eventuelle Investitionen in Hard- und Software mit entsprechenden Kosten bedeuten. Möglicherweise sind deshalb nicht in jeder Schulumgebung alle Optionen sofort umsetzbar.

Die Schule wird bei der Aktualisierung der Wartungsvereinbarung über die aktuelle Umsetzbarkeit bzw. Zeitpläne und eventuelle Kosten für die Schule informiert.

erstellt von:
Dr. Armin Haller – Abteilung Informationstechnik
Prof. Andrea Bonani – Italienisches Schulamt
Dr. Cristina Motti – Organisationsamt

Entscheidungsbaum

Für jede Benutzergruppe (Lehrkräfte, Schüler …) wählt die Schule ein den Erfordernissen in Bezug auf die Datenverarbeitung im Didaktik-Netz angemessenes Benutzerprofil.

<table>
<tr><td colspan="3">Benutzer/Benutzergruppe (z.B. Lehrkräfte, Schüler, Kursteilnehmer …)
verarbeitet/speichert
Daten im Sinne des Datenschutzgesetzes
im Didaktik-Netz</td></tr>
<tr><td>JA
(für Lehrkräfte wahrscheinlich daher empfohlen,
für Schüler optional möglich)</td><td colspan="2">NEIN
(möglich für Schüler, Kurse
oder auch Lehrkräfte wenn ausdrücklich <u>keine</u>
„Daten" auf dem betreffenden Gerät/Netz
verarbeitet werden)</td></tr>
<tr><td>Benutzer/ Benutzergruppe hat sichere Zugangskriterien einzuhalten

(Benutzerprofil S)
Persönlicher Account,
nur dem Nutzer selbst bekanntes, komplexes Passwort, Mindestlänge 8 Zeichen, Password regelmäßig (max. 6 Monate) erneuert.</td><td>Persönlicher Account mit Passwort ohne bestimmte Kriterien, kann vom Benutzer geändert werden.
(Benutzerprofil P)</td><td>Gruppen-Account oder anonymer Account mit fixem Passwort, kann durch Benutzer nicht geändert werden.
Achtung: keine eindeutige Identifizierung z.B. bei Protokollierung der Internetaktivitäten.
(Benutzerprofil G oder A)</td></tr>
<tr><td>Inhalt der persönlichen Dateiablage ist ausschließlich dem Benutzer zugänglich.</td><td colspan="2">Sollen Inhalte der persönlichen Dateiablage der Schüler für Lehrkräfte zugänglich sein?</td></tr>
<tr><td>Inhalt gemeinsamer Datenablagen sind ausschließlich der befugten Benutzergruppe (z.B. Klassenrat, Lehrerkollegium) zugänglich.</td><td>NEIN</td><td>JA
Benutzer (Schüler / evtl. Eltern) müssen darüber informiert werden.</td></tr>
<tr><td>Sicherheitsmaßnahmen zur Verhinderung von Datenverlust (systematische, regelmäßige Datensicherung), Zerstörung oder unkontrollierten Verbreitung (aktueller Antivirus, Firewall)
obligatorisch</td><td colspan="2">Sicherheitsmaßnahmen gegen Sabotage oder Schadsoftware für die Stabilität des Systems notwendig, wird soweit technisch möglich umgesetzt.
Umfang und Häufigkeit der Datensicherung mit der Schule je nach Anforderung und technischer Möglichkeit
zu vereinbaren.</td></tr>
</table>

Dokument erstellt von:
Dr. Armin Haller: Abt. Informationstechnik **-** Dr. Bonani Andrea: It. Schulamt

4. Das IT-System

Den Rechtsinhabern der mit elektronischen Mitteln durchgeführten Verarbeitungen vorgeschriebene Maßnahmen und Vorkehrungen in Bezug auf die Zuweisung der Funktionen als Systemadministratoren laut Anordnung 27. November 2008 (G.U. n. 300 del 24 dicembre 2008)

Die Datenschutzbehörde hat die Führung einer Liste aller Systemadministratoren angeordnet. Die Einhaltung dieser Anordnung endet nicht mit der Vorbereitung einer neuen Beauftragung zur Erteilung der Befugnis zur Verarbeitung personenbezogener Daten oder in der Änderungen der bestehenden Beauftragung, sondern, verlangt vom Rechtsinhaber eine Reihe von Maßnahmen.
Die Verpflichtung der Erfassung und Ernennung zum Systemadministrator wurde für Organisationen eingeführt, die personenbezogene Daten mit elektronischen und informationstechnischen Mitteln verarbeiten.

Nachdem die Datenschutzbehörde ein mangelndes Bewusstsein der in der Durchführung der Aufgaben eines Systemadministrators enthaltenen Kritizität „nicht nur in Organisation kleineren Umfangs, sondern auch in hohen Verantwortungspositionen, mit einer besorgniserregenden Unterschätzung der Risiken, die durch unkontrollierte Maßnahmen von Seiten jener, die Aufgaben der Überwachung und Kontrolle der korrekten Verwendung des Informationssystems innehaben sollten", festgestellt hat, führte sie die Figur des Systemadministrators mit der Anordnung 27. November 2008 wieder ein.

Diese neue Figur führt beträchtliche Änderungen in der Verwaltung des Datenschutzes der Organisationen ein, tatsächlich bestanden die vorgesehen institutionellen Rollen aus dem Rechtsinhaber der Verarbeitung, dem Verantwortlichen für die Verarbeitung und dem Beauftragten.
Der Systemadministrator konnte vom Rechtsinhaber als Beauftragter oder Verantwortlicher erfasst werden und damit war er der Kontrolle und Prüfung durch die Organisationsstruktur unterworfen; jetzt hingegen muss diese Figur einer Person mit bestimmten beruflichen Vorraussetzungen sein.

Zur Findung und Bewertung ist es günstig eine Art Curriculum vitae für jeden Systemadministrator vorzubereiten, aus dem Studientitel, Berufsqualifikation, Berufserfahrung, besuchte Weiterbildungskurse klar hervorgehen. Das Curriculum muss vom beauftragten Administrator unterzeichnet sein und der Ernennung beigelegt werden.

In der Praxis muss der Administrator nicht nur ein guten Techniker sein, sondern er muss das Datenschutzgesetz und die Prinzipien der Sicherheit in der Informationstechnik beherrschen.

Die wichtigsten Verpflichtungen, die der Rechtsinhaber einhalten muss sind im Wesentlichen folgende:

1. **Bewertung der subjektiven Merkmale** in Bezug auf das Berufsprofil der der Person, die beauftragt werden soll: es muss sich um eine vertrauenswürdige Person handeln.
   Der Rechtsinhaber der Verarbeitung muss die Erfahrung, die Fähigkeiten und Verlässlichkeit der zum Systemadministrator benannten Personen, die eine angemessene Garantie der vollständigen Beachtung der geltenden Vorgaben in Bezug auf die Verarbeitung, Sicherheit inbegriffen vorlegen müssen, bewerten
   Die Benennung zum Systemadministrator ist persönlich: es muss eine eigens erstellte schriftliche Benennung vorbereitet werden, die eine analytische Liste der laut zugewiesenem Autorisierungsprofil erlaubten Aufgabenbereiche enthält. Die Beauftragung muss persönlich erfolgen und kann daher nicht eine Firma betreffen.

2. **Die Liste der Systemadministratoren** muss vom Rechtsinhaber erstellt werden und an einem dem Personal und der Öffentlichkeit zugänglichem Ort zur Verfügung gestellt werden. Das heißt, dass der Öffentlichkeit und dem Personal die Namen der Systemadministratoren bekannt gegeben werden müssen.
   "Die Eckdaten der physischen Personen in der Funktion der Systemadministratoren, mit der Liste der ihnen zugewiesenen Funktionen müssen in einem internem Dokument, das aktuell gehalten werden und im Fall einer Überprüfung, auch von Seiten der Datenschutzbehörde, verfügbar sein muss."
   Wenn Dienste der Systemadministration in Outsourcing ausgegeben werden, müssen der Rechtsinhaber oder der externe Verantwortliche der Verarbeitung für jede Eventualität die Eckdaten der Systemadministratoren direkt aufbewahren.

3. **Überprüfung der Tätigkeiten** des Administrators auf dem Informationssystem einmal pro Jahr.
   Die Überprüfung hat die Übereinstimmung der praktischen Tätigkeiten des Systemadministrators mit organisatorischen, technischen und sicherheitstechnischen Maßnahmen in Bezug auf die Verarbeitung personenbezogener Daten, wie von den geltenden Bestimmungen vorgesehen, zum Ziel.

4. **Registrierung der Zugriff** auf Verarbeitungssysteme und elektronischen Archive von Seiten der Systemadministratoren, über angemessene Systeme zur Registrierung der logischen Zugriffe.
   Die Registrierung (access log) müssen die Merkmale der Vollständigkeit, der Unveränderbarkeit und der Möglichkeit der Überprüfung ihrer Integrität aufweisen, die nötig sind um das Ziel der Überprüfung zu erreichen (Abkürzungen sind nicht erlaubt).
   Die Registrierungen müssen zeitliche Bezüge enthalten und die Beschreibung des Ereignisses, das sie ausgelöst hat und sie müssen für einen angemessenen

Zeitraum, aber nicht weniger als sechs Monate, aufbewahrt werden.
Für diese letzte Maßnahme stehen verschieden Softwarelösungen zur Verfügung, sowohl von Seiten von Firmen gegen Bezahlung als auch kostenlos. Letztere Lösungen bedürfen meist aufwendiger manueller Eingriffe. Alternativ dazu bieten Firmen die **Dienstleistung** der Verwaltung und Kontrolle der Log der Systemadministratoren an, meist zu Kosten in Bezug auf die Anzahl betroffen Schulen, und daher der entsprechenden Systemadministratoren.

Zum Beispiel: *Inspektoren die die Schule aufsuchen, würde als erstes die aktuelle und vollständige Liste der Systemadministratoren oder gleichgestellter Figuren, deren spezifische Benennungen anfordern und außerdem würden einige PC überprüft , um fest zu stellen, ob die Software zur Registrierung der Zugriffe der Systemadministratoren in Funktion ist.*
Dann würden die Mitteilungen laut Datenschutzgesetz (informativa), die Ernennung zum Beauftragen, die Einhaltung der Sicherheitsmaßnahmen in der Verwaltung von Papier und Informationstechnik, im besonderen der sensiblen Daten, u.s.w.

Dokument erstellt von:

Dr. Simonetta Maina – Abteilung Informationstechnik

Technische Verwaltung des Informationssystems – Bereich der Didaktik (Stand 30, Juni 2013)

In Bezug auf das **Filesystem** (Ablage und Organisation der Dateien auf digitalen Archivsystemen wie Speicherplatten von Servern oder PCs, oder CDs) und **Mailserver** (sofern in der Schule vorhanden) sind die Daten nicht differenzierbar (die Techniker können keine Aussage treffen, ob die gespeicherten Daten personenbezogen sind oder nicht, wenn dies nicht vom Rechtsinhaber mitgeteilt wird).

Folgenden Listen enthalten die Namen der Techniker, die Zugang zum Informationssystem der Didaktik der Schuen in Südtirol haben, unter Angabe der Organisationseinheit der sie angehören und des Aufgabenbereichs.

N.	Name	ORGANISATIONSEINHEIT	AUFGABEN
1	Aichner Philipp	Abt. Informationstechnik	Systemadministrator operativo
2	Altstätter Fabian	Abt. Informationstechnik	Systemadministrator operativo
3	Amort Philipp	Abt. Informationstechnik	Systemadministrator operativo
4	Baratta Paolo	Abt. Informationstechnik	Systemadministrator operativo
5	Blasinger Andreas	Abt. Informationstechnik	Systemadministrator operativo
6	Brunner Alexander	Abt. Informationstechnik	Systemadministrator operativo
7	Dejakum Manuel	Abt. Informationstechnik	Systemadministrator operativo
8	Demetz Georg	Abt. Informationstechnik	Systemadministrator operativo
9	Dietl Birgit	Abt. Informationstechnik	Systemadministrator operativo
10	Fieg Thomas-Peter	Abt. Informationstechnik	Systemadministrator operativo
11	Fracchetti Roberto	Abt. Informationstechnik	Systemadministrator operativo
12	Gander Alexander	Abt. Informationstechnik	Systemadministrator operativo
13	Gander Manuel	Abt. Informationstechnik	Systemadministrator operativo
14	Klotz Peter	Abt. Informationstechnik	Systemadministrator operativo
15	Lanz Lothar	Abt. Informationstechnik	Systemadministrator operativo
16	Lazzeri Gustav	Abt. Informationstechnik	Systemadministrator operativo
17	Lisci Gianni Battista	Abt. Informationstechnik	Systemadministrator

			operativo
18	Mairhofer Andreas	Abt. Informationstechnik	Systemadministrator operativo
19	Martello Bruno	Abt. Informationstechnik	Systemadministrator operativo
20	Oberhollenzer Helmut	Abt. Informationstechnik	Systemadministrator operativo
21	Obkircher Jakob	Abt. Informationstechnik	Systemadministrator operativo
22	Padovan Andrea	Abt. Informationstechnik	Systemadministrator operativo
23	Pfeifer Markus	Abt. Informationstechnik	Systemadministrator operativo
24	Pfendt Lukas	Abt. Informationstechnik	Systemadministrator operativo
25	Picozza Luca	Abt. Informationstechnik	Systemadministrator operativo
26	Promberger Alberto	Abt. Informationstechnik	Systemadministrator operativo
27	Rauch Anita	Abt. Informationstechnik	Systemadministrator operativo
28	Regensburger Markus	Abt. Informationstechnik	Systemadministrator operativo
29	Reiner Ingo	Abt. Informationstechnik	Systemadministrator operativo
30	Rottensteiner Daniel	Abt. Informationstechnik	Systemadministrator operativo
31	Runggatscher Georg	Abt. Informationstechnik	Systemadministrator operativo
32	Soraru Raimund	Abt. Informationstechnik	Systemadministrator operativo
33	Tarini Sabine	Abt. Informationstechnik	Systemadministrator operativo
34	Thöni Gunnar	Abt. Informationstechnik	Systemadministrator operativo
35	Untersteiner Kathrin	Abt. Informationstechnik	Systemadministrator operativo
36	Waldboth Bernd	Abt. Informationstechnik	Systemadministrator operativo
37	Waldboth Helene	Abt. Informationstechnik	Systemadministrator operativo
38	Zwerger Florian	Abt. Informationstechnik	Systemadministrator operativo

Technische Verwaltung des Informationssystems - Bereich Verwaltung (Stand 30, Juni 2013)

a) File System: Systemadministratoren haben sowohl Lese-, als auch Schreibrechte auf die Dateien

b) Datenbanken: DBA (Datenbankadministratoren) und Programmierer haben Zugang. Der Endanwender greift auf die Datenbank immer über eigenes vorgesehen Programme zu.

SYSTEMADMINISTRATOR	ORGANISATIONSEINHEIT	AUFGABE
Metz Gerald	Abt. Informationstechnik	Systemadministrator operativo
Moriggl Zeno	Abt. Informationstechnik	Systemadministrator operativo / Programmierer
Simon Tengler	Südtiroler Informatik	Systemadministrator operativo
Manfred Kerschbamer	Südtiroler Informatik	Systemadministrator operativo / Systemadministrator Mail Server
Barbara Scudier	Abt. Informationstechnik	Systemadministrator Mail Server
Kurt Pöhl	Abt. Informationstechnik	Systemadministrator Mail Server
Moriggl Irene	Abt. Informationstechnik	Systemadministrator operativo
Regensburger Markus	Südtiroler Informatik	Systemadministrator operativo
Scudier Barbara	Abt. Informationstechnik	Systemadministrator operativo
Santer Andreas	Südtiroler Informatik	Systemadministrator operativo / Progr.
Secchi Daniela	Abt. Informationstechnik	Systemadministrator operativo
Demarco Francesco	Südtiroler Informatik	Systemadministrator operativo
Bertignoll Egon	Südtiroler Informatik	Systemadministrator operativo
Rivelli Antonello	Südtiroler Informatik	Systemadministrator operativo
Prosch Martin	Südtiroler Informatik	Systemadministrator operativo / Progr.
Bertoldi Francesco	Südtiroler Informatik	Systemadministrator operativo / Progr.
Pöhl Harald	Südtiroler Informatik	Systemadministrator operativo / Datenbankadministrator
Niederkofler Albin	Südtiroler Informatik	Systemadministrator

		operativo / Datenbankadministrator
Matteo Cuzzolin	Südtiroler Informatik	Netzwerkadministrator
Matthias Eller	Südtiroler Informatik	Netzwerkadministrator
Roberto Fabbri	Südtiroler Informatik	Netzwerkadministrator
Marco Tienghi	Südtiroler Informatik	Netzwerkadministrator
Valentinelli Ermano	Dedagroup	Programmierer
Piz Lorenzo	Entity	Programmierer
Alessandro Bottonelli	AXISNet	Systemadministrator operativo / Anwendungsverwalter
Sergio Bonfiglio	AXISNet	Programmierer / Anwendungsverwalter
Simonetta Maina	Abt. Informationstechnik	Anwendungsverwalter

Den Datenbanken entsprechen verschiedenen Anwendungen in den Schulen.

DATENBANK	ART PERSONEN-BEZOGENENER DATEN	ART SENSIBLER DATEN	ART NICHT PERSONENBE-ZOGENDER DATEN	ANMER-KUNGEN
POPCORN	Meldedaten Schüler, Meldedaten unterrichtendes Personal, Meldedaten Eltern, Noten, Bewertungen		Sitz der Schule (Gebäude), Bankkoordinaten der Schule	
OBU			Buchhaltung Schule Inventar	
Supplenze	Meldedaten unterrichtendes Personal Arbeitsverträge			Datenüber-gabe an das Ministerium (MIUR)
Contributi	Meldedaten Schüler Meldedaten Eltern		Buchhaltungsdaten	Datenüber-gabe an SAD
Trasferte insegnanti	Meldedaten unterrichtendes Personal		Buchhaltungsdaten	
Straordinari (file excel)	Meldedaten unterrichtendes Personal		Buchhaltungsdaten	
Sport scolastico	Meldedaten Schüler Meldedaten unterrichtendes Personal			
Gestione orari	Meldedaten unterrichtendes			

	Personal			
LIBRO ACS ALEPH	Meldedaten Schüler Meldedaten unterrichtendes Personal		Datenbücher	

CALL CENTER der Landesverwaltung (und Techniker des Call Centers / /RTI)

Die Mitarbeiter des Call Center unterstützen im Allgemeinen nur Nutzer und PC der der Verwaltung der Schulen.

Sie haben keinen Zugang zum Netz der Didaktik.

Dem unterrichtenden Personal stehen im Lehrerzimmer ein oder mehrerer PC im Landesnetz zur Verfügung; sie können also Dienste und Techniker des Call Center in Bezug auf diese Arbeitsplätze im Landesnetz, Landesmail und digitales Personalfaszikel nützen.

Die Mitarbeiter des Call Center können mit den Informationssystemen und informationstechnischen Mitteln der Schulen wie folgt interagieren:

- Die Techniker des Call Center greifen nicht direkt auf die Datenbank von Popcorn zu, können aber die Daten daraus in Excel exportieren und in andere Datenstrukturen importieren.
- Sie können das Kennwort von Axam (Programm zur Verwaltung der Verarbeitung personenbezogener Daten) zurücksetzen.
- Sie greifen über das Programm Netviewer auf den Desktop des Endanwenders zugreifen. Der Nutzer muss diesen Zugriff explizit gewähren, erst dann kann das Call Center interagieren. In keinem Fall ist der Zugriff auf das Filesystem möglich, in Ausnahmefällen wird dem Call Center erlaubt, direkt auf dem PC zu agieren. Jede Aktion kann der Nutzer am Bildschirm verfolgen und überprüfen. Netviewer erlaubt keine Operation ohne Wissen des Nutzers.
- Telefonische Unterstützung bei den verschiedenen Problemen mit HW und SW. in bestimmen Fällen kann sich das Call Center Daten vom Nutzer schicken lassen, die dem Incident beigelegt werden. (Diese Daten können Auszüge aus der Datenbank von Popcorn oder Screenshots der verschiedenen Programme sein, um die Arbeit der Techniker zu erleichtern). Diese Daten werden direkt von Nutzer verschickt. Das Call Center kann diese Daten nicht autonom entnehmen.

Im folgenden die Techniker des Call Center:

Call Center	Tecniker Datef	Tecniker on site	Asset manager
Marco Schiavone	Josef Scheiber	Martin Crepaz	Stefano Forcelloni
Roland Innerebner	Clemens Santa	Matteo Greghi	Roberto Della Pietra
Dietmar Thaler	Thomas Donega		
Patrick Guerra	Bernhard Aichner		
Michael Menz	Samuel Fink		
Tobia Porto	Markus Weger		
Luca Ferrari			

Zugänge der Techniker von Datef:

- Physischer Zugang zu PC und Server bei Reparutren auf Anfragen der Nutzer oder der Abteilung Informationstechnik.

Zugänge der Techniker on site:

- Physischer Zugang zu den PC der Anwender auch mit Administratorenrechten, aber nur auf Anfrage des Nutzers oder nach Gemehmigung durch die Abteilung Informationstechnik.

Dokument erstellt von:

Dr. Simonetta Maina – Abteilung Informationstechnik

Datenfelder in der Schülerverwaltungssoftware - Popcorn

Allgemein:
Grundsätzlich kann man die Daten in Popcorn in 3 größere Bereiche einteilen.

- **Personenbezogenen** Daten (anagrafische Daten)
- **Schulbezogenen** Daten (Adresse der Schule usw.)
- **Schülerbezogenen** Daten (Noten, Fachrichtungen, Einschreibungen, Klassen usw.)

In diesem Dokument werden die Datenfelder festgehalten, die sowohl der Benutzer in der Schule (Sekretär) als auch der Benutzer im Schulamt bearbeiten kann, sowie diesbezüglich relevante Daten, die das System berechnet um dem Benutzer visualisiert.

Personenbezogene Daten *(Vollrepliziert PAB-Schulen)*

- Zuname
- Vorname
- Geburtsdatum
- Geburtsort (Codiert, d.h. hier wird aus einer Liste von Orten gewählt. Die List der Gemeinden Italiens ist vorgegeben und kann vom User nicht geändert werden, ausländischen Orte kann der User selbst hinzufügen, allerdings nicht löschen oder ändern).
- Geschlecht (männlich/weiblich)
- Steuernummer (wird mit den eingegebenen Daten überprüft)
- Titel (wird nur bei Eingabe eines Elternteils angezeigt)
- Sanitätscodex (freies Feld)
- Staatsbürgerschaften (mit Beginndatum, mehrere möglich)
- Vater, Mutter, gesetzlicher Vormund
- Sprache (kann nur bei Eltern angegeben werden, nicht bei Schülern)
- Adresse:
    - Strasse (freies Feld)
    - Gemeinde (als Auswahlfeld)
    - Postleitzahl
    - Fraktion
- Zusätzliche Adresse/Heim
- Kontakte (mehrere vom gleichen Typ sind möglich. Z.B. mehrere e-mail-adressen)
    - Telefonnummer
    - Handynummer
    - Fax
    - E-Mail
    - Pager
    - Webadresse
- Bankkoordinaten:
    - IBAN
    - SWIFT
    - Name der Bank
- FD-Code (zufällige 6-stellige vom System berechnete Nummer für jeden Schüler)

Schulbezogene Daten *(Vollrepliziert PAB-Schulen)*

- Direktion:
  - Bezeichnung (DE,IT,LA)
  - Kurzbezeichnung
  - LasisCODE
  - Direktor (= Person)
  - Vizedirektor (=Person)
  - Sekretär (=Person)
  - Mwst-Nr
  - Adresse:
    - Gemeinde
    - Strasse
    - Fraktion
    - CAP
  - Beginn Datum
  - End Datum
  - Typ (Kindergarten, Grundschule, Mittelschule, Oberschule, Berufsschule, Schulübergreifend)
  - Schulamt (Abt. 16,17,18,20,21,22, oder Privatschule)
  - Bankkoordinaten der Schule
- Schulstelle:
  - Gleich wie Direktion nur ohne Direktor, Vizedirektor und Sekretär
- Angebotene Fachrichtungen pro Schulstelle

Schülerbezogene Daten

- Einschreibung *(nicht repliziert)*
  - Beginn
  - Ende
  - Grund für Ende (vorgegebenen Liste)
  - Fachrichtung
  - Stufe
  - Schule
  - Schuljahr

Die Einschreibung bezieht sich immer auf eine Schule / Fachrichtung / Stufe / Schuljahr Kombination. Ein Schüler kann zu einem bestimmten Zeitpunkt im gleichen Schuljahr nur eine Einschreibung haben.

Replikation:
Einschreibungen werden über eine redundante Tabelle (eigene Tabelle, die alle nötigen Teilinformationen (Personenschlüssel, Schuljahr, Direktion/Schule, Beginn/Ende enthält) voll repliziert.

- Klassen: *(nicht repliziert – werden wöchentlich gesammelt)*
  - Bezeichnung Lang
  - Bezeichnung Kurz
  - Beginn-Ende
  - Sektion (A,B,C, usw.)
  - Fachrichtung bzw. Fachrichtungen oder Schulstufen (es kann zusammengelegte Klassen bestehend aus mehreren Fachrichtungen geben (z.B. 1 A Biologie und 1 A Chemie) als auch bestehend aus

mehreren Schulstufen (z.B. 1,2,3 Grundschule) bzw. auch eine Kombination aus beiden)

- Zusatzinformationen zu den Einschreibungen (eine Liste vorgegebenen Werte, die pro Schüler mit JA/NEIN und einem Datum ausgewählt werden können): *(nicht repliziert – wöchentliche Sammlung)*
  - Besondere Einschreibung
  - Der Schüler wiederholt die Klasse das dritte Mal
  - Der Schüler wiederholt die Klasse das erste Mal
  - Der Schüler wiederholt die Klasse das zweite Mal
  - Einschreibung wegen Kontrolle ausgesetzt
  - Erfüllung der Impflicht
  - Erhebung Abteilung (nur für Berufsschulen sichtbar)
  - hat das Fach Katholische Religion nicht besucht - mit Alternativunterricht
  - hat das Fach Katholische Religion nicht besucht - ohne Alternativunterricht
  - Schüler aus einem anderen Einzugsgebiet
  - SII - ABO+ nicht beantragt
  - SII – Spezialtransport

Weiters kann sich die Schule selbst neue Einträge erstellen (z.B. Mensa) und für die Schüler JA/NEIN Werte vergeben.

- Herkunftsschule *(nicht repliziert)* (automatisch berechenbar, wenn der Schüler aus einer Schule kommt, die in Popcorn erfasst ist. Die Berechnung erfolgt aufgrund der Einschreibungen in Popcorn. Oder ein freies Textfeld, falls der Schüler vom Ausland kommt)
- Fächer (pro Fachrichtungsstufe) (*nicht bzw. Teilrepliziert*)
  - Auswahl an Fächern die von den Schulämtern vorgegeben werden
  - Möglichkeit zur Eingabe eigener Fächer
  - Bewertungstyp pro Fach und Semester (mündlich, schriftlich, praktisch, Leistung)
  - Bewertungsform pro Fach und Semester (ausgeschrieben, numerisch, Bewertungsskala)
  - Anzahl der Wochenstunden
  - Länge der Unterrichtseinheiten in Minuten
  - Gesamte Unterrichtsstunden des Faches im Schuljahr
  - Fächertyp (Unterricht, Wahlfach, Übergreifende Kompetenz, fächerübergreifendes Lernangebot)
  - Reihenfolge der Fächer auf dem Zeugnis
  - Zählt zum Druchschnitt JA/NEIN
- Bewertung (Noten) *(nicht repliziert)*
  - Pro Fach und Schüler
  - Jede Note hat ein vordefiniertes Gewicht zur Berechnung des Durchschnitts (wichtig bei ausgeschriebenen Noten (z.B. sechs = 6)
  - Absenzen pro Fach
  - Kommentar pro Fach
- Jahresbewertung *(nicht repliziert)*
  - Versetzt

  - Nicht versetzt
  - Aufgeschoben
  - Versetzt / Nicht versetzt nach aufgeschoben
  - Zur Prüfung zugelassen /nicht zugelassen
  - Jahresabsenzen (entschuldigte /nicht entschuldigte)
  - Datum der Notenkonferenz
  - Kommentar zur Jahresbewertung
  - Ausgeschriebenen Jahresbewertung
  - Gültigkeit des Schuljahres (gültig, nicht gültig, durch Ausnahme gültig)
- Guthaben *(nicht repliziert)*
  - Schulguthaben (Wert wird aus dem Notendurchschnitt berechnet und vorgeschlagen)
  - Bildungsguthaben
  - Ergänzendes Guthaben (gibt es nicht mehr)
- Diplomdaten für Mittel und Oberschulen *(nicht repliziert)*
  - Bestanden / nicht bestanden
  - Diplomnummer
  - Kommissionsnummer
  - Vorsitzende (Textfeld)
  - Zweites schriftliches Prüfungsfach (Auswahlliste aus allen zugewiesenen Fächern)
  - Diplomdatum
  - Gesamte Punktezahl
  - Aufgesplitterte Punktezahl (schriftlich, mündlich, Schulguthaben, zusätzliche Punkte)
  - Kommentar der Kommission
- Diplomdaten der Berufsschulen *(nicht repliziert)*
  - Praktika (siehe -> Praktika)
  - Gesamtnote
  - Teilnoten (jeweils eine Zahl)
    - Prüfungsgespräch
    - Schriftliche Prüfungsarbeiten
    - Praktische Prüfung oder Simulierung
    - Anderes
  - Ergänzende Bemerkungen (freies Textfeld)
- Praktika (nur bei Berufsschulen) *(nicht repliziert)*
  - Anfang (Datum)
  - Ende (Datum
  - Beschreibung (DE,IT,LA)
  - Organisation (DE,IT)
  - Gemeinde
  - Ort
  - Dauer
  - Eventuelle andere Praktische Erfahrungen (Auslandserfahrungen)
    - Beschreibung (freies Feld)
    - Dauer
    - Modalität (freies Feld)

Spezielle Eingabefelder

ASTAT-Datenerhebung: *(nicht repliziert, die Daten werden manuell gesammelt sobald die Schulen mit der Eingabe fertig sind)*
Dies stellt eine elektronische Nachbildung des ASTAT-Fragebogens zur jährlichen Datenerhebung in den Schulen dar. Dabei werden Daten, die bereits in Popcorn vorhanden sind automatisch berechnet und eingefügt (z.B. die Schülerzahlen, Anzahl der Ausländischen Schüler usw.). Andere Daten müssen händisch eingetragen werden, wobei es sich meistens um aggregierte Daten handelt (z.B. Anzahl der Schüler, die vom Religionsunterricht befreit sind (aufgeschlüsselt nach Klassenstufe und Geschlecht), bzw. Daten über die im Schulgebäude verfügbaren Räume (Turnhalle, verschiedene Labors usw.).

Die genauen Felder können aus dem Astat-Fragebogen erhoben werden.

Ansuchen für Schulfürsorge *(Teilrepliziert: d.h. die Daten werden auf die zentrale DB kopiert, aber nicht an andere Schulen weitergegeben)*

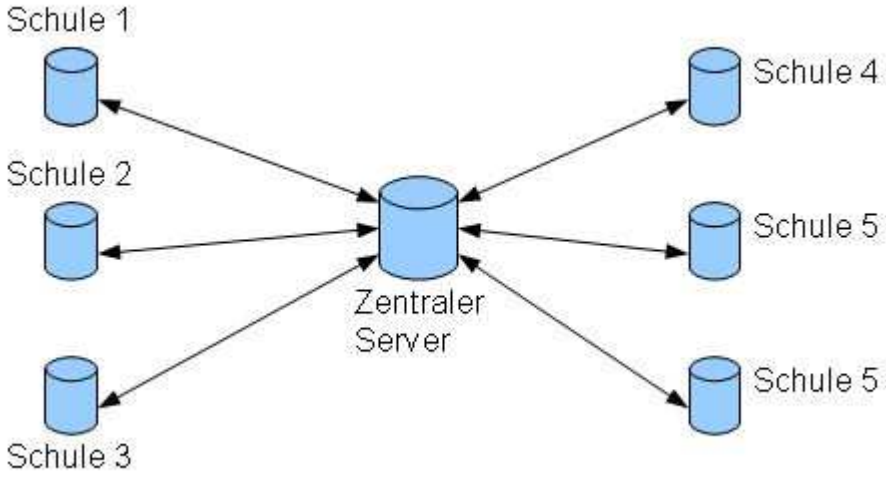
- Eingaben werden pro Schüler gemacht
- 2 Typen:
  - Bewerber die außerhalb der Familie (Heim) leben
  - Alle anderen
- Eventuell Daten des Heimes
  - Mit den Kosten des Heimes
- Finanzelle Situation der Familie des Schülers
  - Zu Lasten lebende Personen
  - Einkommen (Vater, Mutter usw.
  - Vermögenswerte
  - Finanzvermögen
  - Bankkoordinaten des (eines) Erziehungsberechtigten bzw. des Schülers selbst, wenn er bereits 18 Jahre alt ist.

Außendienste *(Teilrepliziert)*

- Pro Lehrer
- Beschreibung
- Spesen (Kassabons) z.B. vom Mittagessen…
- Kilometer (Start-Ziel) wobei die Kilometer zwischen den Orten codiert sind (also nicht frei einzugeben)
  - Asphaltiert nicht asphaltiert
  - Transportmittel
- Datum des Außendienstes (Beginn – Ende)
- Eventuell gewährter Vorschuss
- Anmerkungen der Schule und des Amtes
- Typ des Außendienstes (Ausland, Reduzierte Vergütung, Begleitet Schüler usw…)
- Routenbeschreibung

Workflow – Replikation

Architektur
Grundsätzlich besteht die Datenbank für Popcorn aus einem verteilten System von Datenbanken. D.h. es gibt ca. 130 „lokale" Datenbanken an den Schulen und eine zentrale Datenbank (in Bozen).
Die zentrale Datenbank stellt dabei den Knoten mit allen anderen lokalen DB dar. D.h. eine lokale DB kann nicht direkt mit einer anderen lokalen DB kommunizieren sondern nur mit der Zentralen DB.



Die Daten werden mit der Zentralen DB über die SQL-Replikation des SQL-Servers ausgetauscht. Diese Replikation erfolgt über Nacht. Dabei repliziert jeder lokale Server seine Änderungen auf den zentralen Server und übernimmt die Änderungen aus dem zentralen Server. Die Replikation der Daten erfolgt immer auf Tabellenebene. D.h. es wird Tabelle für Tabelle abgeglichen.

Es gibt:
Vollreplizierte Daten: d.h. die Daten werden Vollständig mit dem zentralen Server ausgetauscht und dieser gibt sie vollständig an die anderen Server weiter.
Teilreplizierte Daten: der lokale Server repliziert nur für ihn bestimmte Daten mit dem zentralen Server. Diese Daten (die normalerweise auf dem lokalen Server entstanden sind, werden nicht auf andere lokale Schulserver weiterrepliziert).
Nicht replizierte Daten: Daten/Tabellen, die nicht auf den zentralen Server kopiert werden.
Nicht replizierte Daten werden falls benötigt mit manuellen Scripts auf den zentralen Server kopiert (z.B. wöchentliche Datensammlung für ASTAT-DWH)

- **Personenbezogenen** Daten (Anagrafische Daten) -> Vollrepliziert
- **Schulbezogenen** Daten (Adresse der Schule usw.) -> Vollrepliziert
- **Schülerbezogenen** Daten (Noten, Fachrichtungen, Einschreibungen, Klassen usw.) ->Voll-, Teil bzw. nicht replizierte Daten (für die genau Auflistung siehe Beschreibung der Datenfelder)

Dokument erstellt von:
Dr. Martin Prosch – Abteilung Informationstechnik

5. Mindestanforderungen Schulen staatlicher Art Check-List

1. Die Schulen müssen den Betroffenen (Inhaber der Daten) die Mitteilungen mit den Beschreibung der Datenverarbeitung und den anderen gefragten Elementen gemäß Art. 13 des Datenschutzkodex zukommen lassen.
2. In der Regel handelt es sich um drei Kategorien physischer Personen: Schüler/Eltern, unterrichtendes und nicht-unterrichtendes Personal, Lieferanten. Die Schulen sollten einen Nachweis dafür aufbewahren, in der Regel unterschrieben mit dem Vermerk „gesehen und angenommen".
3. Die Schulen müssen dem gesamten Schulpersonal detaillierte Beauftragungen zugestellt haben (somit eigentlich an fast alle Bediensteten), welche genau das Arbeitsumfeld und die erlaubten Arbeitsschritte definieren.
4. Auch wenn es sich um eine fakultative Figur handelt, ist es angemessen, eine Ernennung als Verantwortlicher für die Verarbeitung von personenbezogenen Daten vorzunehmen. Diesbezügliche Norm: Art. 29-30 des gesetzesvertretenden Dekretes vom 30.6.2003, Nr. 196.
5. Die Schulen müssen Maßnahmen ergreifen, welche die Authentifizierung und entsprechende Benutzerberechtigungen ermöglichen, und zwar durch persönliche Authentifizierungsmethoden (*username, password*); und zwar für jeden einzelnen Beauftragten unter Beachtung der Punkte 1-14 der Anlage B – Technische Vorschriften im Bereich der Mindestsicherheitsmaßnahmen des gesetzesvertretenden Dekretes vom 30.6.2003, Nr. 196.
6. Die Schulen müssen ihre Anwendungen und Abläufen anpassen (*antivirus, antispy*, usw.), um den Zugang zu ihren Programmen durch Viren, Malware oder Ähnlichem verhindern, um Schaden an Daten, Netz und System abzuwenden. Anlage B – Technische Vorschriften im Bereich der Mindestsicherheitsmaßnahmen des gesetzesvertretenden Dekretes vom 30.6.2003, Nr. 196.
7. Die Schulen müssen ihre Anwendungen und Abläufen anpassen (z.B. *firewals, proxyserver*, usw.) um den Zugang zu ihren Programmen durch Viren, Malware oder Ähnlichem verhindern, um Schaden an Daten, Netz und System abzuwenden. Anlage B – Technische Vorschriften im Bereich der Mindestsicherheitsmaßnahmen des gesetzesvertretenden Dekretes vom 30.6.2003, Nr. 196.
8. Die Schulen müssen ihre Abläufen anpassen, um die Sicherheitskopien sicher aufzubewahren, für die Wiederherstellung und die Verfügbarkeit von Daten und Systemen, im Falle dass diese verloren oder zerstört sind. Anlage B – Technische Vorschriften im Bereich der Mindestsicherheitsmaßnahmen des gesetzesvertretenden Dekretes vom 30.6.2003, Nr. 196. Art. 150 bis des „Codice di Amministrazione digitale".
9. Die Schulen müssen periodisch die Einhaltung der zugewiesenen Anweisungen überprüfen; dies ist Aufgabe des Direktors. Siehe Artikel 29, Absatz 5 des gesetzesvertretenden Dekretes Nr. 196/2003. In Hinblick darauf ist es empfehlenswert, die Ergebnisse der durchgeführten Kontrolle zu protokollieren.

10. Die Schulen müssen periodisch (mindestens einmal jährlich) die den einzelnen Beauftragten erlaubten Verarbeitungen (Punkt 15-27, Anlage B – Technische Vorschriften im Bereich der Mindestsicherheitsmaßnahmen des gesetzesvertretenden Dekretes vom 30.6.2003, Nr. 196.) und eventuelle verschiedene Authorisierungs-Profile für den Zugang zu den Daten in elektronischer Form ((Punkt 14, Anlage B – Technische Vorschriften). Auch in diesem Falle kann es nützlich sein, die Einhaltung der Vorschriften zu protokollieren. Es handelt sich demnach um eine Kontrolle der Aktualität und der Sinnhaftigkeit der zugewiesenen Aufgaben (im Abstand von einem Jahr) und die eventuelle Ergreifung von Korrekturmaßnahmen (z.B. Beauftragung von Personen, die vorher nicht berechtigt waren, oder durch eine systematische Änderung, damit einzelne Mitarbeiter Zugang zu den Daten bekommen).
11. Im Falle, dass an einer Schule Systemadministratoren arbeiten, welche autonom vom Rechtsinhaber ernannt wurden, ist folgende Regelung anzuwenden: Maßnahme der Datenschutzbehörde "**Misure e accorgimenti prescritti ai** titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008".
12. Auf den IT-Systemen, welche im Besitz der Schule sind (didaktisches Netz), ist es zu empfehlen, Systeme für die Protokollierung der Zugänge durch die Systemadministratoren zu installieren (Maßnahme der Datenschutzbehörde "**Misure e accorgimenti prescritti ai** titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008, 4.5").
13. Die Schulen müssen die Ernennungen der externen Verantwortlichen für die Datenverarbeitung im Sinne von Art. 29 des Kodex vornehmen, wann immer die elektronische Verarbeitung von personenbezogenen Daten oder ein Teil der Verarbeitung an Dritte anvertraut wird.
14. Unter den verschiedenen Anforderungen des „Codice di Amministrazione Digitale" (auch CAD, D.lgs.82/2005) ist die Vorschrift einen Plan für die **kontinuierliche Operativität** zu erstellen hervorzuheben (Art. 50 bis).
15. Es wird dringend empfohlen, den Sicherheitsplan (DPS) beizubehalten - auch wenn dies seit 2012 nicht mehr verpflichtend ist - vor allem unter Berücksichtigung der 2014 in Kraft getretenen europäischen Durchführungsbestimmung für den Datenschutz (gilt für alle 27 Mitgliedsstaaten der EU), nach welcher alle öffentlichen und nicht-öffentlichen Verwaltungen verpflichtet sind, geeignete Unterlagen zu erstellen und aufzubewahren, welche das Organisationsmodell und die Sicherungstellung der Privacy nachweisen.
16. Für den Fall, dass Clouds genutzt werden, hat die Datenschutzbehörde entsprechende Richtlinien erstellt, die vor allem in der Fase der Auswahl des Dienstleisters (für die Cloud) und für die Vertragsbedingungen zu berücksichtigen sind (siehe „CLOUD COMPUTING - PROTEGGERE I DATI PER NON CADERE DALLE NUVOLE. La guida del Garante della Privacy per imprese e pubblica amministrazione").
    http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1894503

Redaktion:

Dr. Cristina Motti – Organisationsamt, Dr. Simonetta Maina – Abteilung Informationstechnik

6. Anlagen

A. Anfrage der ASSA

B. Dekret des Unterrichtsministerium vom 7.12.2006, Nr. 305
"Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali»"

Informationsblätter:
Bezeichnung der Verarbeitung und zusammenfassende Beschreibung
Infoblatt Nr. 1 – Selezione e reclutamento e gestione del rapporto di lavoro
Infoblatt Nr. 2 – Gestione del contenzioso e procedimento disciplinare
Infoblatt Nr. 3 – Organismi collegiali e commissioni istituzionali
Infoblatt Nr. 4 – Attività propedeutiche all'avvio dell'anno scolastico
Infoblatt Nr. 5 – Attività educativa, didattica e formativa, di valutazione
Infoblatt Nr. 6 – Scuole non statali
Infoblatt Nr. 7 – Rapporti scuola-famiglia: gestione del contenzioso

C*. Vorlagen für die Ernennungen (Entwürfe) und Richtlinien:*
Redaktion:
dr. Cristina Motti – Organisationsamt
dr. Simonetta Maina – Abteilung Informationstechnik

Nr. 1 - Ernennung des Verwaltungsverantwortlichen zum Verantwortlichen der Datenverarbeitung
Nr. 2 - Ernennung Sekretariatsmitarbeiter und Hilfspersonal zu Beauftragten der Datenverarbeitung
Nr. 2a - Entwürfe Richtlinien Datenschutz für Sekretariatsmitarbeiter
Nr. 2b - Entwürfe Richtlinien Datenschutz für Hilfspersonal
Nr. 3 - Ernennung der Dozenten zu Beauftragten der Datenverarbeitung
Nr. 3a - Entwürfe Richtlinien Datenschutz für Dozenten
Nr. 4 – Ernennung zum externen Verantwortlichen für die Verarbeitung personenbezogener Daten – APB
Nr. 5 – Ernennung zum Systemadministrator (Schulen)
Nr. 6 – Ernennung zum externen Verantwortlichen für die Verarbeitung personenbezogener Daten– Firmen

D. Anhang B - Technische Vorschriften im Bereich der Mindestsicherheits-maßnahmen (Gesetzesvertretendes Dekret Nr. 196/2003)