Datenschutz-Folgenabschätzung mobile Videoüberwachung bei illegaler Abfallablagerung (Pilotphase)

konkret, abgrenzbar und rechtlich legimitierter Zweck der Verarbeitung
vom Verantwortlichen berechtigten Interessen

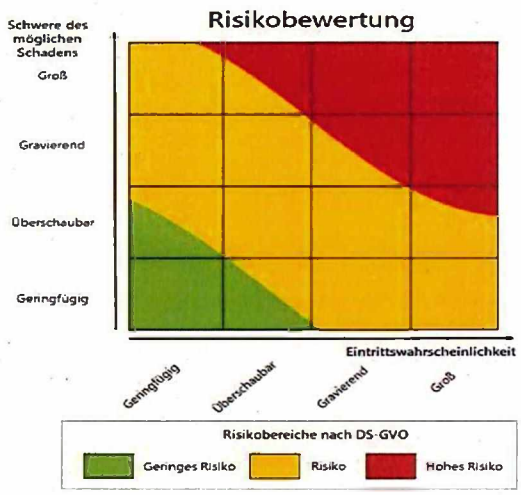
Gewährleistungsziele
- Datenminimierung (die Erhebung personenbezogener Daten und ihre Weiterverarbeitung ist auf das dem Zweck angemessene, erheblich und notwendige Maß zu beschränken)
- Verfügbarkeit (personenbezogene Daten sind im Zugriff der Berechtigten, sind konkret auffindbar, werden angemessen dargestellt und können inhaltlich interpretiert werden)
- Integrität (informationstechnische Prozesse und Systeme halten die Spezifikation ein und die zu verarbeitenden Daten bleiben unversehrt, vollständig und aktuell; wird als eine Form der Richtigkeit verstanden)
- Vertraulichkeit (keine unbefugte Person kann personenbezogene Daten zur Kenntnis nehmen)
- Nichtverkettbarkeit (personenbezogene Daten dürfen nicht zusammengeführt werden)
- Transparenz (Betroffene, Betreiber von Systemen sowie zuständige Kontrollinstanzen können erkennen, welche Daten für welchen Zweck bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und die rechtliche Verantwortung besitzt)
- Intervenierbarkeit (Betroffenen wird die ihn zustehenden Rechte auf Benachrichitgung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt)

Risikoquelle
- städtische Mitarbeiter*innen (Innen- und Außendienst)
- externe Mitarbeiter*innen (beauftragte Firma für Videoüberwachung, Reinigungsfirma, externe Zusteller)
- Fachseitige Anwendungsbetreuung (FAB)
- Software
- Umwelteinflüsse (Naturgewalt)
- Dritte (bspw. Einwohner*innen, Anwohner*innen, Diebe, Hacker, Familienangehörige, Raucher)
- Datenübertragung (Netzwerk- und Kommunikationsverbindungen)
- Internetprovider
- mobile Infrastruktur (Kfz inkl. Netzkomponenten, Kamera, Datenspeicher, Stromversorgung, ungesicherte Kabel oder Netzwerkdosen)
- Server
- Rechenzentrum
- Besucher im Gebäude
- externe Datenträger (Staatsanwaltschaft und Gericht, Betroffene, Anwalt)
- zur Verfügungstellung der Software/Updates

Art des Zielobjektes gem. DSM
Daten (personenbezogene Daten)
Systeme (Hardware, Software und Infrastruktur)
Prozesse (technische, organisatorische und personellen Prozesse der Verarbeitung)

möglicher Schaden
Daten werden nicht oder nicht richtig übermittelt, dadurch drohender finanzieller Verlust (Datenverlust)
Manipulation von Informationen
Reputationsschaden für Stadt
Verletzen der Rechte und Freiheiten, Eingriff in die Privatsphäre / heimliche Überwachung
Ausfall von Systemen
Verlust der Vertraulichkeit
Verarbeitung von sensiblen Daten (Eth. Herkunft, Politik, Religion, Sexualleben, Gesundheit, etc.)
Profilbildung durch Bewertung persönlicher Aspekte (Vorlieben, Interessen, Aufenthaltsort, etc.)
Verarbeitung von Kinderdaten
Große Menge personenbezogener Daten
Große Anzahl von betroffenen Personen
Rufschädigung, Diskriminierung, andere wirtschaftliche Schäden

Risikomatrix



Geringes Risiko

Ein geringes Risiko bedeutet, dass weder die mögliche Schwere des Schadens für den Betroffenen noch die Eintrittswahrscheinlichkeit hoch sind und in Kombination weder mittel noch hoch.
Bei einem geringen Risiko ergeben sich in der DS-GVO für den Verantwortlichen gewisse Ausnahmen verschiedener Verpflichtungen, so dass manche Maßnahmen nicht durchgeführt werden müssen:

- Bei einer Datenschutzverletzung ohne Risiko (z. B. harmloser Fehlversand innerhalb einer Organisation) muss die Datenschutzaufsichtsbehörde nicht informiert werden.
- Ein Verzeichnis der Verarbeitungstätigkeiten ist (unter Berücksichtigung anderer Faktoren wie z. B. unregelmäßige Verarbeitung) bei geringem Risiko nicht zu erstellen.

Risiko ("Normal")

Auch bei einer rechtmäßigen Verarbeitung personenbezogener Daten entstehen Risiken für die betroffenen Personen, z. B. bei der Verarbeitung von Adresslisten, Einkaufsverhalten, der Kommunikation am Arbeitsplatz oder von Mitgliederlisten eines Sportvereins. Dort kann also die Schwere des Schadens und die Eintrittswahrscheinlichkeit in Kombination ein mittleres Niveau für das Risiko des Betroffenen erreichen.
Bei der Verarbeitung besonderer Arten personenbezogener Daten, d.h. sensibler Daten, ist das Risiko nicht immer gleich als hoch einzustufen. Die Risiko-Stufe "normal" kann also dort auch erreicht werden wie z. B. bei Angaben zur Religionszugehörigkeit "Römisch-Katholisch" in Bayern oder der Diagnose eines "Schnupfens" beim Hausarzt.

Hohes Risiko

Ein hohes Risiko umfasst dagegen potentielle Schäden, deren Ausmaß für die Rechte und Freiheiten von Betroffenen gravierend und/oder ziemlich wahrscheinlich sind. Unter der DS-GVO wird dieses Risiko-Level im Verhältnis aller Verarbeitungen eher selten vorkommen. Da ein hohes Risiko aber wesentliche Rechtsfolgen für den Verantwortlichen hat, muss das mögliche Vorkommen eines hohen Risikos zwangsläufig im Blick behalten werden.

Eintrittswahrscheinlichkeit und Schadensauswirkung (Schwere des Schadens): Vernachlässigbar (1) Begrenzt (2) Wesentlich (3) Maximal (4)

Ergebnis

Ergebnis
geringes Risiko (2-3)
Risiko (4)
Risiko (5)
Risiko (6)
hohes Risiko (7-8)

Planung

Risikobeurteilung														
I. Risikoindentifikation					II. vorläufige Risikoanalyse			III. Risikobewertung	Gegenmaßnahmen	IV. endgültige Risikoanalyse		V. endgültige Risikobewertung		
Gewährleistungsziele	Verarbeitungs-, Arbeitsvorgang	Risikoquelle	Eindeutige Bezeichnung des Risiko (Risikobeschreibung)	Art des Zielobjektes gem. DSM	Möglicher Schaden	Eintrittswahrscheinlichkeit	Schadensauswirkung	vorläufiges Ergebnis	geeignete und angemessene, technische und organisatorische Maßnahmen	Eintrittswahrscheinlichkeit	Schadensauswirkung	endgültiges Ergebnis		
Vertraulichkeit	Datenübertragung	Datenübertragung (Netzwerk- und Kommunikationsverbindungen); Dritte	Während Übertragung können Daten von unberechtigten Dritten eingesehen werden	Daten	Verlust der Vertraulichkeit; Reputationsschaden für Stadt	3	3	6	Verschlüsselung der drahtlosen Übertragung der Videodaten zum städtischen Server aufgrund des hohen Schutzbedarfs der übertragenen Daten. Nutzen eines VPN-Tunnels[5]	1	1	1		
Integrität	Auswahl von Software	- Software	Ungeeignete Auswahl von Software führt zu Inkompatibilität, fehlerhafte Konfiguration wie Cloud-Back-up Lösungen Zudem könnte Software aus unzuverlässiger Quelle bezogen werden, was zum Einsatz von fehlerhafter Software führen könnte (bspw. Trojaner)	Systeme	Manipulation von Informationen Reputationsschaden für Stadt Rufschädigung, Diskriminierung, andere wirtschaftliche Schäden	2	3	5	Software enthält generelle Sicherheitsfunktionen wie Authentifizierung, sichere Verschlüsselungsfunktionen etc., siehe verlinkten Bericht [redacted] Software wird nach IT-Grundschutz-Kriterien ausgesucht[7,8,9]	1	1	1		
Integrität	Auswahl von Software	Software	Auswahl von Software mit Designfehlern in - Sicherheit - Datenschutz - Funktion	Systeme	Manipulation von Informationen Reputationsschaden für Stadt Rufschädigung, Diskriminierung, andere wirtschaftliche Schäden	2	3	5	Software enthält generelle Sicherheitsfunktionen wie Authentifizierung, sichere Verschlüsselungsfunktionen etc., siehe verlinkten Bericht [redacted] Benutzergruppen und -rechte können explizit vergeben und eingestellt werden. 4-15 beschreibt welche städtischen Mitarbeiter*Innen in welchem Umfang autorisiert sind, Daten zu erfassen, zu lesen, zu verändern und zu löschen (Berechtigungskonzept) und zeigt den Eskalationsweg zu Vorgesetzten auf. Software wird nach IT-Grundschutz-Kriterien ausgesucht[1,2,4,5,8,9]	1	1	1		
Verfügbarkeit	Auswahl des Kfz	mobile Infrastruktur	unsichere Kommunikationsschnittstellen und ungeregelte Datenübertragung mit der Folge, dass unberechtigt Daten übermittelt werden (moderne Fahrzeuge verfügen für die Benutzer direkt ersichtliche drahtlose Kommunikationsschnittstellen, wie z.B. Bluetooth oder WLAN als auch für den Benutzer nicht direkt ersichtliche wie z.B. integrierte Mobilfunkschnittstellen mit IT-Systemen der Hersteller, wobei dieser Informationsaustausch von den Anwendern i.d.R. nicht beeinflusst werden kann.)	Daten	Manipulation von Informationen Verlust der Vertraulichkeit	2	2	4	Es wird ein Kfz - entsprechend des Einsatzzweckes - ohne Kommunikationsschnittstellen zum unerlaubten und undefinierten Datenaustausch verwendet. Nicht benötigte Funktionen werden abgeschaltet (Anforderung aus IT-Grundschutz).[6,8,9]	1	1	1		
Verfügbarkeit	Sicherung des Kfz	mobile Infrastruktur	Möglichkeit in das Fahrzeug hineinzusehen und Kamera zu entdecken, was Begehrlichkeiten bei potentiellen Angreifern weckt (Kompromittieren des Kfz und Verfügbarkeit der Systemumgebung (drohender Verlust der Verfügbarkeit))	Systeme	Daten werden nicht oder nicht richtig übermittelt, dadurch drohender finanzieller Verlust (Datenverlust) Ausfall von Systemen	3	3	6	Sichtschutzfolie (verdunkelte Fenster) und sicheres Schließsystem Sicherungsmaßnahmen innerhalb des Kfz (Käfig zur Sicherung der Kameras) Für alle wesentlichen Situationen, die das Kfz und die darin vorhandenen Gegenstände mit Relevanz für die Informationssicherheit betreffen, wird eine Handlungsanweisung in Form von Checklisten vorliegen (wann, wie und wo ein Kfz sachgerecht abgestellt werden darf).[9]	2	2	4		
Verfügbarkeit	Sicherung des Kfz	mobile Infrastruktur	Das Kfz wird von außen beschädigt und die Fahrtüchtigkeit beeinträchtigt	Systeme	Ausfall von Systemen	2	1	3	Sicherungsmaßnahmen für IT-Komponenten (Käfig); Alarmieren der Polizei[8]	1	1	1		
Verfügbarkeit	Stromquelle im Kfz	mobile Infrastruktur	unzureichende Stromquelle und daraus resultierender Datenverlust	Systeme	Daten werden nicht oder nicht richtig übermittelt, *dadurch drohender finanzieller Verlust (Datenverlust)* Ausfall von Systemen	3	1	4	Es wird eine entsprechend der vorgesehenen Intervalle für das Tauschen der Stromquelle ausreichende Kapazität zur Verfügung gestellt	1	1	1		
Verfügbarkeit	Stromquelle im Kfz	mobile Infrastruktur	Stromquelle könnte eine Brandgefahr darstellen bei Anschluss der Batterie oder beim Betrieb	Systeme	Daten werden nicht oder nicht richtig übermittelt, Ausfall von Systemen, Gefahr für Leib und Leben	2	3	5	Alarmieren der Feuerwehr bei Brand[8] Wechsel und Anschluss der Batterie durch geschultes Personal	2	2	4		
Datenminimierung, Transparenz	Standortauswahl	städtische Mitarbeiter*innen (Innen- und Außendienst)	Unberechtigte Aufnahme	Prozesse	Verarbeitung von Kinderdaten Große Menge personenbezogener Daten Große Anzahl von betroffenen Personen Reputationsschaden für Stadt Verarbeitung von sensiblen Daten (Eth. Herkunft, Politik, Religion, Sexualleben, Gesundheit, etc.)	3	4	7	Standortauswahl innerhalb Pilotphase erfolgt in Abstimmung mit LfDI und ist ausführlich im Konzept "Pilot mobile Videoüberwachung Installation von mobilen Kameras zur Verhinderung illegaler Abfallablagerungen" beschrieben. Aufnahmebereich und Verpixelung sowie Vier-Augen-Prinzip bei Entpixelung wie im Konzept beschrieben.	1	1	1		
Datenminimierung, Transparenz	Standort Kfz	städtische Mitarbeiter*innen (Innen- und Außendienst)	Unberechtigte Aufnahme	Prozesse	Verarbeitung von Kinderdaten Große Menge personenbezogener Daten Große Anzahl von betroffenen Personen Reputationsschaden für Stadt Verarbeitung von sensiblen Daten (Eth. Herkunft, Politik, Religion, Sexualleben, Gesundheit, etc.)	3	4	7	Standortauswahl innerhalb Pilotphase erfolgt in Abstimmung mit LfDI und ist ausführlich im Konzept "Pilot mobile Videoüberwachung Installation von mobilen Kameras zur Verhinderung illegaler Abfallablagerungen" beschrieben. Aufnahmebereich und Verpixelung sowie Vier-Augen-Prinzip bei Entpixelung wie im Konzept beschrieben.[9]	1	1	1		

Datenminimierung, Transparenz	Einstellen der Kamera	städtische Mitarbeiter*Innen (Innen- und Außendienst)	Unberechtigte Aufnahme	Prozesse	Verarbeitung von Kinderdaten Große Menge personenbezogener Daten Große Anzahl von betroffenen Personen Reputationsschaden für Stadt Verarbeitung von sensiblen Daten (Eth. Herkunft, Politik, Religion, Sexualleben, Gesundheit, etc.)	3	4		Standortauswahl innerhalb Pilotphase erfolgt in Abstimmung mit LfDI und ist ausführlich im Konzept "Pilot mobile Videoüberwachung Installation von mobilen Kameras zur Verhinderung illegaler Abfallablagerungen" beschrieben. Aufnahmebereich und Verpixelung sowie Vier-Augen-Prinzip bei Entpixelung wie im Konzept beschrieben.	1	1	
Transparenz	Hinweisschilder planen je ausgewählten Standort	städtische Mitarbeiter*Innen (Innen- und Außendienst)	Betroffene Personen werden nicht (ausreichend) informiert.	Prozesse	Verletzen der Rechte und Freiheiten, Eingriff in die Privatsphäre / heimliche Überwachung	2	2		Es werden Hinweisschilder in Größe DIN A4 in Abstimmung mit LfDI angebracht und ist ausführlich im Konzept "Pilot mobile Videoüberwachung Installation von mobilen Kameras zur Verhinderung illegaler Abfallablagerungen" beschrieben. Zudem werden die Vorgaben zur Gestaltung eingehalten.	1	1	
Vertraulichkeit, Verfügbarkeit	Qualifizierung der Mitarbeiter*Innen	städtische Mitarbeiter*Innen (Innen- und Außendienst)	sicherheitsrelevante Ereignisse können nicht als solche identifiziert werden und illegale Abfallablagerungen bleiben unerkannt; unzureichende Reaktion bei Störungen im Betrieb der Software; fehlerhafter Umgang mit Hard- und Software, was zu unberechtigten Aufnahmen führen könnte	Prozesse	Verlust der Vertraulichkeit	2	2		Es werden Schulungen durchgeführt, sodass eine Achtsamkeit, Sorgfältigkeit beim Umgang mit Hardware, Software und Infrastruktur erreicht wird und angemessen auf Störungen reagiert wird.[4]	1	1	
Vertraulichkeit	Prozessdefinition	städtische Mitarbeiter*Innen (Innen- und Außendienst)	Die unzureichende Prozessdefinition führt zu unberechtigten Zugriffen	Prozesse	Verlust der Vertraulichkeit Manipulation von Informationen	2	2		Zugriffsrechte und Rollen klar definieren, siehe Berechtigungskonzept[2,3,4]	1	1	
Vertraulichkeit, Verfügbarkeit, Integrität	Kfz sichern	städtische Mitarbeiter*Innen (Innen- und Außendienst)	Einbruchmöglichkeit gegeben, unbefugte Dritte erhalten Zugriff auf Informationen	Systeme	Daten werden nicht oder nicht richtig übermittelt, dadurch drohender finanzieller Verlust (Datenverlust) Ausfall von Systemen	3	3		Sicherungsmaßnahmen einhalten Für alle wesentlichen Situationen, die das Kfz und die darin vorhandenen Gegenstände mit Relevanz für die Informationssicherheit betreffen, wird eine Handlungsanweisung in Form von Checklisten vorliegen (wann, wie und wo ein Kfz sachgerecht abgestellt werden darf).[9]	2	2	
Vertraulichkeit, Verfügbarkeit	Diebstahl des Kfz	Dritte	Schützenswerte Informationen verbleiben im Fahrzeug und unbefugte Dritte erhalten Zugriff auf Informationen und daraus resultierend Ausfall von integrierten IT-Komponenten innerhalb Kfz	Systeme	Ausfall von Systemen Verlust der Vertraulichkeit	2	3		siehe Datenverschlüsselung Für alle wesentlichen Situationen, die das Kfz und die darin vorhandenen Gegenstände mit Relevanz für die Informationssicherheit betreffen, wird eine Handlungsanweisung in Form von Checklisten vorliegen (wann, wie und wo ein Kfz sachgerecht abgestellt werden darf). Es wird eine Inventarliste und Handlungsanweisungen für Diebstahl oder der darin vorhandenen Gegenstände mit Relevanz für die Informationssicherheit erstellt.[9]	2	1	
Datenminimierung	Inbetriebnahme Kfz oder der darin verbauten IT-Komponenten	städtische Mitarbeiter*Innen (Innen- und Außendienst)	Relevante Einstellungen könnten falsch konfiguriert werden und zur Videoüberwachung von Hauseingängen, Hausfronten und anderen schützenswerten Bereichen führen	Daten	Verarbeitung von Kinderdaten Große Menge personenbezogener Daten Große Anzahl von betroffenen Personen Reputationsschaden für Stadt	1	1		In der Planungsphase finden Schulungen statt und es erfolgt vor der Inbetriebnahme am jeweiligen Standort eine Überpfüung der Einstellungen.[9] Private Zonen werden auf den Kameras gesetzt und sind unwiederruflich bei den Aufzeichnungen. Verpixelung erfolgt auf dem Rekorder für einzelnene Usergruppen. Das heißt Verpixelungen können aufgehoben werden. Schwärzungen können nicht aufgehoben werden, da das Bild schon geschwärzt am Rekorder ankommt.	1	1	
Integrität	Verändern von Daten während Übertragung zwischen Kfz und Stadtserver	- Datenübertragung (Netzwerk- und Kommunikationsverbindungen)	Schadsoftware in Dateien einspielen	Daten	Verlust der Vertraulichkeit; Reputationsschaden für Stadt	2	3		VPN-Tunnel; Transportverschlüsselung[8]	1	1	
Integrität, Vertraulichkeit	Aufzeichnungsmaterial sichten; Aufheben der Verpixelung	städtische Mitarbeiter*Innen (Innen- und Außendienst)	Unberechtigtes Aufheben der Verpixelung und Verletzung der Persönlichkeitsrechte	Daten	Profilbildung durch Bewertung persönlicher Aspekte (Vorlieben, Interessen, Aufenthaltsort, etc.) Reputationsschaden für Stadt Verletzen der Rechte und Freiheiten, Eingriff in die Privatsphäre / heimliche Überwachung	1	2		Zum Aufheben der Verpixelung ist eine 2-Personen Authentifikation notwendig. Es wird die Auf-/Abschaltung der Bilder und das 4-Augen Login (inkl. der normalen logs. Backup, Aufschaltung) protokoliert. Zudem ist das Erstellen von Backups möglich. Logfiles speichern sämtliche Steuerungen und Zugriffe im Hintergrund und können abgerufen werden. IP Adressen sind auf jedem einzelnen Gerät gespeichert. Logfiles liegen auf den einzelnen Geräten, Zugriffe auf dem Rekorder. siehe Punkt Berechtigungskonzept[6,8]	1	1	
Vertraulichkeit	Aufzeichnungsmaterial sichten durch Externe	- externe Mitarbeiter*Innen (beauftragte Firma für Videoüberwachung, Reinigungsfirma, externe Zusteller)	Unberechtigter Zugriff auf Daten durch beauftragte Firma zur mobilen Videoüberwachung	Daten	Manipulation von Informationen, Reputationsschaden für Stadt, Verletzen der Rechte und Freiheiten, Eingriff in die Privatsphäre / heimliche Überwachung, Verlust der Vertraulichkeit	2	3		Nur direkt über den Rekorder. Wenn über einen separaten Jump Client kein Servicezugang eingerichtet wird, kann auch nicht aus der Ferne zugegriffen werden. Sofern Fernwartung im Leistungsumfang beauftragt würde, wird eine Vereinbarung zur Auftragsverarbeitung abgeschlossen. Würde ein Fernzugriff Bestandteil des Leistungsumfangs sein, könnte die beauftragte Firma auf die Daten zugreifen. Jedoch können Sitzungsprotokolle angefordert werden und der Zugriff muss freigegeben werden. Es wird also jede Bewegung und jeder Klick in einem Logfile gespeichert.[8,9]	1	2	
Integrität	Verändern von Daten während Sachbearbeitung unterer Abfallbehörde	- städtische Mitarbeiter*Innen (Innen- und Außendienst)	Administrator können Aufzeichnung manipulieren (Änderung, Löschung von einzelnen Aufzeichnungen)	Daten	Manipulation von Informationen	1	3		Es wird die Auf-/Abschaltung der Bilder und das 4-Augen Login (inkl. der normalen logs. Backup, Aufschaltung) protokoliert. Zudem ist das Erstellen von Backups möglich. Logfiles speichern sämtliche Steuerungen und Zugriffe im Hintergrund und können abgerufen werden. Vertraulichkeitsvereinbarung / Verpflichtungen der städtischen Mitarbeiter*Innen	1	1	

Betrieb	Integrität	Löschen von Daten	- städtische Mitarbeiter*Innen (Innen- und Außendienst)	städtische Mitarbeiter*Innen greifen unrechtmäßig auf aufgezeichnetes Material zu oder Datenverlust, keine weitere Schritte im abfallrechtlichen Verfahren möglich	Daten	Manipulation von Informationen, Reputationsschaden für Stadt	2	3	5	Löschvorgang entsprechend den Vorgaben siehe verlinkten Bericht[1,2,6] [redacted]	1	1	2
	Integrität	Löschen von Daten durch Externe	- externe Mitarbeiter*Innen (beauftragte Firma für Videoüberwachung, Reinigungsfirma, externe Zusteller)	Unberechtigtes Löschen von Daten	Daten	Manipulation von Informationen, Reputationsschaden für Stadt	2	3	5	Es bestünde ausschließlich die Möglichkeit direkt am Rekorder über den Administratorzugang Daten zu löschen, jedoch kann das Kfz nicht aufgeschlossen werden (Zugang nur berechtigte städtische Mitarbeiter*Innen) und somit besteht keine Zugang zu den darin integrierten IT-Komponenten.[3]	1	1	2
	Integrität, Verfügbarkeit	Aufbewahrung der Verfahrensakte einschließlich Videomaterial (analoge Akte mit Videosequenz auf CD nur bei Bedarf)	städtische Mitarbeiter*Innen (Innen- und Außendienst) und externe Mitarbeiter*Innen (beauftragte Firma für Videoüberwachung, Reinigungsfirma, externe Zusteller)	Unberechtigter Zugriff	Daten	Manipulation von Informationen, Reputationsschaden für Stadt	2	3	5	Verschwiegenheitsverpflichtung besteht, Büros der Sachbearbeiter*Innen sind abgeschlossen[1]	1	1	2
	Integrität, Verfügbarkeit	Archivieren von Daten	städtische Mitarbeiter*Innen (Innen- und Außendienst)	Unberechtigter Zugriff	Daten	Reputationsschaden für Stadt	1	1	2	Nach Abschluss des Verfahrens erfolgt die Archivierung in geeigneten, abschließbaren Räumlichkeiten[1,7]	1	1	2
	Transparenz	Weitergabe von Informationen an betroffene Person (Anhörung, Akteneinsicht beantragen, Bußgeldbescheid)	städtische Mitarbeiter*Innen (Innen- und Außendienst)	unberechtigte Einsichtnahme	Daten	Verlust der Vertraulichkeit	1	1	2	Einsichtnahme des aufgezeichneten Videomaterials für Betroffenen vor Ort in Dienststelle oder Cloud und Übermittlung der Videosequenzen über virtuelle Poststelle, Cloud für Anwalt Rahmenbedingungen für den Informationsaustausch sind formal beschrieben[3,7]	1	1	2
	Transparenz	Informationsweitergabe an Anwalt der betroffenen Person, Staatsanwaltschaft, Gericht	externe Datenträger (Staatsanwaltschaft und Gericht, Betroffene, Anwalt)	Datenverlust und unberechtigter Zugriff	Daten	Manipulation von Informationen, Daten werden nicht oder nicht richtig übermittelt, dadurch drohender finanzieller Verlust (Datenverlust)	1	1	2	4-15 sensibilisiert und informiert die betroffenen Mitarbeiter*Innen, wie sie einen sicheren Datenexport vornehmen. Laut der beauftragten Firma können einzelne Sequenzen revisionssicher exportiert werden. Nutzen der virtuellen Poststelle Rahmenbedingungen für den Informationsaustausch sind formal beschrieben[3,7]	1	1	2
	Vertraulichkeit	Wartung Kfz	- städtische Mitarbeiter*Innen (Innen- und Außendienst)	Kfz ist unbeobachtet und Unberechtige können auf die verwendeten IT-Komponenten zugreifen. Dadurch entsteht ein Risiko, dass die IT-Komponenten missbraucht oder schützenswerte Informationen entwendet werden.	Systeme	Ausfall von Systemen, Manipulation von Informationen	1	2	3	Wartungs- und Reparaturarbeiten müssen von befugtem und qualifiziertem Personal in einer sicheren Umgebung durchgeführt werden; Entnahme der IT-Komponenten vor Wartung des Kfz durch berechtigtes Personal[9]	1	1	2
	Integrität	Update für die im Kfz integrierten IT-Systeme	- externe Mitarbeiter*Innen (beauftragte Firma für Videoüberwachung, Reinigungsfirma, externe Zusteller)	Unvollständige, unregelmäßige Updates	Systeme	Ausfall von Systemen, Manipulation von Informationen, Daten werden nicht oder nicht richtig übermittelt, dadurch drohender finanzieller Verlust (Datenverlust)	2	3	5	Updates müssen im Rahmen eines Service- und Wartungsvertrags aufgespielt werden. Eine 12-monatige Wartungslizenz ist zunächst auf dem Rekorder gültig. (Darüber hinaus wichtiger Hinweis: Gegegenbenfalls notwendige Updates nach der Pilotphase werden per Download oder Fernwartung zur Verfügung gestellt.)[8,9]	1	1	2
	Integrität, Verfügbarkeit	Temperatur und Luftfeuchte in Kfz	- Umwelteinflüsse (Naturgewalt)	Jedes Gerät hat einen Temperaturbereich, innerhalb dessen es ordnungsgemäß funktioniert. Über- oder unterschreitet die Raumtemperatur die Grenzen dieses Bereiches, können Geräte sowie IT-Komponenten ausfallen und der Betrieb kann gestört werden. Ähnliches gilt für die Luftfeuchtigkeit. In Fahrzeugen liegen unterschiedliche Voraussetzungen vor, die genau zu solchen Situationen führen können. So kann der Innenraum von in der Sonne abgestellten Fahrzeugen bis zu 70 Grad erreichen und somit den üblichen Temperaturbereich von z.B. Lithium Ionen Akkus überschreiten. Drohender Ausfall von integrierten IT-Komponenten innerhalb Kfz.	Systeme	Ausfall von Systemen	3	3	6	Für alle wesentlichen Situationen, die das Kfz und die darin vorhandenen Gegenstände mit Relevanz für die Informationssicherheit betreffen, wird eine Handlungsanweisung in Form von Checklisten vorliegen (je nach Szenario Tätigkeiten, z. B. Schutzmaßnahmen und Verantwortlichkeiten). Nachfolgend die Temparaturbeständigkeit der IT Komponenten: Kamera -20 - +50 Grad, VNB 3 +5 - +40 Grad[9]	1	1	2
	Intervenierbarkeit	Auskunft gegenüber Betroffenen	städtische Mitarbeiter*Innen (Innen- und Außendienst)	Die Betroffenen sind unzureichend informiert.	Prozesse	Reputationsschaden für Stadt	3	3	6	Flankierende Maßnahmen der Öffnetlichkeitsarbeit, bspw.: - Pressekonferenz - Hinweisschilder - Nutzen verschiedener Kommunikationskanäle, wie social media, Erklärfilm Abnahme des Konzepts inkl. der beschriebenen Maßnahmen durch LfDI und dadurch mehrfache Kontrolle/enge Begleitung der Pilotphase	1	1	2

Fußnoten

[1] CON.3 Datensicherungskonzept: Basis-Anforderung

[2] CON.6 Löschen und Vernichten: Basis-Anforderung

[3] CON.9 Informationsaustausch: Basis-/Standard-Anforderung

[4] DER.1 Detektion von sicherheitsrelevanten Ereignissen: Basis-Anforderung

[5] APP.6 Allgemeine Software: Basis-Anforderung

[6] SYS.4.3 Eingebettete Systeme: Basis-Anforderung

[7] SYS.4.5 Wechseldatenträger: Basis-Anforderung

[8] ND.2.1 Allgemeine ICS Komponente: Basis-Anforderung

[9] INF.11 Allgemeines Fahrzeug: Basis-Anforderung

Die Anforderungen von INF.9 Mobiler Arbeitsplatz sind in der einschlägigen DV der Stadt Ludwigshafen aufgegriffen.