

## IT-Sicherheit und Datenschutz im Projekt Berliner Schülerdatei

- Die Schülerdatei dient:
  - a) Der verbesserten Schulorganisation,
  - b) der verbesserten Schulentwicklungsplanung sowie
  - c) der Kontrolle und Durchsetzung der Schul- und Berufsschulpflicht.
- Durch eine ganze Reihe — nicht zuletzt bildungspolitisch begründeter — Entwicklungen der letzten Jahre, hat die Datenerfassung und Zulieferung durch die Schulen drastisch zugenommen. Hauptursachen liegen neben der Ressourcensteuerung - die an spezifische Indikatoren wie Lernmittelbefreiung und nicht deutsche Herkunftssprache gekoppelt ist - in der Notwendigkeit, Planungs- und Controllingdaten für das Management und die Weiterentwicklung des Gesamtsystems der Berliner Schulen zu erfassen.
- Ziel der Schülerdatei ist es, eine zuverlässige und einheitliche und vor allem gemeinsame Datengrundlage für diese Zwecke zu schaffen. Bisher besteht eine solche Datengrundlage im Berliner Schulsystem nicht. Schülerdaten werden an und von verschiedenen Stellen zu je eigenen Zwecken nach unterschiedlichen Kriterien gesammelt und ggf. ausgetauscht.
- Dieser Status Quo hat erhebliche Nachteile für alle im Schulsystem beteiligten Bereiche, die Schülerdaten für die Aufgabenerfüllung benötigen. Leidtragend sind nicht zuletzt die Berliner Schulen selbst, die zahlreichen Berichtspflichten an verschiedene Ebenen zu verschiedenen Zeiten und Zwecken unterliegen und dabei dieselben Informationen in unterschiedlichen Formaten und Medien (vom Papierformular bis zu Online-Abfrage) zuliefern müssen. In der Regel können die Schulen selbst mit diesen Datenbeständen für ihren eigenen Aufgaben und Zwecke nicht weiterarbeiten, sondern müssen hierfür eigene Datenbestände und Softwaresysteme pflegen.
- Für die Schulen stellt sich diese Zunahme an Berichtspflichten als „technische Bürokratisierung“ dar, ohne das bisher adäquate integrierte IT-Systeme flächendeckend zur Verfügung gestellt wurden. Für die Verwaltung entsteht die Anforderung systemweit verlässlicher, eindeutiger und jederzeit verfügbarer Datengrundlagen.
- Leitprinzip der zukünftigen Herangehensweise an die Modernisierung der IT in den Berliner Schulen, insbesondere im Verwaltungsbereich und im Informationsaustausch mit der Zentrale und den Bezirken ist deshalb das Prinzip „Daten sollen dort erfasst werden, wo sie entstehen und dort zur Verfügung gestellt werden, wo Sie gebraucht werden“. Nach Möglichkeit soll also eine Doppelerfassung von Daten vermieden werden, einmal eingegebene Daten sollten allen Berechtigten je nach Rolle und in gesetzlich geregelter Art und Weise zur Verfügung stehen.
- Das Projekt Berliner Schülerdatei dient also dazu, für den Bereich der Schülerdaten einen einheitlichen Datenbestand aufzubauen, der eine wesentliche Grundlage für den Aufbau einer IT-Gestützten Schulverwaltungslösung für Berlin bietet. **Aus Sicht der IT-Sicherheit werden durch dieses Vorhaben jedoch auch neue Fragen aufgeworfen: Welche Risiken ergeben sich aus Berlinweit integrierten Datenbeständen für den Datenschutz? Wie können die Systeme technisch aber auch organisatorisch sicher betrieben werden? Welche Grundlagen sind im Berliner Schulsystem für den Betrieb von IT Verfahren für die Verwaltung zu schaffen?**
- Aufgrund der hohen Sensibilität des Themas im Zusammenhang mit der Verarbeitung personenbezogener Daten wurde deshalb auf eine datenschutzfreundliche Ausgestaltung

der Schülerdatei von vorneherein großer Wert gelegt. Es werden ausschließlich diejenigen Merkmale in der Datei erfasst werden, für die ein gesetzlicher Erhebungszweck auch vorliegt. Dem Grundsatz der Datensparsamkeit wird somit genüge getan. Auch werden die Daten nur solange gespeichert, wie es dem Verwendungszweck nach geboten ist.

- Nichtsdestotrotz ist es für die Erreichung der genannten Ziele einer einheitlichen Datenbasis für verschiedene Zwecke unvermeidbar, dass die Daten als Individualdaten in einer Datenbank zusammengeführt werden. Für bestimmte, klar definierte Zwecke (Schule, Bezirk, Zentrale Stelle) stehen diese Individualdaten in den jeweiligen notwendigen Umfängen/Ausschnitten direkt zu Verfügung. Die echten Individualdaten werden auch genutzt werden müssen, um von Seiten der technischen Systemadministration den systemweit verlässlichen Datenbestand sicherzustellen (ein Schüler nur einmal im System), der ja ein Hauptziel des Vorhabens ist. Hier wird auch die eindeutige Schüler-ID zum Trage kommen. Auch die Zentrale Auskunftsstelle wird mit stark eingeschränkten Zugriffsrechten auf diesen Datenbestand zugreifen können.
- Für alle anderen Zwecke werden die Daten nur in aggregierter oder pseudonymisierter Form zur Verfügung gestellt. Pseudonymisierte Schülerdaten werden insbesondere im Bereich von Aufgaben der Schulentwicklungsplanung und Statistik von Relevanz sein. Hierbei ist technisch eine Einwegpseudonymisierung vorgesehen. Es ist auch vorgesehen, die Datenbestände für die Planung streng **getrennt** von dem operativen Individualdatenbestand zu halten, der für die Organisation im engeren Sinne (eindeutige Zuordnung des Schülers zu einer Schule und Unterstützung der Schüler-Aufnahme/-Abgabe) dienen wird. Alle Zugriffe auf die Datenbestände werden über ein rollenspezifisches Berechtigungsmanagement gesteuert, Zugriffe werden protokolliert etc.

**Stark vereinfacht stellt sich das Datenhaltungskonzept wie folgt dar:**

