POLIZEI

BADEN-WÜRTTEMBERG

POLIZEIPRÄSIDIUM MANNHEIM

Projektgruppe „Videoüberwachung Mannheim 2017“

- Datenschutzkonzept -

Dokumentenstand

Version	Datum	Änderungen	Autoren
1.0	14.03.2018	Erstfassung	[redacted]
1.1	18.05.2018	Ergänzung	[redacted]
1.2	20.06.2018	Ergänzung	[redacted]
1.3	10.12.2018	Aktualisierung	[redacted]
1.4	14.12.2018	Aktualisierung	[redacted]

Inhaltsverzeichnis

1 Kurzbeschreibung der Videoüberwachung

1.1 Allgemeine Kurzbeschreibung

Nach Auswertung der Straßen- und Betäubungsmittelkriminalität im Stadtgebiet Mannheim beabsichtigt das Polizeipräsidium Mannheim, verschiedene Kriminalitätsbrennpunkte mittels Videotechnik zu überwachen. Polizeilich erfolgen eine „konventionelle" Videoüberwachung nach § 21 Abs. 3 und 8 des Polizeigesetzes Baden-Württemberg (PolG BW) sowie eine automatische (Bild-)Auswertung nach § 21 Abs. 4 PolG BW.

Die Bilder der Videokameras werden unmittelbar in das Führungs- und Lagezentrum des Polizeipräsidiums Mannheim übertragen. Hier erfolgt die zentrale Videobeobachtung durch (geschulte) Polizeivollzugsbeamte. Anhand der erhobenen Bilder beurteilen diese Sachverhalte. Im Falle eines polizeilich relevanten Ereignisses können folglich die erforderlichen Interventionsmaßnahmen eingeleitet werden.

Zur Unterstützung der Videobeobachtung wird eine Software eingesetzt. Algorithmen werten die Bilder der Videokameras automatisch nach Verhaltensweisen aus, welche auf die Begehung einer Straftat hindeuten. Im Falle einer Erkennung durch Software werden die beobachtenden Polizeivollzugsbeamten unverzüglich auf den Sachverhalt hingewiesen. Auf Grundlage der aufgezeichneten Bilder können diese den Sachverhalt bewerten und die erforderlichen Interventionsmaßnahmen einleiten.

1.2 Zweck der Anwendung

Die Videoüberwachung dient der präventiven sowie repressiven Bekämpfung von Ordnungsstörungen und Kriminalität. Sie ist Informationsgrundlage für zielgerichtetes polizeiliches Handeln. Durch aktive Beobachtung und automatische Auswertung sollen Bedrohungslagen frühzeitig erkannt und Reaktionszeiten durch die Interventionskräfte erheblich verkürzt werden.

Durch die Videoüberwachung sollen die lokalen Brennpunktbereiche objektiv sicherer gemacht und vorrangig Delikte der Straßen- und Betäubungsmittel-kriminalität

nachhaltig reduziert werden sowie das subjektive Sicherheitsgefühl der Bevölkerung verbessert und örtliche Angsträume verringert werden.

Darüber hinaus können die gespeicherten Videoaufzeichnungen polizeiliche Ermittlungsmaßnahmen unterstützen und forcieren.

Zusammengefasst ist die Videoüberwachung vor allem für folgende Bereiche von wesentlicher Bedeutung:

- Gefahrenabwehr,
- vorbeugende Bekämpfung von Ordnungsstörungen,
- vorbeugende Bekämpfung von Straftaten durch erhöhten Entdeckungs- und Identifikationsdruck,
- Strafverfolgung und
- Personaleinsatz/-steuerung (Verkürzung der Interventionszeiten).

2 Dateiführende Stelle

Dateiführende Stelle ist das Polizeipräsidium Mannheim. Technisch betrieben wird die Videoüberwachung beim Polizeipräsidium Mannheim.
Die Daten der Videoüberwachung werden in einem autarken, kabelgebundenen Netzwerk übertragen und auf einem vom Landesnetz getrennten System gespeichert.

3 Verantwortliche Stelle

Das Polizeipräsidium Mannheim ist verantwortliche Stelle im Sinne der § 30 Abs. 1 Landesdatenschutzgesetz (LDSG) in der ab dem 21.06.2018 gültigen Fassung (im Folgenden: LDSG neu) in Verbindung mit § 48 PolG BW in Verbindung mit § 3 Abs. 3 LDSG in der bis zum 20.06.2018 gültigen Fassung (im Folgenden: LDSG alt).

Das Polizeipräsidium Mannheim trägt die Verantwortung für die Zulässigkeit, Richtigkeit und Aktualisierung der gespeicherten Daten.

Die der Datenspeicherung zugrunde liegenden Akten / Vorgänge werden beim Polizeipräsidium Mannheim geführt. Der Besitz der Videoaufzeichnungen für andere Zwecke im Sinne des § 21 Abs. 8 S. 2 PolG BW wird auf Vorgangsebene in ComVor dokumentiert.

4 Erhebung von Daten

4.1 Rechtsgrundlage der Erhebung

Rechtsgrundlage der „konventionellen" Videoüberwachung an öffentlichen Bereichen ist § 21 Abs. 3 i.V.m. Abs. 8 PolG BW. Zur Bewertung der videoüberwachten Bereiche als Kriminalitätsschwerpunkte wird auf das Fachkonzept verwiesen. Die installierten Videokameras nehmen Bilder auf, welche in der Folge beim Polizeipräsidium Mannheim gespeichert werden.

Die automatische (Bild-)Auswertung nach § 21 Abs. 4 PolG BW erfolgt in Echtzeit anhand bereits erhobener Daten. Folglich verarbeitet die Software lediglich bereits erhobenen Bilddaten und führt keine eigene oder weitere Erhebung durch.

4.2 Transparenzgebot

In den videoüberwachten Bereichen sind entsprechend § 21 Abs. 8 S. 1 PolG BW Hinweisschilder anzubringen (Anlage 1).

4.3 Erhobene Daten

4.3.1 Personenbezogene Daten

Durch die Videokameras können in unterschiedlicher Intensität personenbezogene Daten erhoben werden.

Bei der Erhebung ist zwischen statischen, nicht bedienbaren und steuerbaren Kameras zu unterscheiden. Beide Kameratypen sind in einer Grundeinstellung konfiguriert, welche die Bereiche in einer Übersicht aufnehmen. In der Folge werden

grundsätzlich niederschwellig personenbezogene Daten aufgenommen, da die konkrete Identifizierung einer Person nur bedingt möglich ist.
Im Falle eines relevanten Ereignisses können nur bedienbare Kameras für die gezielte Beobachtung bzw. Erhebung konkreter, personenbezogener Daten genutzt werden. Durch das Schwenken, Neigen und (optische) Heranzoomen bedienbarer Kameras ist im Einzelfall ein gesteigerter Grundrechtseingriff möglich.

4.3.2 Private Bereiche

Kameraausschnitte, die höchstpersönliche Lebensbereiche (bspw. Wohnungen oder Geschäftsräume) tangieren, sind durch technische Vorkehrungen (Verpixelung) von der Videobeobachtung ausgeschlossen, sodass ein Einblick in diese Bereiche nicht möglich ist.

Derzeit erfolgt die Verpixelung direkt in der Kamera (vgl. Technikkonzept Ziffer 7.6). Eine Kenntlichmachung bzw. „Entpixelung" vergangener bzw. bereits gefertigter Aufzeichnung ist nicht möglich.

Zukünftig ist geplant, die Verpixelung über die Videomanagementsoftware vorzunehmen, sodass die verpixelten Bereiche im Live-Stream unter Vorliegen der rechtlichen Voraussetzungen des § 23 PolG BW wieder sichtbar gemacht werden können. Eine nachträgliche Sichtbarmachung (bereits getätigter Aufnahmen) der verpixelten Bereiche ist technisch ausgeschlossen.
Eine Sichtbarmachung der verpixelten Bereiche im Live-Stream ist nur im Einzelfall zulässig, wenn andernfalls die Abwehr einer unmittelbar bevorstehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person gefährdet oder erheblich erschwert würde (vgl. § 23 Abs. 1 PolG BW).
Die Anordnungskompetenz liegt nach § 74a Abs. 4 Gerichtsverfassungsgesetz (GVG) bei der dort genannten Kammer des Landgerichts. Bei Gefahr im Verzug nach § 23 Abs. 3 Satz 8 PolG BW kann die Leitung des Polizeipräsidiums Mannheim (i.S.v. § 22 Abs. 6 PolG BW) die Anordnung treffen – die gerichtliche Bestätigung ist unverzüglich einzuholen (Ausnahme § 23 Abs. 4 PolG BW).
Bei Vorliegen der Anordnung kann die Verpixelung de-/aktiviert werden. Auf die Verhältnismäßigkeit ist zu achten; Aufnahmen des Kernbereichs privater

Lebensgestaltung sind nicht gestattet (§ 23 Abs. 5 PolG BW). Darüber hinaus bleiben sachverhaltsfremde Bereiche verpixelt.

Die Anordnungskompetenzen nach § 23 Abs. 3 PolG BW sind zwingend einzuhalten. Der organisatorische Ablauf ist in der Dienstanweisung „Videoüberwachung an kriminalitätsbelasteten Bereichen" des Polizeipräsidiums Mannheim (Az. PP MA 1102 VIDEO) erläutert.

4.3.3 Versammlungen

Bei Versammlungslagen im überwachten Bereich ist grundsätzlich die Videoüberwachung im betroffenen Bereich zu deaktivieren (sog. „Demoschaltung"), sofern nicht im Einzelfall die Voraussetzungen der §§ 12a, 19a Versammlungsgesetz erfüllt sind. Das Nähere regelt die unter Ziff. 4.3.2 genannte Dienstanweisung des Polizeipräsidiums Mannheim.

4.4 Angemessenheit des Verfahrens

Die Videoüberwachung ist geeignet, das Ziel der Verhinderung bestimmter, ortstypischer Straftaten zu fördern.
Die verantwortlichen Stellen müssen einzelfallbezogen, unter Würdigung des darin liegenden Grundrechtseingriffs prüfen und abwägen, ob die Kenntnisse aus den gespeicherten Videodateien unter Berücksichtigung des § 21 Abs. 8 S. 2 PolG BW (noch) zur Erfüllung der jeweiligen Aufgaben erforderlich sind.

4.5 Zeitliche Beschränkung der Maßnahme

Die Videoüberwachung ist nur zulässig, solange Tatsachen die Annahme rechtfertigen, dass an diesem Ort weitere Straftaten begangen werden („zeitliches Übermaßverbot").
Die Voraussetzungen für eine Fortsetzung der Videoüberwachung entfallen nicht allein durch einen Rückgang der registrierten Kriminalität. Stattdessen muss eine längerfristige Phase der Stabilisierung abgewartet werden.

Die Auswertung der aktuellen Kriminalitätslage hat daher immer im Rhythmus von einem Jahr zu erfolgen. Erst wenn die Kriminalitätslage über einen Zeitraum von mindestens zwei Auswertezeiträumen zeigt, dass die Voraussetzungen für einen Kriminalitätsschwerpunkt nicht mehr gegeben sind, ist die Videoüberwachung zu beenden.

5 Benutzer des Systems

Um den hohen datenschutzrechtlichen Voraussetzungen an eine Videoüberwachung Rechnung zu tragen, ist über die Einrichtung unterschiedlicher Benutzergruppen und differenzierter Rollen bzw. Zugriffsrechte sicherzustellen, dass nur befugte Personen Daten einsehen, kopieren, ändern oder löschen können und ihnen dies auch nur in dem für die Aufgabenerfüllung erforderlichen Umfang gestattet ist (minimale System-Rechte, sog. „Need-to-know-Prinzip").

Die zuvor erläuterten Ziele der Videoüberwachung und der damit verbundene Umgang mit Videoaufnahmen erfolgen nach einem abgestuften Rechtekonzept durch mindestens zwei Benutzergruppen (sog. „vier-Augen-Prinzip").
Im Kern können die von der Videokamera erhobenen Daten zunächst von einer Benutzergruppe (Beobachter) gesichert, aber nur durch eine andere, übergeordnete Benutzergruppe (Entscheider) exportiert bzw. gelöscht werden.

Für die Videoüberwachung sind nur fortgebildete bzw. eingewiesene Polizeivollzugsbeamte einzusetzen. Diese erhalten eine individuelle, am Aufgabenbereich orientierte Berechtigung

- zum Zutritt der erforderlichen Räumlichkeiten, in denen sich die Videotechnik befindet, und
- zur Benutzung der Videotechnik.

Die Berechtigung ist in der Dienstanweisung „Videoüberwachung an kriminalitätsbelasteten Bereichen" des Polizeipräsidiums Mannheim konkretisiert.

5.1 Benutzergruppen und Systemrechte

Der Zugriff auf erhobene Daten erfolgt zentral über die Videomanagementsoftware (VMS). In der VMS wurden vier Benutzergruppen mit jeweils unterschiedlichen Systemrechten angelegt. Nachfolgend eine Übersicht der Benutzergruppen und Systemrechte:

Systemrecht	Beobachter	Auswerter	Entscheider	Admin
Benutzerverwaltung	-	-	-	✓
Anmeldung	✓	✓	✓	✓
Live-Beobachten	✓	-	✓	✓
Kamera steuern	✓	-	-	✓
Wiedergabe / Spulen	✓	✓	✓	✓
Auswählen / Sichern	✓	-	✓	✓
Export / Löschen	-	-	✓	✓
Kamera de-/aktivieren	-	-	✓	✓
Lesen / Export Protokoll	-	-	-	✓

Tabelle 1: Übersicht der Benutzergruppen und deren Systemrechte

5.1.1 Gruppen im Active Directory

Eine Benutzergruppe ist die Gruppierung mehrerer Benutzer der Anwendung mit dem Ziel, ihre Berechtigungen zur Nutzung einzelner Funktionen der Software strukturiert zu verwalten.

Um eine Verbindung zwischen dem informationstechnischen Konzept der Benutzergruppen und der praktisch-organisatorischen Ebene herzustellen, werden sogenannte funktionsorientierte Benutzerrollen eingesetzt.

Das gewählte Modell ermöglicht der Administration die Berechtigungen innerhalb der Rollen bzw. Gruppen spezifiziert zu setzen.

Alle Nutzer des Systems werden gemäß ihrer organisatorischen Aufgabe bestimmten Benutzergruppen des Active Directory (AD) zugewiesen. Diese Benutzergruppen dienen dem Zweck, eine standardisierte Nutzungsrecht-Zuteilung zu gewährleisten, um Arbeitsabläufe und Geschäftslogik abbilden zu können.

Da die Gruppen innerhalb des Videomanagementsystems aus dem AD importiert werden, sind diese dort ebenfalls in gleicher Anzahl und unter gleicher Bezeichnung vorhanden.

5.1.2 Rollen im Active Directory

Eine Benutzerrolle fasst eine zu bestimmende Anzahl von Rechten zusammen. Anstatt jedem Benutzer Rechte einzeln zu vergeben, werden die Rechte gesammelt über diese Rolle an mehrere Benutzer zugewiesen.

Durch das „Single-Sign-On" wird die VMS automatisch mit der entsprechenden Rolle gestartet. Eine Personalisierung der Darstellung ist dabei nicht vorgesehen, da diese aufgrund der fachlichen Vorgaben entworfen wurde.

Um administrative Aufwände zu minimieren, ist der Benutzer berechtigt, systemseitige Meldungen zu schließen, sofern diese nicht zur VMS gehören.

Der benutzerseitige Zugriff auf die Windowsdatenstruktur ist ausgeblendet, da alle erforderlichen Speicherzugriffe über die VMS gesteuert und administriert werden.

Die Benutzer sind berechtigt den Dateiexplorer zu öffnen und zu nutzen. Bei Bedarf kann auch ein Neustart des Clientsystems durchgeführt werden.

Nutzerseitige Änderungen an der Systemspezifikation sind durch Richtlinie blockiert.

5.1.3 Profile im Videomanagementsystem

Die Profile der VMS entsprechen in ihrer Funktion weitestgehend den Rollen im Active Directory (AD). Durch die Profile erfolgt die Rechtevergabe auf Grundlage des Personalkonzepts. Weitergehende technische Details können innerhalb der sog. Anwendungsoptionen berechtigt werden. Analog der AD-Namenskonvention gibt es auch hier vier verschiedene Profile.

Beobachter

- Reservierung; Bedienung und Freigabe einer PTZ-Kamera
- Zugriff auf Übergangsspeicher (72h) nur über VMS möglich
- Zugriff auf Archivspeicher (4 Wochen)
- Bedienung der VMS für Live-Bilder und Wiedergabe von Videoaufnahmen
- Sicherung polizeilich relevanter Bild-/Videoaufnahmen (zur Verhinderung der automatisierten Überschreibung nach 72 Stunden)

- Zugriff auf Snapshots

Auswerter

- Sichtung von ausgewählten, gesicherten Aufzeichnungen
- Bedienung der VMS für die Wiedergabe ausgewählter Aufzeichnungen

Entscheider

- Reservierung; Bedienung und Freigabe einer PTZ-Kamera
- Sicherung polizeilich relevanter Bild-/Videoaufnahmen (zur Verhinderung der automatisierten Überschreibung nach 72 Stunden)
- Zugriff auf Snapshots
- Zugriff auf Archivspeicher (4 Wochen)
- Zugriff auf Übergangsspeicher (72h) nur über VMS möglich
- Bedienung der VMS für Live-Bilder und Wiedergabe von Videoaufnahmen
- Sicherung von Videoaufnahmen auf externen Datenträgern und die Weitergabe an die sachbearbeitende Dienststelle (Export)
- Manuelles Ein- und Ausschalten von Videokameras, bspw. bei öffentlichen Versammlungen (sog. „Demo-Schaltung")
- Manuelles Ein- und Ausschalten der Unkenntlichmachung von privaten Bereichen bzw. Geschäftsbereichen („Verpixelung"), unter Beachtung der rechtlichen Voraussetzungen [Anordnung nach §23 Abs. 3 PolG]

Admin

Vollzugriff und Berechtigung auf alle Inhalte. Das Auslesen oder der Zugriff auf das Protokoll der VMS erfolgt nur, sofern die rechtlichen Voraussetzungen dafür vorliegen.

5.2 Aufgaben der Benutzer

Die Aufgaben und Zuständigkeiten des für die Videotechnik eingesetzten Personals des Polizeipräsidiums Mannheim sind in der Dienstanweisung „Videoüberwachung an kriminalitätsbelasteten Bereichen" konkretisiert.

6 Speicherung von Beschäftigtendaten

6.1 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

Die Beschäftigtendaten werden in der VMS zur Gewährleistung der Datenschutzkontrolle, der Datensicherung und der Sicherstellung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage und hiermit in Zusammenhang stehenden Maßnahmen gegenüber Bediensteten (§§ 5 Abs. 2 Nr. 1 und Abs. 4, 15 Abs. 1 und 5 LDSG neu) gespeichert. Es erfolgen keine vergleichenden benutzerbezogenen statistischen Auswertungen.

6.2 Benutzerverwaltung

Um das Videomanagementsystem nutzen zu können, werden Benutzer -wie unter Ziffer 5.1.1 erläutert- aus der zentralen Benutzerverwaltung berechtigt. Bei einem Aufruf des Videomanagementsystems werden die Anwenderrechte aus dem AD ausgelesen und für die Nutzung umgesetzt.
In der Benutzerverwaltung befinden sich neben den Anwendern auch die Daten (z.B. Anschriften) und Rechte aller Dienststellen und Organisationseinheiten.

6.3 Ablauf der Berechtigungsvergabe

Die unter Ziffer 5 genannten Rechte werden von den Administratoren in der Benutzerverwaltung technisch umgesetzt. Die Berechtigungsvergabe erfolgt fachlich durch die Leitung der Dienststelle und technisch durch den Stabsbereich Technik.
Die Zugriffsberechtigung erfolgt über die Benutzerverwaltung im „Active Directory“. Alle Berechtigungen sind grundsätzlich restriktiv zu vergeben.

7 Rechtsgrundlage der Datenverarbeitung

Spezialgesetzliche Grundlagen für die Verarbeitung personenbezogener Daten in der Videoüberwachung sind:

- das Polizeigesetz Baden-Württemberg und
- die Strafprozessordnung

Das Landesdatenschutzgesetz Baden-Württemberg ist subsidiäres Recht und greift nur dort, wo keine spezialgesetzlichen Regelungen vorhanden sind.

7.1 Speicherung

Die Speicherung, Veränderung und Nutzung personenbezogener Daten von Betroffenen erfolgt zur polizeilichen Aufgabenerfüllung:

- für präventive Daten, nach §§ 37, 38 und 42 Abs. 3 PolG BW bzw.
- für repressive Daten nach § 481 Abs. 1 und 3, 483 Abs. 3 StPO i.V. m. den §§ 37, 38 PolG BW, § 42 Abs. 3 PolG BW.

7.2 Speicherfristen

Nach § 21 Abs. 8 S. 2 PolG BW sind Bild- und Tonaufzeichnungen unverzüglich, spätestens aber nach vier Wochen zu löschen, soweit sie im Einzelfall nicht zur Verfolgung von Straftaten oder von Ordnungswidrigkeiten von erheblicher Bedeutung, zur Geltendmachung öffentlich-rechtlicher Ansprüche oder nach Maßgabe des § 2 Abs. 2 PolG BW zum Schutz privater Rechte, insbesondere zur Behebung einer bestehenden Beweisnot, erforderlich sind.

7.2.1 Allgemeine Videoaufnahmen

Grundsätzlich werden alle beim Polizeipräsidium Mannheim durch die Videobeobachtung erhobenen Daten gespeichert und nach 72 Stunden automatisch durch Überschreiben gelöscht.

7.2.2 Polizeiliche relevante Videoaufnahmen

Eine über die 72 Stunden hinausgehende Speicherung relevanter Daten erfolgt nur nach vorheriger, erster Beurteilung und Sicherung der Videosequenz durch den Videobeobachter. Eine automatisierte Speicherung findet nicht statt.

Eine nachträgliche Einsichtnahme in die Allgemeinen Videoaufnahmen nach Ziffer 7.2.1 zur Sicherung der relevanten Daten darf nur erfolgen soweit es zur Erfüllung polizeilicher Aufgaben erforderlich ist

Ein nachträgliches Sichten der gespeicherten Videodaten ohne konkrete Verdachtsmomente ist nicht zulässig.
Ist bei der Antragstellung zur Sichtung die Tatzeit nicht konkret bekannt, kann auch ein Tatzeitraum gesichtet werden. Hierbei ist auf ein verhältnismäßiges Minimum zu achten.

Die von den Videobeobachtern markierten Bereiche werden für maximal vier Wochen gespeichert und in der Folge automatisiert gelöscht. Die markierten Videosequenzen sind zunächst relevante Daten gemäß § 21 Abs. 8 PolG BW. Der zuständige Bearbeiter prüft die betreffenden Inhalte und entscheidet zeitnah über deren Erhaltung. Erfolgt innerhalb von 4 Wochen keine Entscheidung über die weitere Verwendung der gesicherten Aufnahmen (Export als Beweismittel oder Löschen), werden diese automatisch gelöscht.

7.2.3 Beweiserhebliche Videoaufnahmen

Wird die Erforderlichkeit der Speicherung für die Verfolgung von Straftaten oder von Ordnungswidrigkeiten von erheblicher Bedeutung bejaht, erfolgt die weitere Speicherung nach § 21 Abs. 8 PolG BW, § 483 StPO. Hierzu werden die Daten unverzüglich auf einem externen Datenträger gesichert und anschließend automatisiert aus dem Videoüberwachungssystem gelöscht.

7.3 Weitergabe von Videodateien an polizeiliche Sachbearbeiter

Zugriffe von ermittelnden Polizeibeamten auf gespeicherte Daten sind schriftlich bei einem der beauftragten Bearbeiter gemäß dem Rollenkonzept zu beantragen.
Die Sicherung und Weitergabe der gefertigten Datenträger ist ausschließlich den nach dem Rollenkonzept berechtigten Personen vorbehalten.

Die Übergabe des externen Datenträgers ist gemäß der Dienstanweisung zu dokumentieren.

Zugriffe auf gesicherte Videodateien sind durch den polizeilichen Sachbearbeiter auf Vorgangsebene bzw. in den Ermittlungsakten zu dokumentieren.

7.4 Zulässigkeit der Datenübermittlung an externe Stellen

Die Zulässigkeit der Datenübermittlung ergibt sich insbesondere aus den folgenden Vorschriften:

- an Polizeibehörden und Polizeivollzugsdienst (§ 42 Abs. 1 PolG BW),
- an andere für die Gefahrenabwehr zuständige öffentliche Stellen (§ 42 Abs. 2 PolG BW),
- an andere öffentliche Stellen, insb. der Zoll, die Staatsanwaltschaften und Bußgeldbehörden, (§ 42 Abs. 7 PolG BW i.V.m. §§ 483, 487 StPO),
- an ausländische öffentliche Stellen, über- oder zwischenstaatliche Stellen (§ 43 ff. PolG BW),
- an Personen oder Stellen außerhalb des öffentlichen Bereiches (§ 44 PolG BW).

7.5 Automatische Auswertung

Die gespeicherten Bildaufnahmen können durch eine Software automatisch ausgewertet werden (§21 Abs. 4 PolG BW). Die Auswertung ist auf die Erkennung von Verhaltensweisen beschränkt, welche auf die Begehung einer Straftat hindeuten – eine biometrische Erkennung ist ausgeschlossen.

Hierfür wurde eine Software des Fraunhofer IOSB Karlsruhe an die VMS beim Polizeipräsidium Mannheim angekoppelt bzw. eingesetzt. Für die Übermittlung von Daten und die Weiterentwicklung der Software wird auf Ziffer 9 verwiesen.

Im Ergebnis der Auswertung erzeugt die Software einen Hinweis an die polizeilichen Videobeobachter in der VMS. Auf Grundlage des Hinweises können Videobeobachter das erkannte Ereignis bewerten und die erforderlichen, polizeilichen Maßnahmen einleiten.

Die Software nimmt keine Veränderungen an den erhobenen Daten vor. Eine weitere bzw. automatische Speicherung durch die Software wird nicht ausgelöst. Die zuvor genannten Abläufe der „konventionellen" Videoüberwachung bleiben bestehen.

7.6 Besondere Verarbeitungsregeln

Unter den Voraussetzungen der §§ 131-131c StPO können Aufzeichnungen der Videoüberwachung in die Öffentlichkeitsfahndung eingebunden werden (vgl. Ziffer 9.2 der Dienstanweisung).

8 Protokollierung

Jeder Zugriff auf das System wird automatisiert in einer Protokollierungsdatei erfasst. Die Informationen bleiben für zwölf Monate gespeichert. Anwendungsspezifisch werden Daten gemäß § 37 Abs.5 PolG BW und § 7 DVO PolG BW protokolliert.

8.1 Inhalt der Protokollierung

Die VMS „XProtect Corporate" erfasst automatisch nachfolgende Elemente:

- UTC-Zeit: Zeitpunkt der Eingabe nach der koordinierten Weltzeit. Diese berücksichtigt keine Sommer-/Winterzeit und liegt zwei/eine Stunde/n vor der Mitteleuropäischen Sommer- / Winterzeit in Mannheim.

- Lokalzeit: Zeitpunkt der Eingabe nach der lokalen Uhrzeit in Mannheim (Mitteleuropäische Sommer- oder Winterzeit berücksichtigt).
- Beschreibung: Die nähere Beschreibung der protokollierten Eingabe, welche auch die Örtlichkeit beinhaltet (z.B. Mannheim-Hauptbahnhof).
- Kategorie: Die kategorische Erfassung bzw. Art der Eingabe. Diese umfassen Alarme die durch Manipulationen ausgelöst wurden sowie Zugriffe auf die Smartmap, die PTZ-Kameras und administrative Systemeingaben.
- Berechtigung: Verweigerung oder Gewährung der Eingabe.
- Benutzer: Name des Benutzers, der die Protokollierung verursachte.
- Adresse des Benutzers: Endgerät, von welchem der Benutzer die Protokollierung verursachte. Diese wird als IP4-Adresse ausgegeben.
- Ressourcentyp: Art des Endgerätes, welches bedient wurde.
- Ressourcenname: Kamera bzw. Switch über den die Daten geführt wurden.
- Ressourcenhost: Änderungen der Darstellung der VMS an den Monitoren.

8.2 Umfang der Protokollierung

8.2.1 Eingaben des Benutzers

- An-/Abmeldung an die VMS
- Auswahl / Bedienung einer Kamera über die VMS
- Aktivieren / Deaktivieren einer Kamera
- Aktivieren / Deaktivieren der Verpixelung über die VMS
- Zugriff auf die Aufzeichnung einer Kamera
- Bearbeiten einer Aufzeichnung
- Verlängern der Speicherfrist einer Aufzeichnung
- Export einer Aufzeichnung
- Löschen einer Aufzeichnung
- Zu-/Eingriffe an den Einstellungen der VMS (durch Admin)

8.2.2 Technische Vorgänge

- Automatische Rückführung einer Kamera in die Grundeinstellung (bei Inaktivität),
- automatische Löschung von Aufnahmen nach Verstreichen gesetzlicher Speicherfrist,

- Systemfehler,
- Systemabstürze.

8.3 Zufallsprotokollierung

Da eine 100%-Protokollierung erfolgt, findet keine zusätzliche Zufallsprotokollierung statt.

8.4 Auswertung der Protokolldaten

8.4.1 Zwecke der Protokolldatenauswertung

Der Abruf von Protokolldaten ermöglicht umfassende Einblicke. So kann im Nachhinein u.a. rekonstruiert werden, wer zu welchem Zeitpunkt welche Daten abgerufen hat.
Nach § 48 PolG BW i.V.m. § 5 Abs. 4 LDSG neu dürfen Protokolldaten grundsätzlich nur für den (Erhebungs-)Zweck, mithin zur Aufrechterhaltung von Datenschutz und Datensicherheit sowie für hiermit in Zusammenhang stehenden (Kontroll-) Maßnahmen gegenüber Bediensteten genutzt werden.

Die im Rahmen der Videoüberwachung gespeicherten Protokollierungsdaten unterliegen somit einer strikten Zweckbindung. § 37 Absatz 5 PolG BW durchbricht die in § 5 Abs. 4 LDSG neu festgelegte Zweckbindung.

Eine Auswertung der Protokolldaten ist daher nur zu folgenden Zwecken zulässig:

- zu Zwecken der Datenschutzkontrolle (§ 5 Abs. 4 LDSG neu),
- für Zwecke der Datensicherheit (§ 5 Abs. 4 LDSG neu),
- zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage (§ 5 LDSG neu),
- wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist oder
- wenn Anhaltspunkte dafür vorliegen, dass ohne ihre Verarbeitung die vorbeugende Bekämpfung oder Verfolgung von Straftaten mit erheblicher

Bedeutung (§ 22 Absatz 5 PolG BW) aussichtslos oder wesentlich erschwert wäre.

Beschäftigte haben grundsätzlich das Recht, eine Auswertung ihrer Protokolldaten zu verlangen, wenn sie ein berechtigtes Interesse geltend machen (z. B. zur Ausräumung des Verdachts der unbefugten Nutzung des Videoüberwachungssystems).

Die Erstellung von Statistiken zur Untersuchung der Systemauslastung bzw. des systemtechnischen Verhaltens der Videoüberwachung ist zulässig.
Statistische Auswertungen, die Rückschlüsse auf das Arbeitsverhalten einzelner Nutzer ermöglichen, sind unzulässig. Eine zeitlich unbegrenzte Vollkontrolle ist unzulässig.

8.4.2 Antrag zur Protokolldatenauswertung

In strafrechtlichen Ermittlungsverfahren darf die Auswertung der Protokolldaten nur auf richterlichen Beschluss erfolgen.
In arbeits- bzw. disziplinarrechtlichen Angelegenheiten darf die Auswertung der Protokollierungsdatei nur auf Anweisung des Dienstvorgesetzten und nach Prüfung des Antrages durch die/den behördliche/n Datenschutzbeauftragte/n erfolgen.
Der Antrag auf Auswertung der Protokolldaten ist schriftlich zu begründen. Im Antrag sind folgende Daten zu nennen:

- Antragssteller
- Sachbearbeiter
- Dienststelle
- Organisationseinheit
- Az. / Tgb.-Nummer
- Grund / Anlass gemäß § 37 Abs. 5 PolG BW oder § 5 Abs. 4 LDSG neu
- Zeitraum der Auswertung
- Dinglichkeit der Auswertung (niedrig/mittel/hoch)
- Sachverhaltsdarstellung

Die Darstellung des Sachverhalts muss hierbei eine Prüfung ermöglichen, ob die Voraussetzungen des § 37 Abs. 5 PolG BW bzw. § 5 Abs. 4 LDSG neu vorliegen und

die Genehmigung der Protokolldatenauswertung angeordnet werden darf (§ 7 DVO PolG BW).

Der betroffene Beschäftigte ist über die Protokolldatenauswertung zu informieren. Zusätzlich muss der/die Vorsitzende des örtlichen Personalrates hierüber informiert werden, sofern der betroffene Beschäftigte nicht widerspricht.

8.4.3 Auswertung

Bei einem konkreten Missbrauchsverdacht dürfen Protokolldaten auf Anordnung des Dienstvorgesetzten nur durch einen besonders beauftragten Beschäftigten ausgewertet werden.

8.5 Löschung der Protokolldaten

Die Daten der Protokolldatei werden zwölf Monate vorgehalten und danach automatisiert gelöscht.

9 Auftragsverarbeitung

9.1 Polizei - IZLBW

Die Videoüberwachung wird in einem vom landesnetz vollständig autarken System betrieben. Eine Auftragsverarbeitung durch das Informatikzentrum Landesverwaltung Baden-Württemberg (IZLBW) findet daher nicht statt.

9.2 Polizei - Fraunhofer IOSB

Das Fraunhofer IOSB entwickelt im Auftrag des Polizeipräsidiums Mannheim eine algorithmenbasierte Bildauswertung. Zur Entwicklung und Weiterentwicklung der Algorithmen werden hierfür relevante Daten durch das Fraunhofer IOSB übermittelt und verarbeitet. Diese Auftragsverarbeitung zwischen dem Land Baden-Württemberg, vertreten durch das Polizeipräsidium Mannheim, und dem Fraunhofer IOSB wurde vertraglich geregelt (Anlage 2).

9.3 Polizei als Auftragnehmer

Eine Datenverarbeitung, bei der die Polizei als Auftragnehmer tätig wird, findet in der Videobeobachtung nicht statt.

10 Technisch organisatorische Maßnahmen

10.1 Zutrittskontrolle

Ein unbefugter Zutritt in Räumlichkeiten, welche für die Videoüberwachung relevant sind, ist zu verhindern.
Die Nutzung des Videoüberwachungssystems erfolgt ausschließlich im Hauptdienstgebäude des Polizeipräsidiums Mannheim am Standort L6, 1 in 68161 Mannheim. Hierbei sind folgende Räumlichkeiten relevant:

[redacted]

Der Zutritt in die Diensträume des Polizeipräsidiums Mannheim erfolgt über elektronisch gesicherte Zugänge. Beschäftigte des Polizeipräsidiums Mannheim erhalten eine individuelle, dem Aufgabenbereich entsprechende, elektronische Zutrittsberechtigung („Chip"). Die Berechtigung kann tagesaktuell geändert werden. Darüber hinaus sind Räume, in denen die Servertechnik der Videoüberwachung installiert ist, mit einem Schlüsselsystem gesichert.

[redacted]

Der Zutritt in den Sicherheitsbereich des Führungs- und Lagezentrums (FLZ) ist nur Berechtigten vorbehalten. Berechtigte in diesem Sinne sind:

- Beschäftigte des FLZ und
- sonstige Polizeiangehörige mit dienstlichem Auftrag.

Der Zutritt von Dritten (bspw. Besuchern) ist auf das notwendige Maß zu beschränken und nur nach Feststellung von deren Identität zulässig. Das Vorliegen eines berechtigten Zutritts ist vor Betreten des Sicherheitsbereiches nachzuweisen. Die Begleitung von Besuchern durch einen Berechtigten ist sicherzustellen. Sonstige Personen (z.B. Handwerker) sind grundsätzlich bei ihrer Tätigkeit im Sicherheitsbereich zu beaufsichtigen.

10.2 Zugangskontrolle

Das Eindringen Unbefugter in das Videoüberwachungssystem ist zu verhindern.

10.2.1 Kamerastandorte

Alle eingesetzten Kameras unterstützen neben einer Vielzahl von Standard-Protokollen die für den Betrieb ausgewählten Sicherheitsprotokolle HTTPS und SSL.

[redacted]

[redacted]

10.2.2 Datenübertragung

[redacted]

10.2.3 Zugang zur Datenverarbeitung

Die notwendigen Überlegungen, wer zu welchen Zwecken Zugang zu den Videoüberwachungssystemen, einzelnen Dateiablagen oder Anwendungen haben soll und wie das Verfahren zur Gewährung dieser Rechte ausgestaltet sein soll, werden in Ziffer 5 dieses Konzeptes dargestellt.

10.3 Zugriffskontrolle

Zentral für die angemessene Umsetzung der Zugriffskontrolle ist die gesteuerte und vorhersehbare Vergabe von Nutzungsberechtigungen. Nur derjenige, der Daten aus der Videoüberwachung tatsächlich für seine Tätigkeit benötigt, soll auch auf diese Informationen zugreifen können. Die entsprechend differenzierte Berechtigungsvergabe ist in Ziffer 5.1 erläutert.

Bei der Verwendung externer Datenträger und Endgeräte wie USB-Sticks, Notebooks oder Kameras ist die Datensicherheit durch den Einsatz eines entsprechenden Verschlüsselungsverfahrens sicherzustellen.
Hierfür erfolgt der Export von Daten nicht in einem Standardformat, sondern in einem eigenen Format der VMS. Die exportierte Datei ist nur über die VMS abrufbar, von der ein Abspielprogramm im Zuge des Exports mitkopiert wird. Das „mitkopierte" Abspielprogramm der VMS gestattet nur Lesezugriffe.

10.4 Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten während des Transports oder der Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung erfolgt ist.
Um eine missbräuchliche Nutzung von Daten zu verhindern, hat eine Übertragungskontrolle, eine Transportkontrolle und eine Übermittlungskontrolle stattzufinden.
Im Rahmen der Weitergabekontrolle werden zur Absicherung des physischen Transports der Daten auf einem externen Datenträger folgende Maßnahmen getroffen:

- Verschlüsselung der Datenträger und
- Übergabe an sachbearbeitende Polizeivollzugsbeamte bzw.
- Übergabe an zuverlässigkeitsüberprüfte Mitarbeiter des Fraunhofer IOSB.

Die Weitergabe ist durch organisatorische Kontrollmaßnahmen zu dokumentieren.

10.5 Eingabekontrolle

Um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in das Videoüberwachungssystem eingegeben, verändert oder entfernt worden sind, erhalten die in Ziffer 5 genannten Berechtigten individuelle, personalisierte Kennungen.

Eine Weitergabe von persönlichen Anmeldeinformationen an andere oder die auch noch so kurzfristige Arbeit unter fremder Kennung ist grundsätzlich untersagt.

Die Erhebung, Verarbeitung und Nutzung der Daten im Videoüberwachungssystem werden umfassend protokolliert (vgl. Ziffer 8).

10.6 Auftragskontrolle

Durch die Auftragskontrolle wird die weisungsgemäße Durchführung der Auftragsverarbeitung sichergestellt.

Hierbei werden insbesondere die folgenden Maßnahmen umgesetzt:

- eindeutige Vertragsgestaltung, insbesondere Abgrenzung der Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer und Festlegung der durchzuführenden Kontrollmaßnahmen,
- klare und eindeutige Erteilung von Weisungen (in schriftlicher Form),
- Festlegung der zur Erteilung und zum Empfang von Weisungen berechtigten Personen,
- Kontrolle der technischen und organisatorischen Sicherheitsmaßnahmen, welche bei dem Auftragnehmer getroffenen werden,
- Regelung des Einsatzes von Unterauftragnehmern,
- Verpflichtung der Beschäftigten des Auftragnehmers auf das Datengeheimnis,
- Benennung eines Datenschutzbeauftragten bei dem Auftragsverarbeiter.

Die Umsetzung erfolgt durch die Auftragsvereinbarungsvereinbarung (Anlage 2).

10.7 Verfügbarkeitskontrolle

[redacted] Das Backup bezieht sich ausschließlich auf die Daten, welche auf dem Server gespeichert sind. Diese umfassen das gesamte Servergrundsystem sowie dessen Konfiguration, die Benutzerdaten, die Protokolldateien, die VMS sowie deren Datenbanken. Ein Backup gespeicherter Videoaufnahmen (Übergangsspeicher- und Archivspeicherbereich) ist nicht vorgesehen.

10.7.1 Grundsystem-Backup

Dies bezeichnet die einmalige Sicherung der konfigurierten Images der Server, der VMS sowie des Aufzeichnungsservers mitsamt dessen Datenbank, inklusive der Konfigurationsdaten.

10.7.2 Protokoll-Backup

Wie unter Ziffer 8 erläutert, werden alle Protokolle und Log-Dateien der Hosts, Clients und der Videomanagementsoftware kontinuierlich ergänzt.

10.7.3 Backup-Intervalle

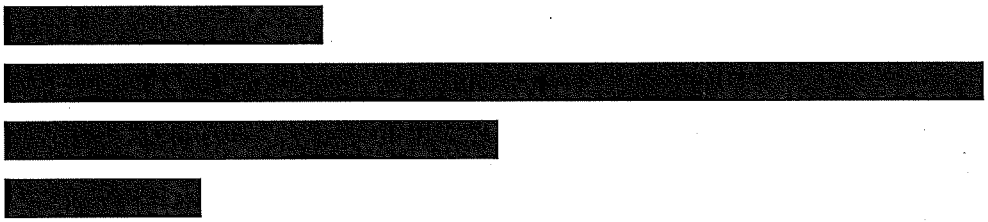
Das Protokoll-Backup erfolgt in Form einer wöchentlichen Vollsicherung und einer täglichen Differenzsicherung. Zusätzlich findet eine monatliche Vollsicherung statt. Mit Ablauf von Monat zwei werden lediglich die wöchentlichen Vollsicherungen und täglichen Differenzsicherungen aus Monat eins gelöscht; die monatliche Vollsicherung bleibt erhalten. Die maximale Speicherdauer für die monatliche Vollsicherung beträgt 12 Monate. Somit werden maximal 12 monatliche Vollsicherungen, sowie die wöchentlichen Vollsicherungen und die täglichen Differenzsicherungen der vergangenen zwei Monate auf dem Speicher abgelegt sein.

	Einmalige Vollsicherung	Tägliche Differenzsicherung	Wöchentliche Vollsicherung	Monatliche Vollsicherung

	(unbegrenzt)	(2 Monate)	(2 Monate)	(1 Jahr)
Grundsystem-Backup	✓			
Protokoll-Backup		✓	✓	✓

10.8 Trennungsgebot

Das Architekturmodell der Videoüberwachung gliedert sich in:



Zur Videodatensicherung wird das Speichersystem in zwei Speicherbereiche unterteilt. Den Übergangsspeicher (72 Stunden) und den Archivspeicher (vier Wochen). Es werden zunächst immer alle Videodaten auf dem Übergangsspeicher gespeichert. Dadurch wird gewährleistet, dass der Videobeobachter bestimmte Videosequenzen nach dem Eintreten eines Verdachts unmittelbar einsehen und letztlich unter Verdacht als vermeintliche Straftat auf dem Archivspeicher sichern bzw. archivieren kann. Alle nicht archivierten Daten, also jene auf dem Übergangsspeicher, werden nach 72 Stunden automatisch überschrieben. Alle auf konkreten Verdacht auf dem Archivspeicher gesicherten Daten werden nach vier Wochen automatisch gelöscht. Innerhalb dieses Zeitraums muss ein Benutzer der Gruppe Auswerter/Entscheider, den auf dem Archivspeicher abgelegten Verdachtsfall bewerten und bestätigen. Soweit eine Straftat vorliegt bzw. die Videosequenz ein Beweismittel darstellt, wird diese nach Sichtung durch den Auswerter (Sachbearbeiter) von einem Entscheider auf einen externen, im Vorfeld bereinigten, Datenträger exportiert. Es können in Abhängigkeit von der Datenmenge DVD, BluRay-Disk oder USB-Speichermedien eingesetzt werden.

Zur Systemsicherung (Protokollierung der Log-Dateien der Hosts, Clients, des Videomanagementsystems und deren Nutzern) wird ein gesonderter Speicher genutzt (Backup).

11 Betroffenenrechte

11.1 Recht auf Auskunft

Betroffene haben nach §§ 45 und §§ 48 PolG i.V.m. § 21 Abs. 1 S. 1 LDSG alt grundsätzlich Anspruch auf Auskunft zu den über ihn gespeicherten Daten. Auf Antrag des/der Betroffenen wird unentgeltlich Auskunft über die zu ihnen gespeicherten Daten gegeben (§21 Abs. 1 Satz 1 LDSG alt).
Betroffene haben bei der Auskunft eine Pflicht zur Mitwirkung. Die Umstände bzw. die betroffenen, personenbezogenen Daten müssen näher beschrieben werden (§ 21 Abs. 2 LDSG alt).
Bezieht sich ein Antrag auf eine Ereigniszeit, die über 72 Stunden in der Vergangenheit liegt, wurden die Daten regelmäßig gelöscht. Eine Auskunft kann dann nicht mehr erteilt werden.

11.2 Recht auf Löschung

Nicht relevante Aufzeichnungen im Sinne des § 21 Abs. 8 S. 2 PolG BW werden spätestens nach 72 Stunden automatisch gelöscht. Grundsätzlich werden präventive Aufzeichnungen nach vier Wochen automatisch gelöscht, sofern sie nicht beweiserheblich i.S.v. § 21 Abs. 8 S. 3 PolG BW sind.

11.3 Benachrichtigung

Eine Pflicht zur Benachrichtigung besteht nach § 14 Abs. 3 Nr. 1 LDSG alt in Verbindung mit § 21 Abs. 3 PolG BW nicht.

Werden ausnahmsweise Daten nach § 23 Abs. 1 PolG BW erhoben (vgl. 4.3.2) sind die Betroffenen nach § 23 Abs. 6 PolG BW zu benachrichtigen.

11.4 Recht auf Anrufung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Wer der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch die Videoüberwachung in seinen Rechten verletzt worden zu sein, kann sich an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg wenden.

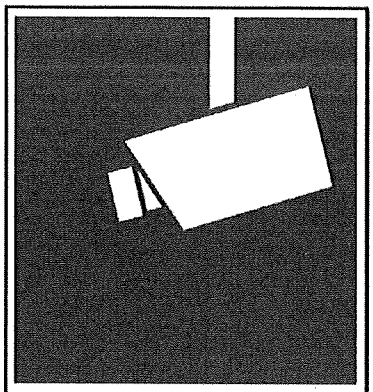
12 Verarbeitungsverzeichnis

Für jede installierte Kamera wird ein Eintrag in das Verarbeitungsverzeichnis erstellt.

gez. [redacted]
Projektleiter

Anlagen

Anlage Nr. 1 Hinweisschild Videoüberwachung



Zu Ihrer Sicherheit!

POLIZEI BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM MANNHEIM

STADT MANNHEIM

Name und Kontaktdaten der Verantwortlichen:
Polizeipräsidium Mannheim
L 6,1, 68161 Mannheim
Zuständige Aufsichtsbehörde:
Der Landesbeauftragte für den Datenschutz und die Informationssicherheit
Königstraße 10a, 70173 Stuttgart

Kontaktdaten des Datenschutzbeauftragten:
Behördlicher Datenschutzbeauftragter des Polizeipräsidiums Mannheim
L6,1, 68161 Mannheim
E-Mail: mannheim.pp.bdsb@polizei.bwl.de

Zwecke und Rechtsgrundlage der Datenverarbeitung:
Die Videoüberwachung dient dem Zweck der Gefahrenabwehr und der vorbeugenden Kriminalitätsbekämpfung (§ 21 Abs. 3, 4 und 8 Polizeigesetz BW).
Versammlungen werden grundsätzlich nicht videoüberwacht, eine Videoüberwachung erfolgt nur bei Vorliegen der Voraussetzungen nach den §§ 12a, 19a des Versammlungsgesetzes.

Rechte Betroffener:
Hinsichtlich des Rechts auf Auskunft, Berichtigung oder Löschung von Daten gelten die §§ 45 bis 48 des Polizeigesetzes BW i.V.m. dem Landesdatenschutzgesetz BW in der Fassung vom 18..September 2000.

Speicherdauer:
Gespeicherte Daten werden automatisiert nach 72 Stunden gelöscht, sofern die weitere Speicherung nicht im Einzelfall nach Maßgabe von § 21 Abs. 8 S. 2 Polizeigesetz BW erforderlich ist.

Über den QR-Code („Quick Response"-Verknüpfung) können online weitere Informationen über die Videoüberwachung abgerufen werden. Die Information ist neben der deutschen auch in der englischen und türkischen Sprache hinterlegt.

Vereinbarung zur Auftragsverarbeitung

Als Anlage zum [redacted]

- nachfolgend „Hauptvertrag" -

zwischen dem

Polizeipräsidium Mannheim, vertreten durch [redacted]

- nachfolgend „Auftraggeber / Verantwortlicher" -

und dem

Fraunhofer IOSB, [redacted]

- nachfolgend „Auftragsverarbeiter" -

- beide nachfolgend gemeinsam „Vertragsparteien" -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhalt

Präambel
Die Vertragsparteien sind mit dem Hauptvertrag ein Auftragsverarbeitungsverhältnis eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben des Landesdatenschutzgesetzes (LDSG) in der Fassung vom 18. September 2000 (a.F.; § 48 des Polizeigesetzes – PolG -, § 30 Absatz 1 LDSG vom 12. Juni 2018) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich
Die Vereinbarung gilt für die Verarbeitung aller personenbezogenen Daten (im Folgenden: Daten), die Gegenstand des Hauptvertrags sind oder im Rahmen von deren Durchführung anfallen oder dem Auftragsverarbeiter bekannt werden. Nicht hierunter fallen Daten von Mitarbeitern des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

§ 2 Konkretisierung des Auftragsinhalts
(1) Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten bestimmen sich nach dem Hauptvertrag nebst dessen Anlagen sowie den nachfolgenden Vereinbarungen.

(2) Gegenstand der Verarbeitung durch den Auftragsverarbeiter sind Videoaufnahmen, die im Rahmen der polizeilichen Videoüberwachung gemäß § 21 Absatz 3 des Polizeigesetzes (PolG) erhoben und dem Auftragnehmer zur Vertragserfüllung zur Verfügung gestellt werden.

(3) Betroffen sind alle Personen, die sich zum Zeitpunkt eines relevanten Ereignisse im Sinne des § 21 Absatz.. 4 und 8 PolG im videoüberwachten Bereich aufhalten.

§ 3 Verantwortlichkeit und Weisungsbefugnis
(1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich (§ 3 Absatz 3, § 7 Absatz 1 LDSG a.F.). Er kann jederzeit die Herausgabe, Berichtigung, Anpassung oder Löschung der Daten sowie die Einschränkung der Verarbeitung verlangen.

(2) Um den Schutz der Rechte der betroffenen Personen zu gewährleisten, unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch die Sicherstellung geeigneter technischer und organisatorischer Maßnahmen.

(3) Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, um ihre Datenschutzrechte geltend zu machen, leitet der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiter.

(4) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, es sei denn, er ist gesetzlich zu einer anderen Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen

diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete schriftliche, elektronische oder mündliche Anordnung des Verantwortlichen. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch den Hauptvertrag definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(5) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird.

(6) Weisungsberechtigt auf Seiten des Auftraggebers ist [redacted] Zur Entgegennahme von Weisungen auf Seiten des Auftragsverarbeiters ist [redacted] Für Weisung zu nutzende Kommunikationskanäle: [redacted] Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für die Geltungsdauer des Hauptvertrages von fünf Jahren und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(7) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder betroffene Personen darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher Zustimmung durch den Verantwortlichen erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt.

(8) Der Verantwortliche führt das Verfahrensverzeichnis gemäß § 11 LDSG (a. F.). Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Artikel 30 Absatz 2 der Datenschutz-Grundverordnung (DSVGO) ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(9) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich im Geltungsbereich des Grundgesetzes statt.

(10) Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit, Home Office, mobiles Arbeiten) bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann.

§ 4 Beachtung gesetzlicher und vertraglicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen. Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu bei Bedarf entsprechende Informationen zur Verfügung.

(3) Beim Auftragsverarbeiter ist als Beauftragter für den Datenschutz [redacted] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht.

(5) Der Auftragsverarbeiter hat die mit der Datenverarbeitung befassten Personen bei der Aufnahme ihrer Tätigkeit zu verpflichten, personenbezogene Daten, die ihnen im Rahmen der Vertragserfüllung zur Kenntnis gelangen, nicht unbefugt zu verarbeiten (Datengeheimnis). Die mit der Datenverarbeitung befassten Personen sind zudem nach dem Verpflichtungsgesetz auf die gewissenhafte Erfüllung ihrer Obliegenheiten zu verpflichten. Der Auftragsverarbeiter teilt diese Personen dem Auftraggeber mit. Die Verpflichtung erfolgt durch das Polizeipräsidium Mannheim. Der Auftragsverarbeiter sichert zu, dass er mit der Durchführung der Arbeiten nur Mitarbeiter beschäftigt, die nach Satz 1 und Satz 2 schriftlich belehrt wurden. Die Verschwiegenheitspflicht besteht auch nach Beendigung dieser Vereinbarung fort.

(6) Auf Grundlage des Auftragsverhältnisses entwickelte Ergebnisse dürfen, sofern im Einzelfall polizeitaktische Erwägungen nicht entgegenstehen, nach vorheriger Information und im Einvernehmen mit dem Auftraggeber, veröffentlicht werden. Eine Veröffentlichung der im Rahmen des Auftragsverhältnisses verarbeiteten personenbezogenen Daten ist ausgeschlossen.

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in dem Anhang „Technisch-organisatorische Maßnahmen" zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang ist Gegenstand dieser Vereinbarung.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technisch-organisatorische Maßnahmen" festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere Überprüfungen/Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Artikel 40 DSVGO, einer Zertifizierung nach Artikel 42 DSVGO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Artikel 41 Absatz 4 DSGVO, den Widerruf einer Zertifizierung gemäß Artikel 42 Absatz 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(4) Der Verantwortliche kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

(5) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 benötigt.

(6) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Absatz 2 DSVGO.

§ 7 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen.

(3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

§ 8 Subunternehmen

(1) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmen) nur mit vorheriger ausdrücklicher schriftlicher Zustimmung des Verantwortlichen in Anspruch nehmen

(2) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

(3) Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortlichen berechtigt, auf schriftliche Anforderung vom Auftragsverarbeiter Auskunft über den Inhalt des mit dem Subunternehmen geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten.

(4) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

§ 9 Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich, der/dem Datenschutzbeauftragten des Verantwortlichen sowie der zuständigen Aufsichtsbehörde zur Erfüllung ihrer jeweiligen gesetzlichen zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte der Genannten einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiter anweisen, mit den Genannten zu kooperieren, insbesondere deren Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 10 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse (z.B. Diebstahl) gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(3) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(4) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

Datum, Ort	Datum, Ort
Unterschrift (Verantwortlicher)	Unterschrift (Auftragsverarbeiter)
Name, Vorname, Funktion	Name, Vorname, Funktion

Anhang „Technisch-organisatorische Maßnahmen“

zur Vereinbarung zur Auftragsverarbeitung vom [*Datum*]
zwischen *dem Polizeipräsidium Mannheim*
und dem Fraunhofer IOSB

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.
Der Auftragsverarbeiter verpflichtet sich zur Gewährleistung eines Informationssicherheitsmanagements nach ISO 27001.

§ 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragsverarbeiters

Der Auftragsverarbeiter wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen

(1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	*Zutrittskontrolle zum Gelände, incl. Pförtner und Wachpersonal.* *Zusätzliches Zutrittskontrollsystem für Serverräume*
2.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	*Durchgängiges RBAC für Zugriffsrechte, Passwortrichtlinie etabliert.* *Verpflichtendes IT-Sicherheitskonzept für alle Mitarbeiter.*
3.	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	*siehe 2 - zusätzlich Protokollierung von Zugriffen* *Nutzung von Standardverfahren, eingeschränkte Lese- und Schreibrechte.* *Über das ERP-System und Fraunhoferweite und institutslokale Directories sowie Rollenverwaltungssysteme wird sichergestellt, dass nur Berechtigte Zugang zu den Daten erhalten.* *Eigene getrennte Ablagen für die Daten.* *Daten werden als Verschlusssache im Sinne der einschlägigen Konzepte des Auftragsverarbeiters deklariert* *Bei Aussonderung der IT-Systeme, auf denen Daten des Auftraggebers verarbeitet wurden, werden die Datenträger nach Schutzklasse 3 / Sicherheitsstufe 5 gemäß DIN 663399 physikalisch vernichtet oder dem Auftraggeber zur physikalischen Vernichtung zur Verfügung gestellt..*
4.	**Weitergabekontrolle** Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	*Daten werden mittels verschlüsselter Festplatten persönlich ausgetauscht* *Eine Übermittlung findet nicht statt* *Übergabe nur an zuvor benannte Personen* *Übergabe wird protokolliert.* *Eingang der Daten bei Fraunhofer und die laufende Verwendung werden dokumentiert*

5.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	• *Siehe 2 und 3 - zusätzlich Protokollierung von Zugriffen.*
6.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.	• *Etabliertes Risikomanagement laut ISMS.* • *Fehler und Auffälligkeiten in der Datenverarbeitung werden an den IT-Sicherheitsbeauftragten gemeldet und danach entsprechend des ISMS verfolgt.* • *Eindeutige Vertragsregelung nach der Auftragsverarbeitungsvereinbarung, regelmäßige Überprüfung i.R.d. Berichtspflicht.* • *Die Auftragsverarbeitung erfolgt ausschließlich durch zum Datengeheimnis und nach dem Verpflichtungsgesetz belehrte Mitarbeiter des Auftragsverarbeiters* • *(5) Der Auftragsverarbeiter gewährleistet dem Informationssicherheitsbeauftragten des Auftraggebers, nach erfolgter vorheriger Absprache, eine Einsichtnahme in die Gebäude, Räume und IT-Systeme, in denen Daten des Auftraggebers verarbeitet werden (in Begleitung eines Verantwortlichen des Auftragsverarbeiters).*
7.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	• *Notfallstromversorgung,* • *Feuer- und Rauchmeldeanlage im Rechenzentrum,* • *Klimaanlage im Rechenzentrum.* • *Backup der Daten auf verschlüsselten Festplatten.*
8.	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	• *Strikte Trennung der verarbeiteten Daten von sonstigen Datenbeständen des Auftragsverarbeiters*

(2) Es ist ein Verfahren zu etablieren, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht.

Datum, Ort	Datum, Ort
Unterschrift (Verantwortlicher)	Unterschrift (Auftragsverarbeiter)
Name, Vorname, Funktion	Name, Vorname, Funktion