reinach.ag

Datensicherheitskonzept Videoüberwachung Reinach AG

(Stand vom 10.03.2022)

für folgende Standorte gemäss Reglement Videoüberwachung vom 10.03.2022, Anhang (in der Fassung vom 20.11.2023)

- Pfrundmatt1-Nord
- Pfrundmatt1-Süd
- Pfrundmatt1-West

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).

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.	- Es findet keine Zugangskontrolle statt - Die Netzwerkverteilung und der Videoserver befinden sich in einem separat abschliessbaren Rack. - Zugang zum Inhalt des Rack haben nur zuständige Personen - Die Protokollierung der Zutritte wird sichergestellt, unveränderbar aufbewahrt und mindestens jährlich überprüft. - Die Zutrittsrechte sind jährlich auf ihre Korrektheit zu überprüfen
Datenträgerkontrolle (§ 4 Abs. 1 lit. b)	Datenträgerkontrollen reduzieren das Risiko, dass unbefugte	- Es werden keine Daten der Videoüberwachung auf Datenträgern abgespeichert

[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).

	Personen Daten von mobilen Datenträgern (USB, externe Festplatten etc.) lesen, kopieren, verändern oder entfernen.	
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 findet in einem separaten Netzwerk ohne Anschlussmöglichkeiten an ein weiteres Netzwerk oder das Internet statt.
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 verschlüsselt abgespeichert, um das Lesen und das Verändern der Videodaten durch unbefugte Personen zu verunmöglichen. Aufgrund der Verschlüsselung 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 soll sichergestellt werden, 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 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 Pro-	- Der Zugriff wird auf die im Anhang zum Reglement bezeichneten Benutzergruppen beschränkt.

	gramme und Daten ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen.	- 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. - Die Zugriffsrechte werden jährlich auf ihre Korrektheit überprüft. - Alle Standard-Passwörter werden durch neue ersetzt
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 von Zugriffen können nicht manuell verändert 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.	- Die Massnahmen für eine Wiederherstellung der Daten beschränken sich aus Kostengründen auf die Installation eines RAID-Systems (Redundante Anordnung von unabhängiger Festplatten). Das Restrisiko eines möglichen 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 gemeldet werden und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können.	Das Videoüberwachungssystem meldet auftretende Fehlfunktionen nicht und das Restrisiko eines möglichen Integritätsverlustes wird getragen.

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.

5734 Reinach, 20.11.2023 **GEMEINDERAT REINACH AG**

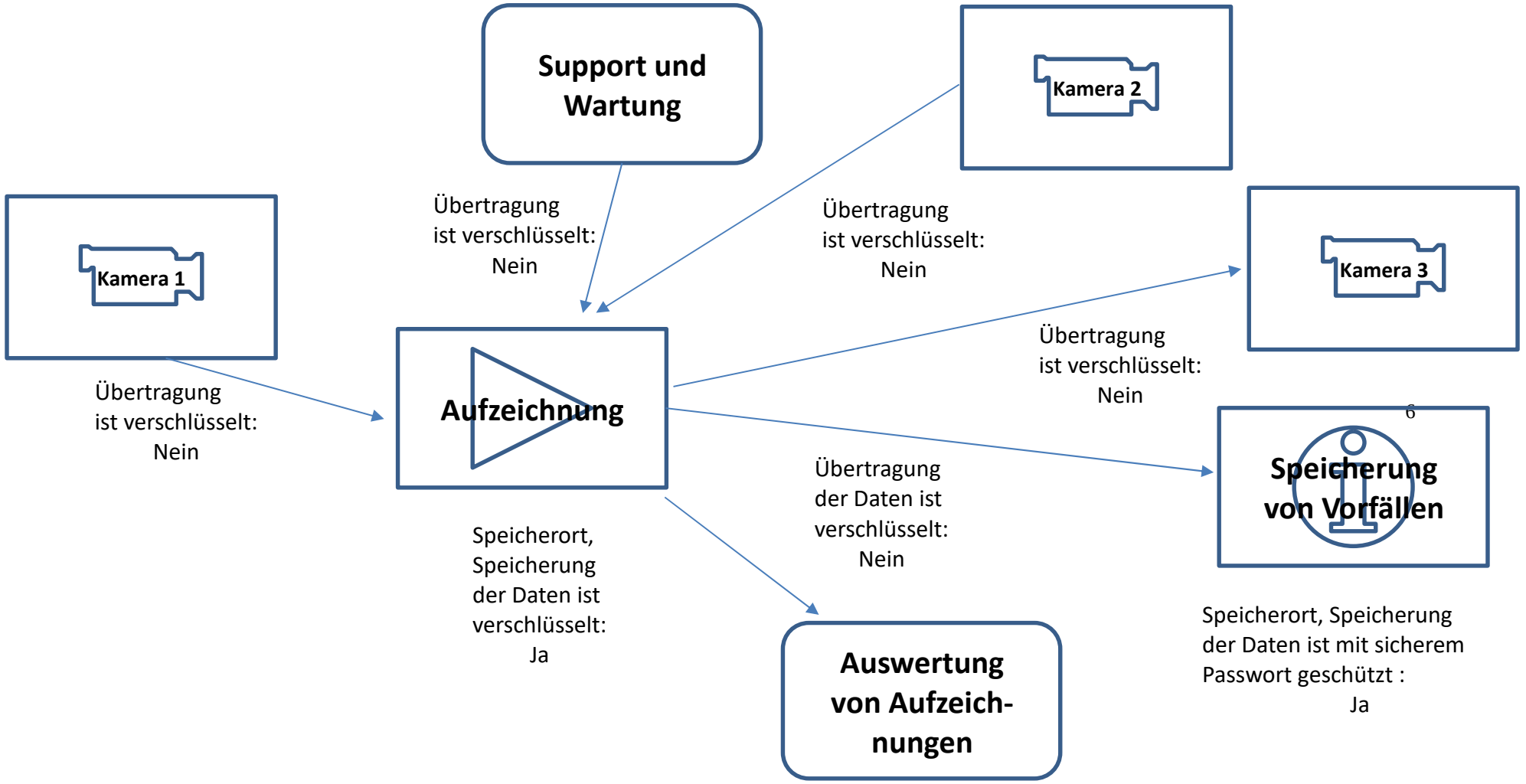
Der Gemeindeammann
Julius Giger

Der Gemeindeschreiber I
Peter Walz

Anhang 1 zum Datensicherheitskonzept vom 20.11.2023

8-12

Systemschema Videoüberwachung, komplett eigenes Netzwerk ohne ext. Anbindung



KANTON AARGAU

Beauftragte für Öffentlichkeit und Datenschutz

Bahnhofplatz 13
5201 Brugg
Telefon 062 835 45 60
E-Mail OEDB@ag.ch

ÖDB.23.360

Bewilligung vom 30. November 2023

Gesuchsteller: **Gemeinde Reinach AG,** Hauptstrasse 66, 5734 Reinach AG

Gegenstand: **Betrieb einer optisch-elektronischen Anlage im Sinn von § 20 IDAG**[1] gemäss Beschluss des Gemeinderats Reinach AG vom 20.11.2023

Verfügung:

1.

Der Betrieb der optisch-elektronischen Anlage richtet sich nach

- dem Rahmenreglement Videoüberwachung des Gemeinderats Reinach AG vom 01.07.2012;
- dem Anhang 2 zum vorstehend genannten Reglement Videoüberwachung (Stand vom 20.11.2023), mit der Benennung der Gebäude/Örtlichkeit; Anzahl Kameras; Überwachungszeit; Zweck der Überwachung; Funktionstragende/Auskunftsstelle (Anhang 1 dieser Bewilligung) und
- den Situationsplänen der Kamerastandorte und Überwachungsperimeter respektive der Standbildeinstellungen (Anhang 2 dieser Bewilligung).

2.

Der Betrieb der in Ziffer 1 näher bezeichneten optisch-elektronischen Anlage wird bewilligt für 10 Jahre.

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

3.

Allfällige Änderungen der optisch-elektronischen Anlage (inklusive der Anhänge 1 und 2) sowie räumliche, sachliche oder bauliche Veränderungen, die vom Überwachungsperimeter erfasst werden, sind unter Angabe der Gründe erneut zur Bewilligung zu unterbreiten.

4.

Der in Ziffer 1 genannte Anhang 2 und die Situationspläne sind vollständig mit Eintritt der Rechtskraft des Anhangs und den Situationsplänen auf der Website der Gemeinde Reinach zu publizieren.

5.

Es werden keine Verfahrenskosten erhoben.

Hinweis:

Die Gesuchstellerin bzw. der Gesuchsteller kann **innert 10 Tagen** seit Zustellung dieses Bewilligungsdispositivs bei der Beauftragten für Öffentlichkeit und Datenschutz (Bahnhofplatz 13, 5201 Brugg) **die vollständig begründete Ausfertigung der Bewilligung** verlangen.

Verlangt die Gesuchstellerin bzw. der Gesuchsteller innert dieser Frist keine vollständige Ausfertigung der Bewilligung, wird diese rechtskräftig.

Ein Rechtsmittel gegen die Bewilligung der Beauftragten für Öffentlichkeit und Datenschutz kann erst nach Erhalt der vollständigen Ausfertigung ergriffen werden.

Beauftragte für Öffentlichkeit und Datenschutz

BEAUFTRAGTE FÜR ÖFFENTLICHKEIT UND DATENSCHUTZ * (AARGAU) *

Gunhilt Kersten
Beauftragte

Anhänge

- In Ziffer 1 dieser Bewilligung erwähnt

Zustellung an

- Gemeindekanzlei Reinach, Peter Walz, Hauptstrasse 66, 5734 Reinach (per A-Post Plus)

Gemeinde Reinach

Anhang 2 zum Reglement Videoüberwachung vom 1. Juli 2012

Videoüberwachungsanlagen: Öffentliche Liste

Gebäude/ Örtlichkeit	**Anzahl Kameras**	**Überwachungs-perimeter**	**Überwachungs-zeit**	**Zweck/ Begründung Überwachungszeit**	**Funktionstragende/Auskunftsstelle** zur Auswertung von Bildern / Vernichtung und Speicherung von Bildmaterial / technischer Support
Schulanlage *Pfrundmatt*	3	- Überdeckter Eingangsbereich Süd - Eingangsbereich / Vorplatz beim Haupteingang Nord - Vorplatz / Schopf bei Bahngleis West	ausserhalb der Schulzeit von 18.00 bis 06.00 Uhr an Wochenenden, Feiertagen und während der Ferien 24 Stunden	**Wahrung des Hausrechts** Verhinderung und Ahndung von groben Sachbeschädigungen, erheblichen Verunreinigungen und Einbruchdiebstahl	**Zuständige Stelle für Auskünfte und Auswertung** Leiter Liegenschaften, Tel.: 062 765 12 59 **Technischer Support** Leiter Technischer Dienst, Reinach AG Saalbaustrasse 11 Tel. 062 765 12 72

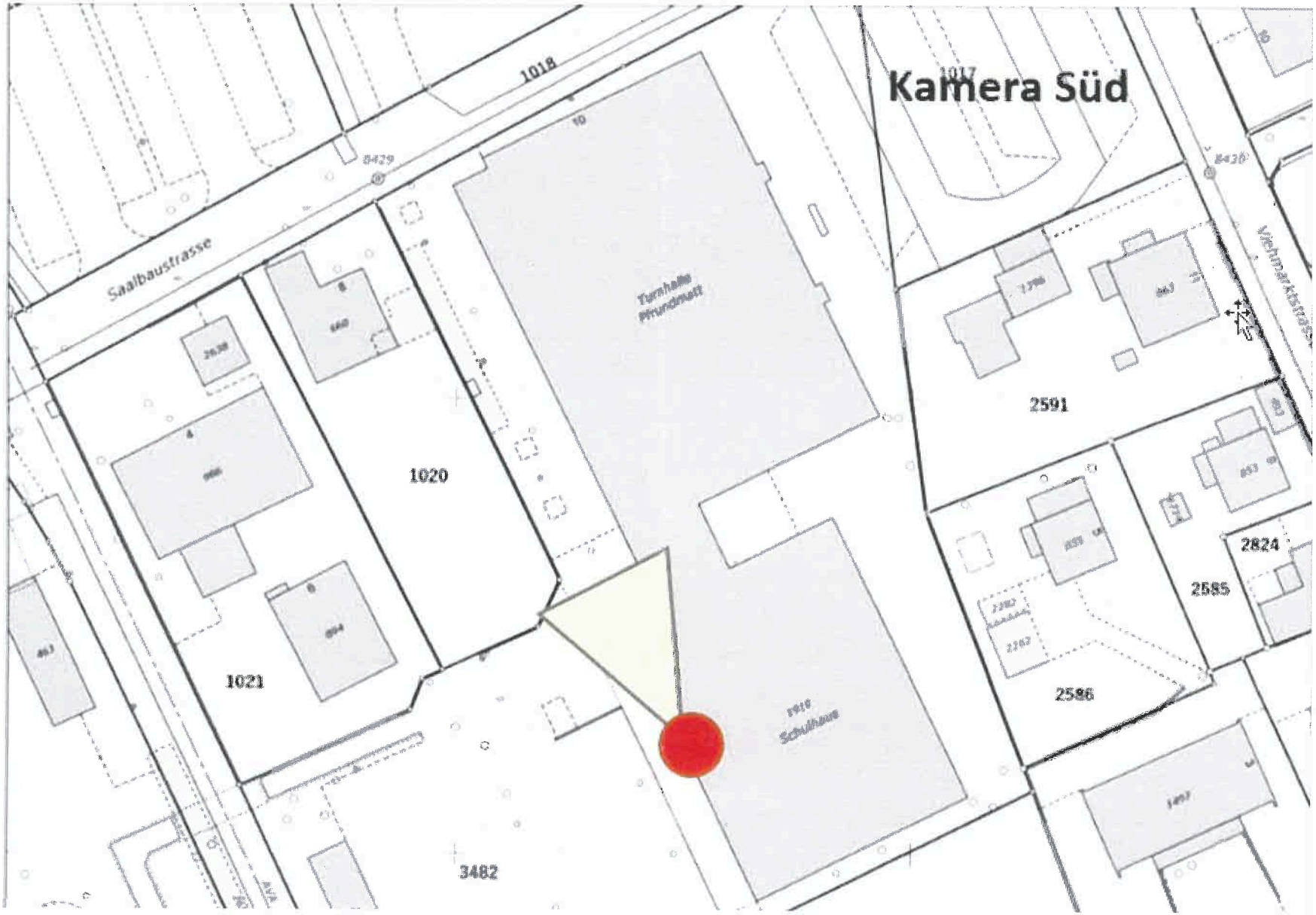
5734 Reinach, 20.11.2023

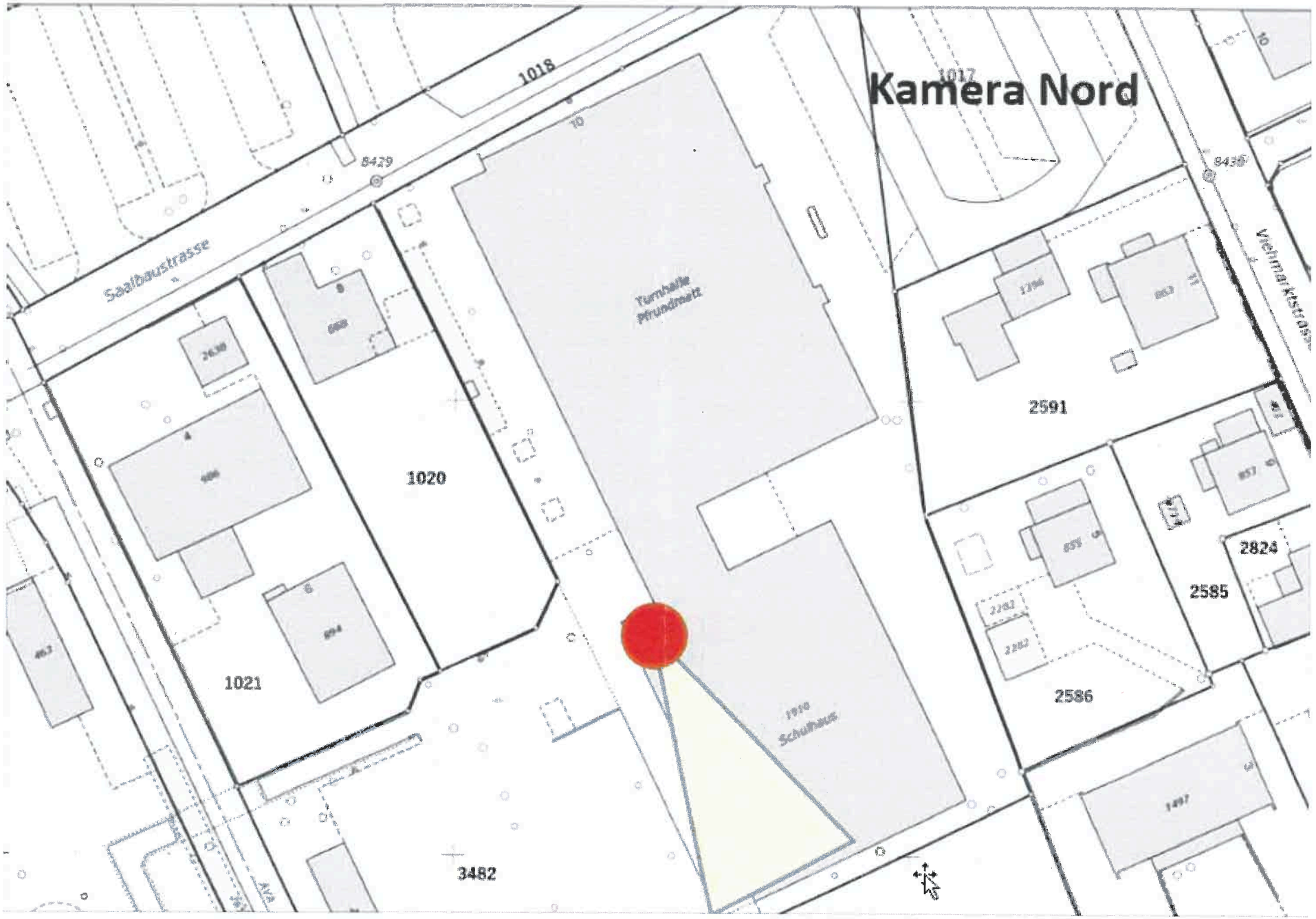
Publikation am 23.11.2023 im Wynentaler Blatt

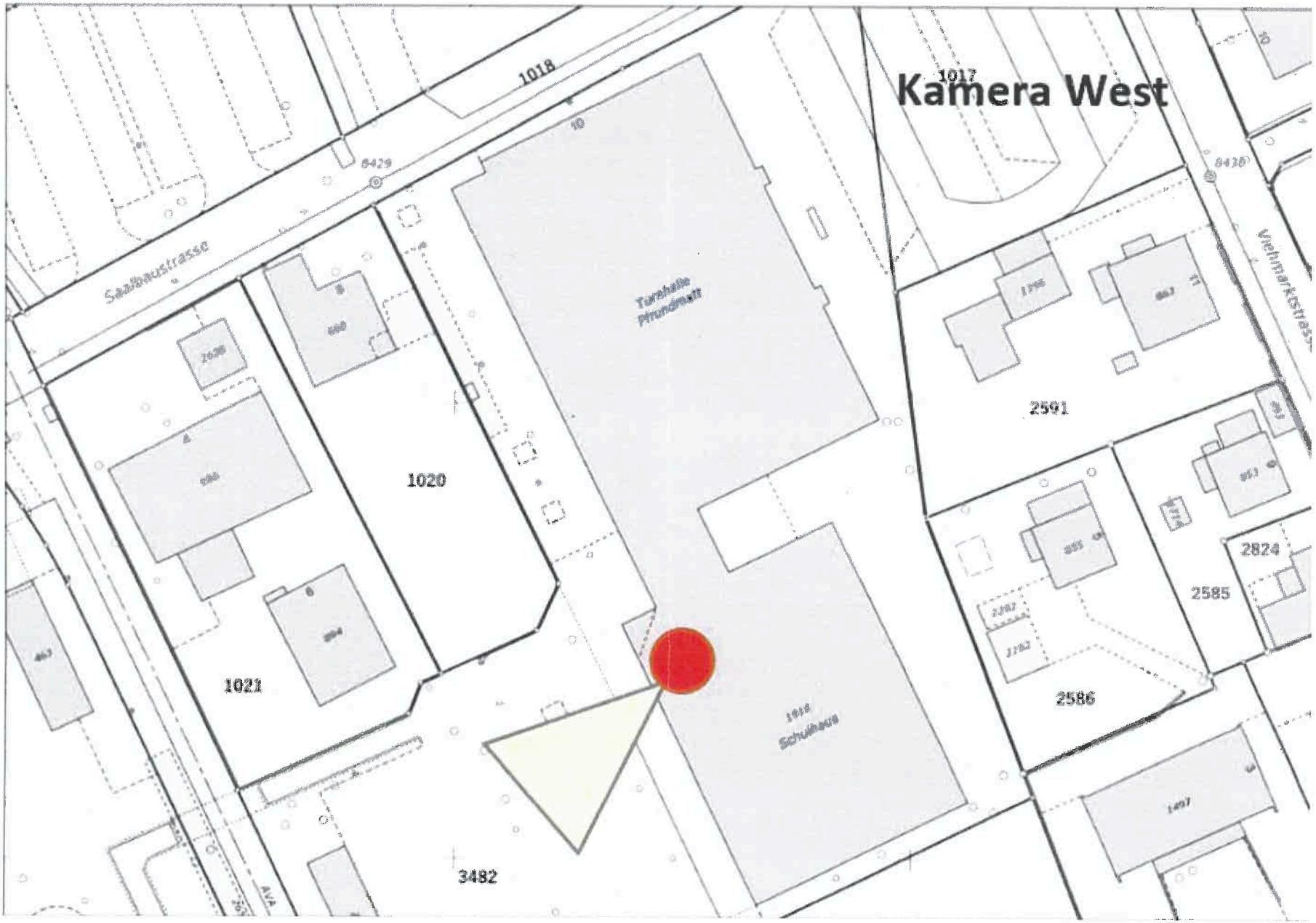
GEMEINDERAT REINACH AG

Julius Giger
Gemeindeammann

Peter Walz
Gemeindeschreiber I


Kamera Süd
1018
Saalbaustrasse
Turnhalle
Pfrundmatt
1020
1021
3482
Schulhaus
2591
2585
2824
2586
Viehmarktstrasse


Kamera Nord
Säulbaustrasse
Turnhalle
Pfrundmatt
1910
Schulhaus
1018
1017
8429
8430
1020
1021
3482
2591
2585
2824
2586
1497


Kamera West
1018
1017
8429
8430
Saalfeldstrasse
Viehmarktstrasse
Turnhalle
Pfrundmatt
1020
1021
3482
2591
2585
2824
2586
1497
1918
Schulhaus