Dienstvereinbarung über die Nutzung von elektronischen Schließanlagen und Zugangskontrollsystemen

zwischen der

Behörde für Bildung und Sport Hamburg

und dem

Gesamtpersonalrat
für das Personal an staatlichen Schulen

1. Zielsetzung und Allgemeines

1.1 Ziel dieser Vereinbarung ist es, beim Einsatz elektronischer Schließanlagen und elektronischer Zugangskontrollsysteme den Schutz personenbezogener Daten vor unzulässigem Gebrauch und unberechtigtem Zugriff zu gewährleisten.

1.2 Ziel des Einsatzes der elektronischen Schließ- und Zugangskontrollsysteme ist ausschließlich die Erhöhung der Sicherheit für Personen, Anlagen und Gegenstände in den Gebäuden und beim Zugang zu den Gebäuden der Schulen sowie die Erhöhung der Flexibilität gegenüber herkömmlichen Systemen.

1.3 Eine Kontrolle oder Überwachung des Verhaltens von Mitarbeiterinnen und Mitarbeitern findet nicht statt. Die Dienststelle und alle Personen, die die Schließanlage betreuen, sind verpflichtet, die Bestimmungen zum Datenschutz einzuhalten.

2. Geltungsbereich

Die Dienstvereinbarung gilt für alle Mitarbeiterinnen und Mitarbeiter der staatlichen Schulen in Hamburg und wird entsprechend angewendet für alle sonstigen schlüsselberechtigten Raumnutzer der Dienstgebäude der Schulen.

3. Betrieb der Anlage

3.1 Verantwortlich für den Betrieb von elektronischen Schließanlagen ist die Schulleitung.

3.2 Vor Inbetriebnahme einer Schließanlage ist von der Schulleitung ist eine Gefährdungsanalyse nach dem Muster der Anlage 1 aufzustellen. Die Gefährdungsanalyse muss unter Abwägung des Rechts auf informationelle Selbstbestimmung erstellt werden.

3.3 Vor Inbetriebnahme einer Schließanlage ist zudem eine Verfahrensbeschreibung nach § 9 Hamburgisches Datenschutzgesetz (HmbDSG) zu erstellen. Sie kann sich am Muster der Anlage 2 orientieren.

4. Erheben und Verarbeiten von Daten

4.1 Die Zutrittsberechtigungen zu einzelnen Gebäuden und Räumen werden in einer Stammdatei der elektronischen Schließanlage bzw. dem Zugangskontrollsystem geführt. Die Stammdatei ist eine Datei im Sinne des Hamburgischen Datenschutzgesetzes, die vor unbefugter Einsichtnahme zu schützen ist. Eine Verknüpfung dieser Datei mit weiteren Dateien ist nicht zulässig. Die Person, die für die Datenpflege der Stammdatei und die Administration des Programms verantwortlich ist, sowie deren Stellvertretung wird von der Schulleitung nach vorheriger Rücksprache mit dem Personalrat namentlich benannt.

4.2 Die in den Schließanlagen vorhandenen Daten dürfen nur ausgewertet (ausgelesen) werden, wenn es Anhaltspunkte für einen strafrechtlich relevanten Tatbestand gibt oder die

Funktionsfähigkeit überprüft werden soll. Die Auswertung dient im Übrigen ausschließlich der Klärung des konkreten Anlasses. Über jede Auswertung wird ein Protokoll erstellt, das einen Ausdruck der im Schließsystem vorhandenen elektronischen Daten umfasst. Protokolle, die für die Strafverfolgung benötigt werden, sind an einem sicheren Ort aufzubewahren. Die sonstigen Protokolle sind binnen vier Wochen zu löschen bzw. zu vernichten.

4.3 Eine Weitergabe der gespeicherten Daten ist nur durch die Schulleitung im Rahmen der Zweckbestimmung zulässig.

4.4 Daten, die vier Wochen lang nicht zur Verfolgung von strafrechtlich relevanten Tatbeständen benötigt wurden, sind unverzüglich zu löschen.

4.5 Eine notwendige Auswertung erfolgt durch die Schulleitung oder eine von der Schulleitung konkret benannte Person sowie eine vom Personalrat konkret benannte Person mittels eines besonderen zweigeteilten Kennwortes (Passwort). Das geteilte Kennwort ist zur einen Hälfte der Schulleitung oder der benannten Person und zur zweiten Hälfte dem Personalrat bekannt.

Zur schnelleren Verfügbarkeit an Wochenenden, Feiertagen und in unterrichtsfreien Zeiten wird bei der Dienstellenleitung die Passworthälfte des Personalrats in einem verschlossenen Umschlag hinterlegt. Bei Öffnung des Umschlages ist die Schulleitung verpflichtet, den Personalrat sofort bzw. am nächsten Werktag zu benachrichtigen.

4.6 Ergibt eine Auswertung Anhaltspunkte dafür, dass Bedienstete an einer Handlung, die zu einer notwendigen Auswertung (s. Punkt 4.2) geführt hat, beteiligt sein könnten, ist der zuständige Personalrat unverzüglich zu informieren. Er erhält auf Wunsch des Bediensteten ein Einsichtsrecht in die gespeicherten Daten.

5. Rechte der Mitarbeiterinnen und Mitarbeiter

5.1 Alle betroffenen Mitarbeiterinnen und Mitarbeiter werden rechtzeitig umfassend und in geeigneter Weise durch die Schulleitung über die Wirkungsweise des Systems (z.B. Verwendung ihrer Daten und die Auswertungsmöglichkeiten) informiert.

5.2 Die Beschäftigten sind für den bestimmungsgemäßen Gebrauch ihres Schlüssels verantwortlich. Der Schlüssel darf nicht weitergegeben werden und nicht benutzt werden, um Unbefugten den Zutritt/Zugang zu ermöglichen.

5.3 Die Beschäftigten sind verpflichtet, der Gebäudeverwaltung den Verlust ihres Schlüssels unverzüglich mitzuteilen, damit die Zutrittsberechtigung schnellstmöglich gelöscht werden kann.

6. System

Die Dienststelle informiert den Schulpersonalrat bei Um– und Ausbau der Schließanlage, mindestens aber einmal jährlich über den technischen Stand der Schließanlage.

7. Altanlagen

Die Dienstvereinbarung findet auch auf bereits in Betrieb genommene Schließanlagen Anwendung. Für sie sind nach Bekanntgabe der Dienstvereinbarung, sofern nicht bereits geschehen, die Gefährdungsanalyse nach Punkt 3.2 sowie die Verfahrensbeschreibung gemäß § 9 HmbDSG nach Punkt 3.3 unverzüglich, spätestens innerhalb von drei Monaten, nachzuholen.

8. Schlussbestimmungen

8.1 Die Dienstvereinbarung tritt am Tag der Unterzeichnung in Kraft.

8.2 Die Kündigung der Vereinbarung bedarf der Schriftform. Sie kann mit einer Frist von sechs Monaten zum Ende eines Schuljahres gekündigt werden; im Fall der Kündigung bleibt sie wirksam, bis sie durch eine neue Dienstvereinbarung ersetzt wird.

Hamburg, den 11.12.2007

Für die Dienststelle	Für den Personalrat
gez. Schuster	gez. Voß

Anlage 1 zur

Dienstvereinbarung über die Nutzung von elektronischen Schließanlagen und Zugangskontrollsystemen, § 8 Abs. 4 Hamburgisches Datenschutzgesetz

Gefährdungsanalyse

Da die Installation einer elektronischen Schließanlage einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen kann, muss kritisch abgewogen werden, ob das eingeschätzte Gefährdungspotential und die Erhöhung der Flexibilität, die mit der Installation einer elektronischen Schließanlage einhergeht, die Installation einer Schließanlage tragen.

Bitte beantworten Sie die nachstehenden Fragen und notieren Sie die Antworten in einem kurzen Protokoll:

1. Welches Türöffnungssystem soll verwendet werden?
2. Welche Türen sollen mit elektronischen Schlüsseln ausgerüstet werden?
3. Wer hält sich üblicherweise in den entsprechenden Räumen auf?
4. Sind in diesem Bereich in der Vergangenheit Straftaten begangen worden oder Unregelmäßigkeiten in Bezug auf die Sicherheit für Personen, Anlagen oder Gegenständen aufgetreten?
5. Welcher Art waren die Straftaten oder Unregelmäßigkeiten?
6. Wie hoch war der Schaden?
7. Wenn in der Vergangenheit keine Straftaten begangen oder Unregelmäßigkeiten festgestellt wurden: welches sind die Gründe für den Einsatz von elektronischen Schlüsseln?
8. Wer wartet und pflegt die Anlage?
9. Wo und wie werden die Speichermedien gesichert?
10. Wie sieht der „Notfallplan“ aus, was soll im Fall eines Vorkommnisses durch wen geschehen?

Anlage 2 zur

Dienstvereinbarung über die Nutzung von elektronischen Schließanlagen und Zugangskontrollsystemen, § 9 Hamburgisches Datenschutzgesetz

Verfahrensbeschreibung

Muster bei Verwendung von Seccor- bzw. Simons-Voss-Schließtechnik

1. Name und Anschrift der Daten verarbeitenden Stelle	Schulname, Adresse
2.1 Bezeichnung des Verfahrens	Zutrittsverwaltung zu schulischen Gebäuden durch elektronisches Schließsystem und elektronische Zutrittsprotokollierung
2.2 Zweckbestimmung des Verfahrens	Zutrittskontrolle, um die Sicherheit für Personen, Anlagen und Gegenstände in den Schulgebäuden zu erhöhen
3.1 Art der verarbeiteten Daten	a. Bei Transponderschließsystem Simons-Voss, Software LDB XX *[Hinweis an Schulleitung: Hier bitte die Version angeben]*, Auslesung mittels PalmCD2, Zutrittsprotokollierung: • Daten in der Schließung (Türschloss): Name und Ident-Nummer der Schließanlage, Name und Ident-Nummer der Schließung (=Schloss); Zutrittsliste: Vor- und Nachname des Transponderbesitzers, Ident-Nummer des Transponderbesitzers, Datum und Uhrzeit des Zutritts an der jeweiligen Schließung • Daten im Transponder: Vor- und Nachname des Transponderbesitzers, Ident-Nummern ihrer Transponder, ggf. Aktivierungs- und Deaktivierungsdatum des Transponders (Gültigkeitsdauer), ggf. Zeitbegrenzung für Transponder (bei begrenzter berechtigter Zutrittsdauer), Anzahl der Schließanlagenberechtigungen (Liste der Räume, die mittels Transponder betreten werden können) • Daten im PalmCD2: wie Daten in Schließung bzw. Transponder • Daten auf Verwaltungs-PC: wie vor b. Bei Schließsystem Seccor Schlüsselverwaltung, Softwareversion XX [*Hinweis an Schulleitung: Hier bitte die Version angeben]* auf Verwaltungs-PC und Transfergerät: • Daten in der Schließung: Zutrittsdatum, Schlüsselcode • Daten im Transponder: wie vor, zusätzlich Name der Schließung • Daten im Transfergerät: wie vor • Daten in Übersichtsmatrix auf Verwaltungs-PC: Vor- und Nachname der Schließberechtigten, Name der Schließung, Schlüsselcode
3.2 Rechtsgrundlage	Für Mitarbeiterinnen und Mitarbeiter der Schule: Dienstvereinbarung (DV) Schließanlagen i.V.m. § 28 Abs. 1 Satz 1 HmbDSG Für andere schlüsselberechtigte Personen: Einwilligungserklä-

	rung vom ___ *[Hinweis an Schulleitung: Hier bitte die Einwilligungserklärungen der jeweiligen externen Schlüsselberechtigten angeben],* § 5 Abs. 1 Nr. 2 HmbDSG
4. Kreis der Betroffenen	Zutrittsberechtigte Lehrkräfte, zutrittsberechtigtes nichtpädagogisches Personal, weitere schlüsselberechtigte Personen (externe Nutzer)
5. Empfänger/innen der Daten	
5.1 Empfangende dritte Stellen	Bei Anhaltspunkten für strafrechtlich relevanten Tatbestand: Ermittlungsbehörden
5.2 Auftragsdatenverarbeiter	entfällt
5.3 Empfänger/innen innerhalb der Daten verarbeitenden Stelle, die andere Aufgaben wahrnehmen	Schulleitung bzw. die von der Schulleitung benannte Person, eine vom Personalrat benannte Person
6. Datenübermittlung nach § 17 Abs. 2 und 3 HmbDSG (Übermittlung an Drittländer)	entfällt
7.1 Fristen für die Sperrung der Daten	entfällt
7.2 Fristen für die Löschung der Daten	Zutrittsdaten in Schließung, Transponder und Transfergerät: spätestens vier Wochen ab Erhebung (Nr. 4.4 der DV Schließanlagen) bzw. früher durch automatische Überschreibung mit jüngeren Zutrittsdaten; Daten einzelner Zutrittsberechtigter in Stammdatei: Bei Rückgabe des Transponders
8. Technische und organisatorische Maßnahmen nach § 8 HmbDSG	• Gewährleistung der Vertraulichkeit: dass nur Befugte die personenbezogenen Daten zur Kenntnis nehmen können, wird durch die Verwendung eines automatisierten Systems mit Verschlüsselungstechnik sowie dadurch gewährleistet, dass die Datenauswertung nur unter Anwendung eines zweigeteilten Kennwortes, dessen eine Hälfte der Schulleitung, die andere dem Personalrat vorliegt, erfolgen kann (Nr. 4.5 der DV) • Gewährleistung der Integrität der Daten: die personenbezogenen Daten bleiben während der Verarbeitung unverfälscht, vollständig und widerspruchsfrei, da sie automatisiert unter Einsatz von Verschlüsselungstechnik im elektronischen Schließsystem verarbeitet werden. • Gewährleistung der Verfügbarkeit der Daten: die personenbezogenen Daten stehen zeitgerecht zur Verfügung und werden ordnungsgemäß verarbeitet, da die Systemtechnik automatisiert und unter Verwendung von Schlüsselberechtigungen arbeitet sowie die Auswertung der Daten an ein zusätzliches, zweigeteiltes Kennwort gebunden ist (s.o.). • Gewährleistung der Authentizität: die personenbezogenen Daten können ihrem Ursprung zugeordnet werden, da ihr Übertragungsweg ab der Registrierung der Daten einzelner Schlüsselberechtigter automatisiert im Schließsystem verläuft. Eingriffe in die Übertragungskette sind auch bei der anlassbezogenen Auswertung der Daten nicht möglich, da insoweit Schulleitung und Personalrat nur gemeinsam mit einem zweigeteilten Kennwort vorgehen können.

	• Gewährleistung der Revisionsfähigkeit der Daten: es kann festgestellt werden, wer wann welche Daten wie verarbeitet hat, da nach Nr. 4.2 der DV Schließanlagen über jede Auswertungsvorgangs ein Protokoll erstellt wird.
9.1 Art der Geräte	Bei Transponderschließsystem Simons-Voss: elektronische Schließung, Transponder, PalmCD2, PC Bei Schließsystem Seccor Schlüsselverwaltung, Softwareversion 4.4: elektronische Schließung, Transponder, Transfergerät, PC
9.2 Verfahren zur Übermittlung, Sperrung, Löschung, Auskunftserteilung und Benachrichtigung	• Übermittlung: Die Übermittlung der Daten an die Ermittlungsbehörden erfolgt nur bei Anhaltspunkten für strafrechtliche Tatbestände; • Sperrung: entfällt • Löschung: die Löschung der Daten erfolgt automatisiert durch Überschreibung früherer Daten bzw. händisch nach Ablauf der in Nr. 7.2 angegebenen Löschungsfristen • Auskunftserteilung: Verantwortlich für die Auskunftserteilung nach § 18 HmbDSG ist die Schulleitung bzw. eine von der Schulleitung benannte Person. Anträge auf Auskunftserteilung über die in der Schule vorgehaltenen personenbezogenen Daten im Zusammenhang mit den Schließanlagen sind schriftlich an die Schulleitung zu richten. Die Entscheidung über eine teilweise oder vollständige Versagung der Auskunft nach § 18 Absatz 3 HmbDSG trifft die Schulleitung oder die von ihr benannte Person. Die Auskunft wird schriftlich erteilt. Soweit die Auskunftserteilung ganz oder zum Teil versagt wird, unterrichtet die Schulleitung die Antragstellerin oder den Antragsteller schriftlich über den Grund der Versagung.