GEMEINDE
ZUFIKON

Datensicherheitskonzept Videoüberwachung Schule Zufikon

Gültig ab 1. Januar 2024

Inhaltsverzeichnis

1. Zweck der Datensicherheit, Schutzziele und Risiken

Eine Videoüberwachung, bei der Personen erkennbar oder ohne übermässigen Aufwand bestimmbar sind, stellt einen schweren Eingriff in die verfassungsmässig geschützten Grundrechte auf Privatsphäre und auf informationelle Selbstbestimmung dar und ist darum strengen Regeln unterworfen.

Personendaten müssen durch angemessene organisatorische und technische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (§ 12 IDAG). Bei der elektronischen Bearbeitung von Personendaten sind zur Einhaltung der Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit sowie der Löschfristen technische und organisatorische Massnahmen umzusetzen (§ 4 VIDAG) und entsprechend zu dokumentieren (§ 5 Abs. 1 VIDAG). Dabei richten sich die Massnahmen nach dem Zweck, der Art und dem Umfang der Datenbearbeitung sowie den möglichen Gefahren für die Persönlichkeitsrechte betroffener Personen (§ 4 Abs. 2 VIDAG).

Der folgende Abschnitt gilt für Videoüberwachungsanlagen, die keine polizeilichen Echtzeitüberwachungen darstellen:

Für die Videoüberwachungsanlagen, deren Sicherheit mit dem vorliegenden Datensicherheitskonzept gewährleistet werden soll, sind effektiv nur diejenigen Bereiche relevant, die direkt oder mittelbar die Vertraulichkeit der bearbeiteten Daten sicherstellen; bei der Videoüberwachung handelt es sich nicht um die Kernaufgabe einer öffentlichen Verwaltung, sondern um eine zusätzliche Möglichkeit, den allgemeinen Auftrag des Erhalts der Sicherheit und der Werterhaltung des Verwaltungsvermögens sicherzustellen. Hohe Verfügbarkeitsanforderungen an ein Überwachungssystem entstehen dadurch bzw. aus Datensicherheitsüberlegungen nicht, ebenso wenig wie qualitative Integritäts- oder ähnliche Anforderungen. Die Anforderungen an die Vertraulichkeit sind erhöht. Als Besonderheit ist sicherzustellen, dass die Auswertung nur durch die gemäss Anhang zum Reglement berechtigten Personen erfolgt und die Auswertung nur dann erfolgt, wenn ein Auswertungsgrund gemäss Reglement vorliegt. Aus diesem Grund ist für Zugriffe auf gespeicherte Aufnahmen eine Protokollierung vorzusehen.

2. Technische und organisatorische Massnahmen zur Eindämmung der Bedrohungen (§ 4 Abs. 1 VIDAG)

Die technischen und organisatorischen Massnahmen richten sich nach den erkannten Bedrohungen und Gefahren für die Persönlichkeit der betroffenen Personen. Die Systematik der hier dargestellten Massnahmen folgt dabei jener gemäss § 4 Abs. 1 VIDAG.

Massnahme	Beschreibung	Umsetzung
Zugangskontrolle (§ 4 Abs. 1 lit. a)	Zugangskontrollen reduzieren das Risiko, dass sich unbefugte Personen Zugang zu Einrichtungen, in denen Personendaten verarbeitet werden, verschaffen.	- Nur autorisierte Mitarbeitende haben Zugang zu Räumen, in denen sich die Aufnahmegeräte befinden. - Die baulichen Massnahmen, welche den Zutritt zum Raum, in dem die Personendaten der Videoüberwachung gespeichert werden, werden jährlich überprüft und bei Bedarf angepasst. - Die Protokollierung der Zutritte wird sichergestellt, unveränderbar aufbewahrt und mindestens jährlich überprüft. - Die Zutrittsrechte werden jährlich auf ihre Korrektheit überprüft. - Der Zugang zum Rack indem sich der Videoserver befinden, ist mit einem Schlüssel-Tresor ausgestattet.
Datenträgerkontrolle (§ 4 Abs. 1 lit. b)	Datenträgerkontrollen reduzieren das Risiko, dass unbefugte Personen Daten von mobilen Datenträgern (USB, externe Festplatten etc.) lesen, kopieren, verändern oder entfernen.	- Daten der Videoüberwachung werden auf Datenträgern abgespeichert, um das Lesen und das Verändern der Videodaten durch unbefugte Personen zu verunmöglichen sind die Daten mit einem Hologramm auf jedem Bild gespeichert UVV Kassen Zertifiziert. Über die IVMS Software verfügen nur befugte Personen Zugang zu Videodaten. Bei Transport muss der USB Stick mit einem Passwort geschützt sein. z.b. mit BitLocker. Aufgrund des Passwortschutzes werden keine weiteren Massnahmen gegen das Kopieren oder Entfernen von Datenträgern vorgesehen. Es wird sichergestellt, dass der Zugriff auf sensitive Informationen auf Datenträgern nicht möglich

		ist, wenn diese entsorgt oder einem anderen Zweck übertragen werden. Es wird sichergestellt, dass als gelöscht markierte oder zur Entsorgung bestimmte Daten nicht wiedergewonnen werden können.
Transportkontrolle (§ 4 Abs. 1 lit. c)	Transportkontrollen reduzieren das Risiko, dass beim Transport von Personendaten über ein IT-Netzwerk die Daten von unbefugten Personen gelesen, kopiert, verändert oder gelöscht werden können.	- Die Videoüberwachung befindet sich in einem separaten Netzwerk VLAN der Schule ohne Anschlussmöglichkeiten an ein weiteres Netzwerk. Der Zugang zum Videoserver ist Passwortgeschützt.
Bekanntgabekontrolle (§ 4 Abs. 1 lit. d)	Bekanntgabekontrollen reduzieren das Risiko, dass Datenempfänger identifiziert werden können und die Personendaten nicht an unbefugte Personen gesendet werden.	- Bevor eine Übertragung von Videodaten erfolgt (z.B. an die Polizei), wird der Datenempfänger identifiziert. Datenübertragungen werden protokolliert und revisionsgerecht für mindestens ein Jahr aufbewahrt.
Speicherkontrolle (§ 4 Abs. 1 lit. e)	Speicherkontrollen reduzieren das Risiko, dass unbefugte Personen Eingaben in den Speicher (Serverfestplatten, netzgebundener Speicher/NAS etc.) sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten vornehmen können.	- Die Daten der Videoüberwachung werden im Logfile protokoliert für Zugriff auf (Live und Wiedergabe der Bilder) und in Metadaten abgespeichert mit Zeit und Datum, um das Lesen und das Verändern der Videodaten durch unbefugte Personen zu verunmöglichen. Aufgrund des Passwortschutzes werden keine weiteren Massnahmen gegen das Kopieren oder Entfernen von Datenträgern vorgesehen. - Es wird sichergestellt, dass der Zugriff auf sensitive Informationen auf Datenspeichern nicht möglich ist, wenn diese entsorgt oder zu einem anderen Zweck verwendet werden. Es wird sichergestellt, dass als gelöscht markierte oder zur

		Entsorgung bestimmte Daten nicht wiedergewonnen werden können.
Benutzerkontrolle (§ 4 Abs. 1 lit. f)	Benutzerkontrollen reduzieren das Risiko, dass unbefugte Personen automatisierte Datenverarbeitungssysteme mittels Einrichtungen zur Datenübertragung / Remote-Zugriffe (Fernzugriffe) benutzen können.	- Es finden keine eingerichteten Remote-Zugriffe auf den Computer oder Datenträger, auf welchem die Videodaten gespeichert werden, statt.
Zugriffskontrolle (§ 4 Abs. 1 lit. g)	Zugriffskontrollen reduzieren das Risiko, dass unbefugte Personen auf Personendaten zugreifen können. Der Zugriff auf Programme und Daten ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen.	- Der Zugriff wird auf die im Anhang zum Reglement bezeichneten Benutzergruppen beschränkt und die Auswertung nur dann erfolgt, wenn ein Auswertungsgrund gemäss Reglement vorliegt. Aus diesem Grund ist für Zugriffe auf gespeicherte Aufnahmen eine Protokollierung vorzusehen. - Der Zugriff eines Benutzers auf die Videodaten wird auf diejenigen Personendaten beschränkt, welche für die Erfüllung einer Aufgabe benötigt werden. - Die Zugriffsrechte werden jährlich auf ihre Korrektheit überprüft. - Alle Standard-Passwörter sind durch neue ersetzt. - Ein komplexes, langes Passwort vorzusehen
Eingabekontrolle (§ 4 Abs. 1 lit. h)	Eingabekontrollen reduzieren das Risiko, dass nicht nachvollzogen werden kann, welche Person Daten eingegeben hat. In elektronischen Systemen muss nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden.	- Es werden keine Personendaten manuell erfasst. Das Videoaufzeichnungssystem zeichnet das Datum und die Uhrzeit automatisch auf. Die Videodaten und die Protokollierung im Logfile von Zugriffen können nicht manuell verändert oder gelöscht werden.

Wiederherstellung (§ 4 Abs. 1 lit. i)	Das Risiko, dass Personendaten verloren gehen, soll reduziert werden. Es soll gewährleistet werden, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.	- Auf Massnahmen für eine Wiederherstellung der Daten wird aus Kostengründen verzichtet. Das Restrisiko eines Datenverlustes wird vom verantwortlichen Organ getragen. - Die Videoserver haben keine RAID Speicherung.
Zuverlässigkeit (§ 4 Abs. 1 lit. j)	Das Risiko von Systemausfällen und Beschädigung von Daten soll reduziert werden. Die Zuverlässigkeit / Integrität der Personendaten soll gewährleistet werden. Alle Funktionen des Systems sollen zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können.	- Es wird periodisch überprüft, ob der Hersteller neue Sicherheits-Patches zur Verfügung stellt. Sicherheits-Patches werden zeitnah installiert. - Das Videoüberwachungssystem meldet auftretende Fehlfunktionen (z.B. sich häufende Schreib- oder Lesefehler via Signalton und Protokoliert dies im Logfile). Die ganze Schule ist mit einem Brandmeldesystem ausgestattet um Schäden mit Feuer früh zu erkennen. Um eine möglichst hohe Sicherheit und Integrität der Daten sicherzustellen.

3. Aktualisierung

Die in diesem Konzept vorgesehenen Massnahmen orientieren sich nach dem Zweck, der Art und dem Umfang der Videoüberwachung sowie den möglichen Gefahren für die Persönlichkeitsrechte betroffener Personen. Sie sind periodisch (insbesondere bei Änderungen an der Hard- oder Software) auf ihre Zweck- und Verhältnismässigkeit hin zu überprüfen und den technischen Entwicklungen anzupassen.

Vom Gemeinderat beschlossen an der Sitzung vom 13. November 2023.

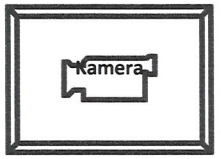
NAMENS DES GEMEINDERATES

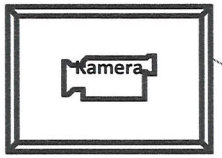
Der Gemeindeammann, Daniel Stark

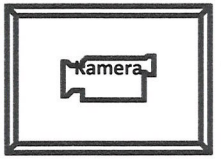
Der Gemeindeschreiber, Uwe Krzesinski

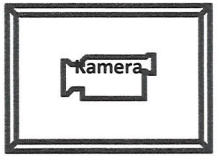
Anhang 1 zum Datensicherheitskonzept vom 31.10.2023

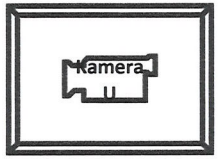
Systemschema Videoüberwachung Schulhaus B Gemeinde Zufikon

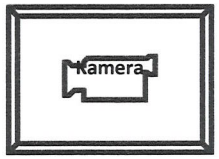




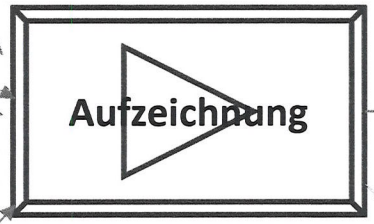








Übertragung der Daten ist verschlüsselt:
Nein / Analoge Kamera



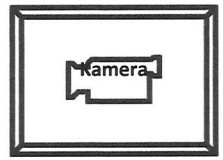
Speicherort UG,
Speicherung
der Daten ist
verschlüsselt:
Nein / Passwortgeschützt

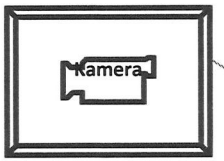
Übertragung
der Daten ist
verschlüsselt:
Nein / Passwortgeschützt

Auswertung von Aufzeichnungen

Speicherort, Speicherung der Daten ist verschlüsselt und mit sicherem Passwort oder zusätzlicher Authentisierung geschützt :
Nein / Software und Passwortgeschützt

Systemschema Videoüberwachung Schulhaus A Gemeinde Zufikon





Übertragung der Daten ist verschlüsselt:
Nein / Analoge Kamera

Speicherort UG,
Speicherung
der Daten ist
verschlüsselt:
Nein / Passwortgeschützt

Übertragung
der Daten ist
verschlüsselt:
Nein / Passwortgeschützt

Auswertung von Aufzeichnungen

Speicherort, Speicherung
der Daten ist verschlüsselt und
mit sicherem Passwort oder zu-
sätzlicher Authentisierung ge-
schützt :
Nein / Software und Passwort-
geschützt