

KI-Gesichtserkennung im Fußballstadion

Möglichkeiten und Grenzen nach KI-VO und Datenschutzrecht

Dr. Matthias Eichfeld

Der Hamburgische Beauftragte für Datenschutz und
Informationsfreiheit

Herbstakademie 2026

Beschluss der IMK im Dezember 2024:

„Verbesserung und Stärkung des Sicherheitsmanagements durch die Vereine und Verbände als unerlässliche Voraussetzung für ein sicheres Stadionerlebnis insbesondere bei Risikospielen.

Hierzu sollen die technologischen Entwicklungen, insbesondere **im Bereich von Videotechnik, KI, Einlass/Crowdmanagement etc. geprüft und einheitlich hohe Sicherheitsstandards** entwickelt werden.“

Szenario 1: Biometrischer **Live-Abgleich**

Videoüber- wachung von Eingangs- bereichen und Zuschauer- blöcken	Biometrische Identifizierung von Gefährder:innen oder einer Straftat Verdächtigen in Echtzeit	Gezielte Nachverfolgung durch Einsatzkräfte im Stadion	Anschluss- maßnahmen wie Gewahrsam oder Ausschluss von der Veranstaltung
--	--	--	--



Vereinbarkeit mit der KI-VO?

Verbot der	Ausnahme:	Problem 1:	Problem 2:
Verwendung	Abwehr einer	Anforderungen	Realisierung
von	Gefahr für	an Gefahr:	der Gefahr
biometrischen	Leben oder	„konkret,	abwendbar
Echtzeit-	körperliche	erheblich und	durch Fern-
Fernidentifizie-	Unversehrtheit	unmittelbar“	identifizierung
rungssystemen			
(Art. 5 Abs. 1 lit.		(-) bei	(-) bei akuten
h KI-VO)		Eingangs-	Vorfällen im
		kontrollen	Stadion-
			innenraum

Vereinbarkeit mit der KI-VO?

Ausnahme:	Problem 1:	Problem 2:	Problem 3:
Lokalisierung einer Person, die der Begehung einer Straftat verdächtig wird	Nur qualifizierte Straftaten (Anhang II KI- VO)	Kein Abgleich ins Blaue hinein	Identifizier- barkeit bei Tatbegehung
	(-) bei zu geringer Deliktsqualität	(-), wenn keine individuellen Anhaltspunkte	(P) Datensatz zum Abgleich

Vereinbarkeit mit Datenschutzrecht?

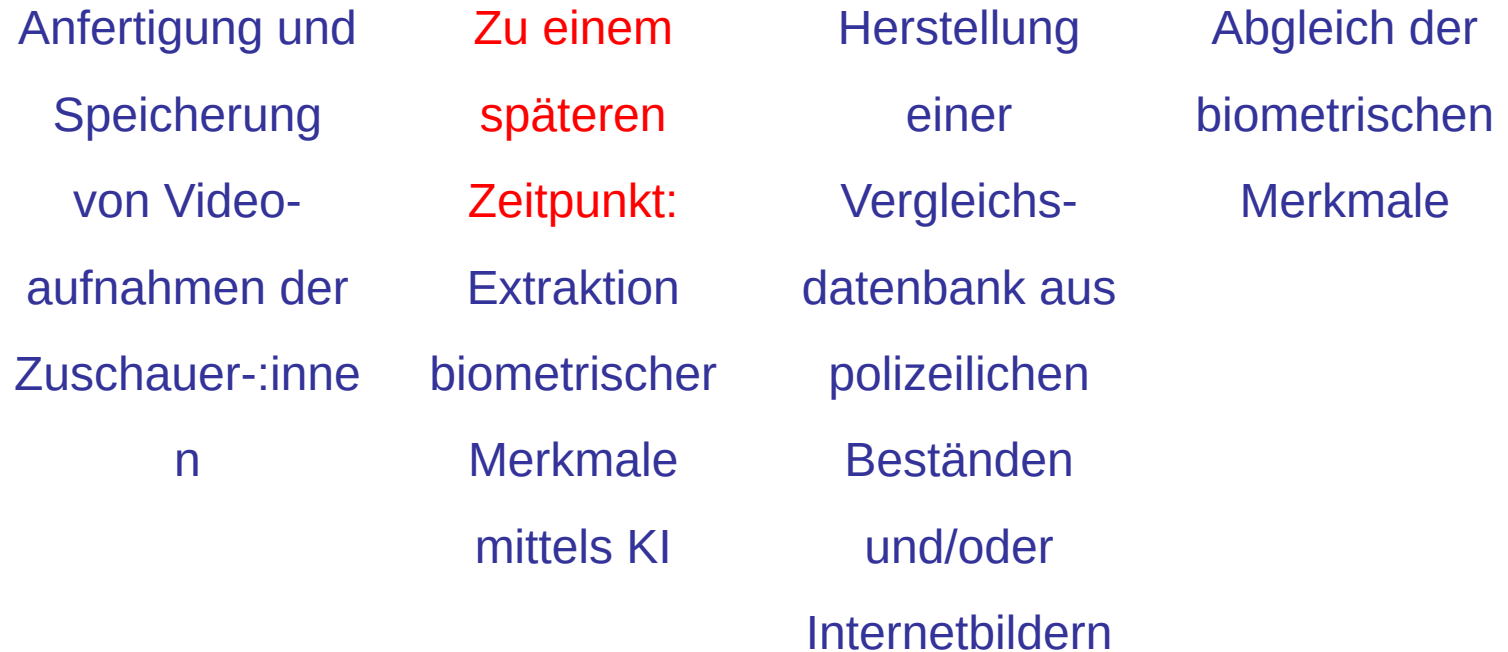
**DSGVO nicht
anwendbar, es
gilt die JI-RL**

Erwägungsgrund 38 Satz 2 KI-VO:

Die Vorschriften dieser Verordnung [...] sollten als Lex specialis in Bezug auf die in Artikel 10 der Richtlinie (EU) 2016/680 enthaltenen Vorschriften über die Verarbeitung biometrischer Daten gelten und somit die Verwendung und Verarbeitung der betreffenden biometrischen Daten umfassend regeln.

KI-VO stellt selbst keine RGL bereit, es bedarf gesetzlicher Regelung eines Mitgliedsstaats

Szenario 2: **Nachträglicher** biometrischer Abgleich



Vereinbarkeit mit der KI-VO?

Nachträgliche KI-Auswertung fällt nicht unter Verbot von Art. 5 Abs. 1 lit. h KI-VO	Art. 5 Abs. 1 lit. e KI-VO: Verbot der Herstellung von Datenbanken zur Gesichts- erkennung durch ungezieltes Auslesen des Internets (+), wenn für Web Scraping KI genutzt wird	Art. 26 Abs. 10 KI- VO: Verwendung muss zielgerichtet zur Gefahren- abwehr oder Strafverfolgung erfolgen + Gebot der Nachprüfung durch einen Menschen	Verwendung beschränkt auf das „unbedingt erforderliche Maß“ → keine alltägliche, flächendeckende Verwendung
---	--	--	---

Vereinbarkeit mit Datenschutzrecht?

**Keine
Sperrwirkung**
der KI-VO in
Bezug auf die
JI-RL für
nachträgliche
Fern-
identifizierung
(vgl. ErwGr 94
KI-VO)

Mehrere Schritte

1. Anfertigung u.
Speicherung
der Videos
2. Extraktion der
biometrischen
Merkmale
3. Herstellung v.
Vergleichs-
datenbank
4. Datenabgleich

**Hohe Eingriffs-
intensität**

- ▶ Zeitlich und
räumlich
umfangreiche
Aufnahmen
- ▶ Vielzahl von
Betroffenen
- ▶ Risiko von
Fehlidentifika-
tionen

→ **Spezifische
RGL
notwendig**

Materielle Mindestanforderungen

Zweck- bindungs- grundsatz	Gefahren- abwehr:	Straf- verfolgung:	Art. 10 JI-RL:
	Konkrete	Dringender	Verarbeitung
+	Gefahr	Tatverdacht	muss
Löschfristen	+	+	„unbedingt erforderlich“
	Hochwertiges	Straftat von	sein
	Rechtsgut	besonderer	
	(Leib, Leben	Bedeutung	→ Keine
	oder Freiheit)		systematische
			Verwendung