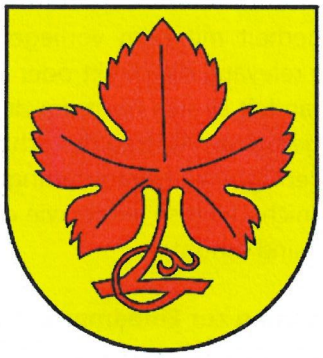
GEMEINDE KAISTEN



DATENSICHERHEITSKONZEPT VIDEOÜBERWACHUNG GEMEINDE KAISTEN

(Standort: Gemeindehaus Kaisten)

Ausgabe Juni 2024

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).

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.

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.

2.1 Zugangskontrolle

Zugangskontrollen reduzieren das Risiko, dass unbefugte Personen sich Zugang zu Einrichtungen, in denen Personendaten verarbeitet werden, verschaffen.

- Die baulichen Massnahmen, um den Zutritt zum Raum, in dem die Personendaten der Videoüberwachung gespeichert werden, zu schützen, sind mindestens jährlich zu überprüfen und bei Bedarf anzupassen.
- Die Protokollierung der Zutritte wird sichergestellt, unveränderbar aufbewahrt und mindestens jährlich überprüft.
- Die Zutrittsrechte sind jährlich auf ihre Korrektheit zu überprüfen.

2.2 Datenträgerkontrolle

Datenträgerkontrollen reduzieren das Risiko, dass unbefugte Personen Daten von mobilen Datenträgern (USB, externe Festplatten etc.) lesen, kopieren, verändern oder entfernen.

Es werden keine Daten der Videoüberwachung auf mobilen Datenträgern abgespeichert.

2.3 Transportkontrolle

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 Verschlüsselung schützt vor unberechtigtem Zugriff und Veränderung von sensitiven Informationen während deren Übertragung und Transport. Um eine Falschadressierung zu vermeiden, wird die Empfängeradresse vor dem Absenden zweifach geprüft.

Die Protokolle sind während eines Jahres revisionsgerecht festzuhalten. Sie dürfen ausschliesslich zur Überprüfung der Rechtmässigkeit der Datenbearbeitung und der Sicherstellung der Informations- und Informatiksicherheit verwendet werden.

2.4 Bekanntgabekontrolle

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 protokoliert und revisionsgerecht für mindestens ein Jahr aufbewahrt.

2.5 Speicherkontrolle

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.

Zugriffe auf Videodaten sind wie folgt zu protokollieren:

a) Zugriffe von Systemadministratoren

b) Zugriffe von Nutzenden zur

1. Authentifizierung und Autorisierung,
2. Dateneingabe und -veränderung,
3. Dateneinsicht,
4. Datenübermittlung,
5. Datenlöschung.

Die Protokolle sind während eines Jahres revisionsgerecht festzuhalten. Sie dürfen ausschliesslich zur Überprüfung der Rechtmässigkeit der Datenbearbeitung und der Sicherstellung der Informations- und Informatiksicherheit verwendet werden.

2.6 Benutzerkontrolle

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.

2.7 Zugriffskontrolle

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 eines Benutzers auf die Videodaten wird auf diejenigen Personendaten beschränkt, welche für die Erfüllung seiner Aufgabe benötigt werden. 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 sind jährlich auf ihre Korrektheit zu überprüfen. Alle Standard-Passwörter sind durch neue zu ersetzen. Wenn möglich, ist eine Zwei-Faktoren-Authentisierung, sonst ein komplexes, langes Passwort vorzusehen.

2.8 Eingabekontrolle

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.

2.9 Wiederherstellung

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.

2.10 Zuverlässigkeit, Integrität

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, Hitze, Feuer oder Wasser im Raum in welchem die Datenspeicherung stattfindet), um eine möglichst hohe 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.

5082 Kaisten, 05.06.2024

GEMEINDERAT KAISTEN

Árpad Major, Gemeindeammann

Manuel Corpataux, Gemeindeschreiber

Anhang: Prinzipschema

ALINAG
C. F. Bally-Strasse 36
5012 Schönenwerd
Tel.062/858 70 00 Fax 062/858 70 10

Gez: 11. 10. 22 mhä	Geä: 25. 08. 23 mhä	Prinzipschema/Kabelplan	1.1
Geä: 23. 02. 23 mhä	Geä:	Kunde: Gemeindeverwaltung Kaisten	
Geä: 10. 03. 23 mhä	Geä:	Nr. 101345pri.skf Alin AG