Rheinfelden
Lebenswert. Liebenswert.

23. Mai 2022
Ref. pa

Stadtverwaltung Rheinfelden
Marktgasse 16, Rathaus
4310 Rheinfelden

Hauptnummer: +41 61 835 52 22
informatik@rheinfelden.ch

Patrick Antonetty
Tel: +41 61 835 52 85
patrick.antonetty@rheinfelden,ch

Stadtverwaltung Rheinfelden, Marktgasse 16, Rathaus, 4310 Rheinfelden

Datensicherheitskonzept Videoüberwachung Stadtverwaltung Rheinfelden

Stand vom 01.05.2022

für folgende Standorte gemäss Reglement Videoüberwachung vom 30 November 2020, Anhang in der Fassung vom 30. November 2020

- Schul- und Sportanlage Schützenmatt
- Schulanlage Engerfeld
- Parkplatz Schützenweg
- Parkplatz Storchennest
- Unterflursammelstelle Schützenweg
- Unterflursammelstelle Migros
- Parkhaus Rheinparking
- Schulanlage Robersten
- Bahnhof Rheinfelden: Rosenau, Bahnhof Süd, Unterflur Rosenau, Veloparkplatz SBB

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[1]). 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[2]) 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).

Die Videoanlage der Stadtverwaltung Rheinfelden wird nicht für polizeiliche Echtzeitüberwachungen verwendet. Ein Zugriff auf die Videobilder erfolgt jeweils im Ereignisfall durch die im Anhang des Reglements berechtigten Personen. Die Zugriffe werden in speziell dazu zur Verfügung gestellten elektronischen Formularen protokolliert und zentral gesammelt und aufbewahrt.

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.

[1] Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006 (SAR 150.700).

[2] Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG) vom 26. September 2007 (SAR 150.711).

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 das Aufnahmegerät befindet. - Die baulichen Massnahmen, welche den Zutritt zum Raum, in dem die Personendaten der Videoüberwachung gespeichert werden, werden laufend überprüft und bei Bedarf angepasst. - Die Protokollierung der Zutritte wird im Ereignisfall sichergestellt und unveränderbar aufbewahrt. Dazu werden Protokolldaten des elektronischen Schliesssystems verwendet. - Die Zutrittsrechte werden laufend auf ihre Korrektheit überprüft. - Der Raum wird mittels Alarmanlage vor unberechtigtem oder gewaltsamen Zutritt gesichert
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.	- Die Daten der Videoüberwachung werden auf nicht mobilen Datenträgern unverschlüsselt abgespeichert. Der Datenträger, auf welchem die Videodaten gespeichert sind, wird unter Verschluss aufbewahrt. Über Schlüssel zum Aufbewahrungsort verfügen nur befugte Personen. - Die Daten werden nach 7 Tagen automatisch gelöscht und können danach nicht mehr wiederhergestellt werden. - Im Ereignisfall werden die Daten auf demselben Datenträger durch die auswertende Person für eine durch sie definierte Zeitperiode auf 'legal hold' gesetzt so dass sie vor versehentlicher automatischer Löschung geschützt sind. - Im Anzeigefall an die Staatsanwaltschaft oder den Gemeinderat kann eine Kopie auf einem mobilen Datenträger erstellt werden. - Die Datenträger werden nach Ablauf ihres Lebenzyklus durch spezialisierte Unternehmen nach internationalen Standards entsorgt, so dass darauf befindliche 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,	- Die Daten der Videoüberwachung stehen der auswertenden Person während der Untersuchung im Ereignisfall über eine verschlüsselte Netzwerk Verbindung innerhalb des internen Verwaltungsnetzes 'online' zur Verfügung. Es findet dabei kein Transport von physischen Datenträgern statt. - Bei Anzeige einer Straftat an die Staatsanwaltschaft oder einer Ordnungswidrigkeit an den Gemeinderat

	kopiert, verändert oder gelöscht werden können.	kann die auswertende Person zur Beweissicherung eine Kopie auf einen mobilen Datenträger erstellen und diesen dem Empfänger persönlich übergeben. Die Daten der Videoüberwachung werden während dem beschriebenen Transport nicht verschlüsselt abgespeichert. - Die Kopie, der Transport und die Übergabe werden protokolliert.
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, wird der Datenempfänger identifiziert und dessen Rechtmässigkeit des Datenempfangs geprüft. Datenübertragungen werden protokolliert.
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 auf Datenspeicher nicht verschlüsselt abgespeichert. - Der Datenspeicher, auf welchem die Videodaten gespeichert sind, wird in einem separaten abschliessbaren Rack aufbewahrt. Schlüssel zum Rack haben nur befugte Personen. Zugriffe auf Videodaten werden elektronisch oder manuell protokolliert: a) Zugriffe von Systemadministratoren b) Zugriffe von Nutzenden zur 1. Authentifizierung und Autorisierung, 2. Dateneinsicht, 3. Datenübermittlung Die Protokolle werden während mindestens einem Jahr revisionsgerecht festgehalten.
Benutzerkontrolle (§ 4 Abs. 1 lit. f)	Benutzerkontrollen reduzieren das Risiko, dass unbefugte Personen automatisierte Datenverarbeitungssysteme mittels Einrichtungen zur Datenübertragung / Remote-Zugriffe (Fernzugriffe) benutzen können.	- Das Videosystem steht ausschliesslich Benutzern zur Verfügung, welche im internen zentralen Benutzerverzeichnis registriert (Active-Directory) und als Mitglieder der dafür notwendigen Sicherheitsgruppen eingetragen sind (Security-Groups). - Ein standardisierter Prozess über Änderungen in diesem Verzeichnis und dessen Gruppen (z.B. durch Aus- und Eintritte von Mitarbeitenden) ist eingerichtet.
Zugriffskontrolle (§ 4 Abs. 1 lit. g)	Zugriffskontrollen reduzieren das Risiko, dass unbe-	- Der Zugriff wird auf die im Anhang zum Reglement bezeichneten Benutzergruppen beschränkt.

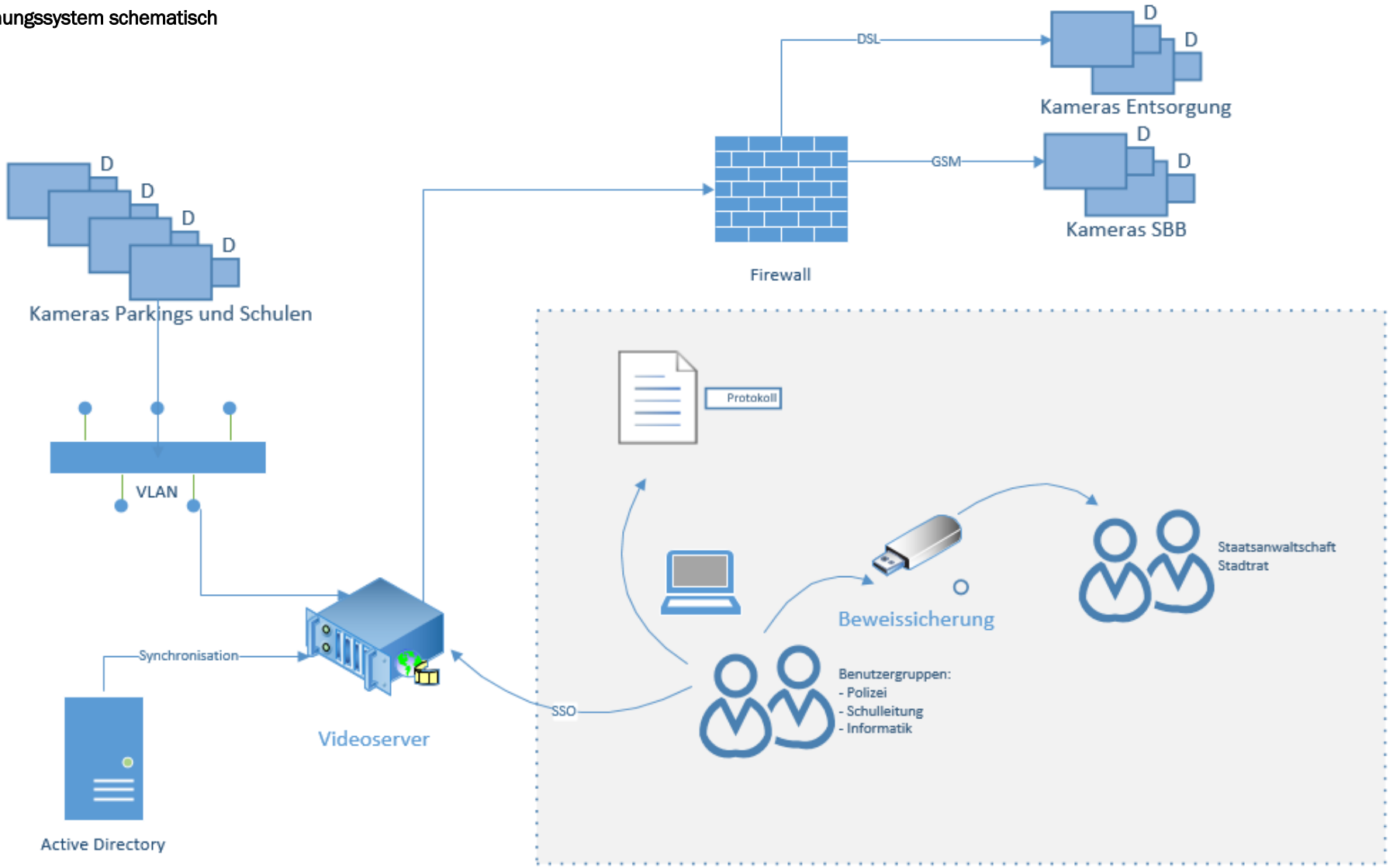
	fugte Personen auf Personendaten zugreifen können. Der Zugriff auf Programme und Daten ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen.	- Der Zugriff eines Benutzers auf die Videodaten wird auf diejenigen Personendaten beschränkt, welche für die Erfüllung einer Aufgabe benötigt werden. - Die Zugriffsrechte werden laufend auf ihre Korrektheit überprüft. - Alle Standard Passwörter werden durch neue ersetzt. - Zugriffe von ausserhalb des internen Netzwerkes – beispielsweise aus dem HomeOffice – werden durch 2 Faktor Authentifizierung geschützt. - Die Benutzer haben ausschliesslich Zugriff auf Videodaten der ihnen zugeordneten Kameras. - Es wird unterschieden zwischen dem Zugriff auf Live Videodaten und dem Zugriff auf in der Vergangenheit aufgenommenen Daten
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.
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.	Die Massnahmen für eine Wiederherstellung der Daten beschränken sich auf die Installation einer redundanten Anordnung von unabhängigen Festplatten. Es werden keine Backups erstellt. Das Risiko eines allfälligen Datenverlustes wird getragen.
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 ge-	Das Videoüberwachungssystem meldet auftretende Fehlfunktionen oder Anomalien an ein automatisiertes Monitoring System, welches darauf eine Störungsmeldung an das interne Informatik Team auslöst. Die gemeldeten Störungen werden innerhalb der Bürozeiten der Verwaltung bearbeitet.

	meldet werden und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können.	

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.

Videoaufzeichnungssystem schematisch



Rheinfelden, 25.05.2022

Digital
unterschrieben von
Patrick Antonetty
(Qualified Signature)
Datum: 2022.06.20
12:47:39 +02'00'

Patrick Antonetty
Leiter Informatik