ISDS-Konzept Videoüberwachung
Gemeinde XY

*(Kursiver Text kann nach Abschluss des Konzepts gelöscht werden, gelb hinterlegter ist durch die Gde auszufüllen)*

Header \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Installation eines Systems zur Videoüberwachung öffentlicher Gebäude oder Bereiche in der Gemeinde XY
* Projektverantwortlicher: , inkl. Kontaktinformationen
* ISDS-Verantwortlicher, inkl. Kontaktinformationen
* Version 1.0
* Visum Projektauftraggebers:

# 1. Angaben zum Projekt

*(es kann auch auf bereits bestehende Projektdokumente verwiesen werden)*

Die Gemeinde XY hat mit Beschluss vom XY festlegt, einzelne öffentliche Gebiete zu den gesetzlich erlaubten Zwecken mit Videokameras zu überwachen.

Der Gemeinderat hat in Anwendung der geltenden Rechtsgrundlagen[[1]](#footnote-1) diese Überwachungsmassnahmen der Kantonspolizei Bern (Kantonspolizei Bern) zur Genehmigung beantragt, vgl. XY.

Mit dem Gesuch vom XY hat die Gemeinde die Überwachung in folgendem Rahmen beantragt:

* Strasse, Platz, Front etc. mit Zeitfenster XY
* Strasse, Platz, Front etc. mit Zeitfenster XY
* Etc.

Das im Folgenden ausgeführte Projekt XY hat zum Ziel, ein geeignetes IT-System zur Umsetzung des Gemeinderatsbeschlusses vom XY im Rahmen der kantonalen Genehmigung vom XY zu installieren und in Betrieb zu nehmen. Es werden damit keine neuen Verwaltungsprozesse geschaffen. Das System soll – mit Ausnahme allfälliger Wartungsarbeiten - ohne weiteres Zutun der Gemeindebehörden betrieben werden können. Stattdessen stehen die vom System aufgezeichneten Informationen, also Bild- und Tonaufnahmen von Orten und Personen, ausschliesslich den gesetzlich befugten polizeilichen Stellen zur Verfügung.

Der Betrieb der geplanten Lösung stellt in Sachen ISDS hohe Anforderungen an die Vertraulichkeit der bearbeiteten Daten. Aspekte wie Verfügbarkeit oder Integrität sind dagegen wenig ISDS-relevant, sodass im vorliegenden Konzept praktisch ausschliesslich Anforderungen und Massnahmen zum Schutz der betroffenen Personen ausgeführt werden. Die übrigen Anforderungen und Massnahmen richten sich nach dem kantonalen Standard für Grundschutz (vgl. Punkt 4).

Das System verfügt über folgende Inputschnittstellen:

* Kameras: es werden insgesamt XY Kameras des Typs XY an den genehmigten Standorten installiert. Dieser Typ zeichnet sich dadurch aus, dass …
* Netzwerkschnittstellen: Zur Übermittlung der Daten von den Kameras zum verarbeitenden System wird die Technologie XY verwendet. Das System verfügt über insgesamt XY entsprechende Schnittstellen, wovon XY aktiviert sind.
* Netzwerk der Gemeinde? Das System ist zusätzlich mit dem Verwaltungsdatennetz der Gemeinde verbunden, insbesondere um Aktualisierungen des Betriebssystems und der eingesetzten Software sowie die Fernwartung des Systems via Netzwerk/Fernzugriff zu ermöglichen. Ein Fernzugriff auf die Nutzdaten ist für Wartungsarbeiten nicht vorgesehen.

Das System verfügt über folgende Ausgabeschnittstellen:

* Bildschirm: zur Administration des Systems sowie zur berechtigten Nutzung der Bildaufzeichnungssoftware
* USB- und andere Schnittstellen zur Beschreibung von Datenträgern: die berechtigte Nutzung der Bildaufzeichnungssoftware umfasst zwingend den Export bestimmter Daten auf Datenträger der Kantonspolizei.
* Drucker?
* Netzwerk der Gemeinde? Vgl. oben. Der Export von Daten über die Netzwerkschnittstellen ist nicht vorgesehen und die Bildaufzeichnungssoftware dafür nicht konfiguriert.
* Ein Abrufverfahren der Daten der Bildaufzeichnungssoftware ist nicht vorgesehen bzw. installiert.

*Beschreibung der zur Wahl stehenden IT-Lösung(en).
Evt. Verweis auf Produktdokumentation, Offerten, Verträgen etc, vgl. auch Zustimmungsgesuch an Kantonspolizei Bern gemäss Art. 49 Abs. 2 lit. f und h PolV*

Das zu installierende System besteht aus den folgenden Komponenten:

* Server
* OS
* Fachanwendung
* Kameras
* Netzwerke
* Partner/Lieferanten

# 2. Datenschutz

Die geplante Videoüberwachung ist als Bearbeiten von Personendaten im Sinne des kantonalen Datenschutzgesetzes KDSG zu betrachten; das KDSG ist demnach anwendbar. Sie wird gestützt auf das bernische Polizeigesetz vom 10. Februar 2019 (PolG, BSG 551.1) sowie die Polizeiverordnung vom 20. November 2019 (PolV, BSG 551.111) umgesetzt. Diese erlauben eine Überwachung in dem Rahmen, der der Gemeinde von der Kantonspolizei Bern mit Verfügung vom XY genehmigt worden ist. Weitere Rechtsgrundlagen sind zum Betrieb der geplanten Lösung nicht erforderlich.

Die zulässige Aufbewahrungsdauer der aufgezeichneten Bild- und Tondaten richtet sich nach den erwähnten Rechtsgrundlagen. Demnach werden unbenutzte Daten 100 Tage nach Aufzeichnung vom System automatisch gelöscht. Über die Löschung wird Protokoll geführt. Eine weitere Datenarchivierung findet im Zuständigkeitsbereich der Gemeinde nicht statt.

Betroffene Personen haben ein Recht auf Einsicht in die Aufnahmen. Entsprechende Gesuche sind an die Kantonspolizei Bern zu richten. Diese gewährt die Einsicht im genehmigten Umfang und sorgt für die Umsetzung der übrigen berechtigten Ansprüche.

Das Benutzerberechtigungskonzept für das System sieht folgende Rollen vor:

* Admin Extern: wer?
* Admin intern: wer?
* Hauptbenutzer (Rolle Kantonspolizei Bern; wird ad hoc innerhalb der Kantonspolizei Bern der zuständigen Person zugewiesen)

Die verschiedenen Rollen werden nur jeweils mit denjenigen Zugriffsberechtigungen versehen, die sie zur Erfüllung ihrer Aufgaben zwingend benötigen:

* Admin Extern: administrative Zugriffe auf Systembefehle u.ä., aber nicht auf Nutzdaten des Systems.
* Admin intern: administrative Zugriffe auf Systembefehle u.ä.; Zugriff auf Nutzdaten des Systems zu Wartungszwecken gemäss Artikel 56 der Polizeiverordnung.
* Hauptbenutzer (Rolle Kantonspolizei Bern; wird ad hoc innerhalb der Kantonspolizei Bern der zuständigen Person zugewiesen) mit Nutzungsrechten der bearbeiteten Daten, aber ohne Zugriff auf Systembefehle u.ä.

Die Anmeldung der Datensammlung bei der Datenschutzaufsichtsstelle erfolgt, sobald von dieser entsprechende Formulare angeboten werden.

# 3. Informationssicherheit

Die Klassifizierung der geplanten Lösung mittels des frames Klassifizierung (Anhang 1 zur Ausführungsweisung des KAIO über die Weisung des Regierungsrates über Informationssicherheit und Datenschutz vom 1. Oktober 2008, hat ergeben, dass aufgrund der Datenschutzrelevanz des Systems in sämtlichen Kontrollzielen nach RRB ISDS eine vertiefte Risikoanalyse durchzuführen ist.

Tatsächlich sind von diesen jedoch nur die Bereiche relevant, die direkt oder mittelbar die Vertraulichkeit der bearbeiteten Daten sicherstellen; bei der Videoüberwachung handelt es sich nicht um die Kernaufgaben einer öffentlichen Verwaltung, sondern um eine zusätzliche Möglichkeit, den allgemeinen Sicherheitsauftrag umzusetzen. Hohe Verfügbarkeitsanforderungen an ein Überwachungssystem entstehen dadurch bzw. aus ISDS-Überlegungen nicht, ebenso wenig wie qualitative Integritäts- oder ähnliche Anforderungen.

# 4. Risikoanalyse

Im Rahmen der Risikoanalyse hat sich folgendes Bild ergeben:

* Zu den Kontrollzielen Zutritt, Zugang, Zugriff, Verfügbarkeit und Trennung drängen sich keine anderen Massnahmen als diejenigen in der Checkliste Grundschutz auf;
* Die Risiken des Kontrollziels Eingabekontrolle ist mangels Nutzdateneingabe nicht relevant;
* Das Kontrollziel Weitergabe ist gemäss unten stehenden Massnahmen abzuändern.

# 5. Massnahmen

Massnahmen sind grundsätzlich als Eignungskriterien für das zu beschaffende System zu verstehen, soweit dies möglich ist.

Es wird auf jeden Fall ein Benutzerberechtigungskonzept mit den aufgeführten Rollen erarbeitet, welches von der systemverantwortlichen Stelle unterzeichnet wird. Dieses beinhaltet abschliessend die vorgesehenen Rollen inkl. Zugriffsberechtigungen sowie einen Beschrieb, wie und von wem die Rollen einzelnen Mitarbeitenden bzw. Externen zugeteilt werden.

Die übrigen Massnahmen gemäss der erwähnten Checkliste Grundschutz werden vollständig umgesetzt bzw. Abweichungen davon werden im Einzelfall begründet. Eingeschlossen ist die Massnahme M-5.1.1 (Regelung der Benutzerberechtigungen und der Datenschutzverantwortung), jedoch im Rahmen des Benutzerberechtigungskonzepts. Zusätzlich zu den Grundschutzmassnahmen ist durch die Kantonspolizei sicherzustellen, dass jeglicher Export und die Übermittlung von Nutzdaten aus dem System, unbesehen des Datenträgers, ausschliesslich verschlüsselt erfolgt.

Ein Massnahmenplan wird erarbeitet, sobald dies sinnvollerweise möglich ist (i.d.R. nach einem Beschaffungsentscheid, damit zusammen mit dem Lieferanten die Umsetzung der bekannten Massnahmen geplant werden kann).

# 6. Kontrolle

Die Kontrolle der Einhaltung der ISDS-Vorgaben erfolgt mittels der Genehmigungsverfügung der Kantonspolizei zum Betrieb des beschriebenen Überwachungssystems. Im Übrigen gelten die Bestimmungen der kantonalen Datenschutzgesetzgebung; das bedeutet, dass die Datenschutzaufsichtsstelle der Gemeinde die Einhaltung der Datenschutzvorgaben auch nachträglich überprüfen oder überprüfen lassen kann.

1. Insbesondere Polizeigesetz vom 10. Februar 2019 (PolG), Polizeiverordnung vom 20. November 2019 (PolV) und Datenschutzgesetz vom 19. Februar 1986 (KDSG) [↑](#footnote-ref-1)