Smart City DIALOG

# Smart Cities und Datenschutz – Rechtliche Leitplanken nach der DSGVO

FAQ zum Thema Datenschutzrecht im Förderprogramm Modellprojekte Smart Cities

# Smart Cities und Datenschutz – Rechtliche Leitplanken nach der DSGVO

## FAQ zum Thema Datenschutzrecht im Förderprogramm Modellprojekte Smart Cities

**Inhalt:**

Die „FAQ Datenschutzrecht“ stellen eine Zusammenfassung der Beantwortung von Fragen von Kommunen dar, die vom Bund durch das Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen (BMWSB) als Modellprojekte Smart Cities gefördert werden. Die Übersicht wurde von der Kanzlei Becker Büttner Held als Partnerin der Koordinierungs- und Transferstelle Modellprojekte Smart Cities (KTS) im Rahmen des Bundesförderprogramms „Modellprojekte Smart Cities“ erstellt.

Das Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen hat die Erstellung der „FAQ Datenschutzrecht“ gefördert. Die präsentierten Rechtsausführungen, -meinungen und -auslegungen sind solche der Kanzlei Becker Büttner Held.

Version 1.0, 19. Januar 2026

Referat S III 3 – Smarte Städte und Regionen
Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen
Rudi-Dutschke-Straße 4
10969 Berlin

**Ansprechpartner KTS Smart Cities**
Koordinierungs- und Transferstelle Modellprojekte Smart Cities
c/o DLR Projektträger
Postadresse: Heinrich-Konen-Str. 1 | 53227 Bonn

Michael Huch | Projektleitung | DLR Projektträger | Berlin
Telefon +49 30 67055 600 | Michael.Huch@dlr.de

Julien Wilmes-Horváth | Kanzlei Becker Büttner Held | Köln
Telefon +49 221 650 25-112 | julien.wilmes-horvath@bbh-online.de

www.smart-city-dialog.de

# Inhalt

Einleitung und Zielsetzung ..... 4
Smart Cities und Datenschutz: Grundlagen ..... 4
Rechtsgrundlagen der Datenverarbeitung in Smart Cities ..... 5
Datenschutzrechtliche Grundprinzipien und ihre praktische Umsetzung ..... 6
KI in Smart Cities ..... 10
Typische Anwendungsfälle aus der Praxis ..... 12
Rechtsfolgen von Datenschutzverstößen ..... 17
Fazit ..... 18

# Einleitung und Zielsetzung

Smart-City-Projekte nutzen vernetzte Infrastrukturen, Sensorik, Datenplattformen und zunehmend auch künstliche Intelligenz (KI), um kommunale Aufgaben effizienter und nachhaltiger zu erfüllen. Dabei werden häufig Daten verarbeitet, die personenbezogen im Sinne der Datenschutzgrundverordnung (DSGVO) sind oder zumindest mittelbare Rückschlüsse auf identifizierbare Personen zulassen, etwa durch Bewegungs-, Nutzungs- oder Verbrauchsmuster. Datenschutz ist daher eine zentrale rechtliche Rahmenbedingung für Planung, Umsetzung und Betrieb von Smart-City-Anwendungen. Defizite können Projekte verzögern, aufsichtsbehördliche Maßnahmen nach sich ziehen und die Akzeptanz datenbasierter Lösungen beeinträchtigen.

Dieses Hinweispapier beschreibt allgemeine datenschutzrechtliche Leitlinien, ersetzt jedoch keine Einzelfallprüfung, da die Zulässigkeit konkreter Projekte maßgeblich von ihrer technischen und organisatorischen Ausgestaltung sowie von der jeweiligen landesrechtlichen Aufsichtspraxis abhängt.

# Smart Cities und Datenschutz: Grundlagen

### Wann sind Smart-City-Daten personenbezogene Daten?

Die DSGVO gilt nur, wenn personenbezogene Daten verarbeitet werden (Art. 4 Nr. 1 DSGVO). Personenbezogen sind nicht nur Daten mit direktem Namensbezug, sondern auch solche, die eine Person mittelbar identifizierbar machen, etwa über Kennungen, Standortdaten oder die Kombination mehrerer Informationen. Entscheidend ist dabei nicht eine rein theoretische Identifizierbarkeit, sondern ob eine Identifizierung realistisch mit vertretbarem Aufwand möglich ist (Erwägungsgrund 26 DSGVO). Der Personenbezug ist stets im Gesamtzusammenhang der Verarbeitung zu beurteilen, insbesondere wenn Daten aus verschiedenen Quellen zusammengeführt werden.

Für Smart-City-Projekte bedeutet dies: Bereits scheinbar „neutrale“ Daten (z. B. Verkehrs-, Sensor- oder Nutzungsdaten) können personenbezogen sein, wenn sie zusammengeführt oder zentral ausgewertet werden. Projektverantwortliche sollten daher frühzeitig prüfen, ob einzelne Daten oder ihre Kombination Rückschlüsse auf Personen zulassen. Nur wirksam anonymisierte Daten fallen vollständig aus der DSGVO heraus, pseudonymisierte Daten dagegen nicht. Diese Einordnung sollte zu Beginn des Projekts dokumentiert werden, da sie darüber entscheidet, ob und in welchem Umfang Datenschutzpflichten einzuhalten sind.

Beachte: Besteht kein Personenbezug, können aber andere Datenschutzgesetze oder europäische Vorgaben einschlägig sein, wie z.B. Datennutzungsgesetz (DNG), Telekommunikations-Digitale-Dienste-Datenschutz-Gesetz (DDG), EU Data Governance Act (DGA), EU Data Act (DA), oder landesrechtliche Regelungen gelten.

### Wer ist im Smart-City-Kontext für die Datenverarbeitung verantwortlich?

Zentrale Voraussetzung für die DSGVO-Konformität von Smart-City-Projekten ist die klare Zuordnung von Rollen und Verantwortlichkeiten. Verantwortlich ist nach Art. 4 Nr. 7 DSGVO die Stelle, die tatsächlich über Zwecke und wesentliche Mittel der Datenverarbeitung entscheidet. Treffen mehrere Akteure diese Entscheidungen gemeinsam, liegt eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO vor, die eine transparente Vereinbarung über Zuständigkeiten erfordert. Verarbeitet ein Dienstleister Daten hingegen ausschließlich weisungsgebunden und ohne eigene Zwecke, handelt es sich um eine Auftragsverarbeitung nach Art. 28 DSGVO.

Für die Projektpraxis heißt das: Rollen dürfen nicht allein nach Vertragsbezeichnungen („Plattformbetreiber", „Dienstleister") festgelegt werden, sondern müssen sich an der realen Steuerung der Datenverarbeitung orientieren. Bereits bei der Projektkonzeption sollte geprüft werden, wer über Zweck und Ausgestaltung der Datenverarbeitung entscheidet und ob eine gemeinsame Verantwortlichkeit vorliegt. Entsprechend sind rechtzeitig die erforderlichen Vereinbarungen nach Art. 26 oder Art. 28 DSGVO abzuschließen und in der Projektorganisation klar zu verankern, um spätere Haftungs- und Zuständigkeitsprobleme zu vermeiden.

## Rechtsgrundlagen der Datenverarbeitung in Smart Cities

Jede Verarbeitung personenbezogener Daten in Smart-City-Projekten bedarf einer tragfähigen Rechtsgrundlage im Sinne von Art. 6 Abs. 1 DSGVO.

Die im Folgenden dargelegten Rechtsgrundlagen erlangen bei Smart-City-Anwendungen besondere Relevanz, da diese typischerweise im Spannungsfeld zwischen öffentlicher Aufgabenerfüllung, nutzerbezogenen Dienstleistungen, freiwilligen Zusatzangeboten und einer fortschreitenden Weiterverwendung einmal erhobener Daten die Datenverarbeitung rechtfertigen.

### Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung hoheitlicher Gewalt

Für Smart-City-Projekte öffentlicher Stellen ist Art. 6 Abs. 1 lit. e DSGVO häufig die maßgebliche Rechtsgrundlage. Danach ist eine Verarbeitung zulässig, wenn sie für die Wahrnehmung einer gesetzlich zugewiesenen Aufgabe im öffentlichen Interesse erforderlich ist (Art. 6 Abs. 3 DSGVO). Ein allgemeiner Innovations- oder Digitalisierungszweck reicht nicht aus. Erforderlich ist stets ein konkreter Bezug zu einer bestehenden öffentlichen Aufgabe (z. B. Verkehrssteuerung, Daseinsvorsorge, Energieversorgung). Der Umfang der Datenverarbeitung ist dabei auf das Erforderliche zu begrenzen. Ergänzend sind regelmäßig die einschlägigen Landesdatenschutzgesetze zu beachten, die Art. 6 Abs. 1 lit. e DSGVO für öffentliche Stellen konkretisieren (z. B. § 3 DSG NRW, § 4 LDSG BW, Art. 4 BayDSG, § 3 HDSIG).

Projektverantwortliche sollten frühzeitig klären und dokumentieren, welche konkrete öffentliche Aufgabe durch die jeweilige Datenverarbeitung erfüllt wird. Dabei ist zusätzlich zu prüfen, ob das anwendbare Landesdatenschutzrecht weitere Vorgaben enthält, etwa zum Vorrang der Direkterhebung, zu Dritterhebungen oder zu Dokumentationspflichten. Diese Anforderungen sollten bereits in der Projektkonzeption berücksichtigt werden, da sie Einfluss auf Datenerhebung, Systemarchitektur und Projektabläufe haben können.

### Verarbeitung zur Vertragserfüllung und vorvertraglicher Maßnahmen

Daneben kann in bestimmten Konstellationen Art. 6 Abs. 1 lit. b DSGVO einschlägig sein, insbesondere bei Smart-City-Apps oder digitalen Dienstleistungen, die auf einer vertraglichen Beziehung mit den Nutzenden beruhen. Diese Rechtsgrundlage trägt jedoch nur solche Datenverarbeitungen, die objektiv zur Erfüllung des jeweiligen Vertrags erforderlich sind.

### Verarbeitung nach Einwilligung

Eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO spielt im Smart-City-Kontext eine ambivalente Rolle. Zwar kann sie in bestimmten Fällen, etwa bei freiwilligen Zusatzfunktionen oder personalisierten Diensten, eine geeignete Rechtsgrundlage darstellen. In vielen Smart-City-Anwendungen ist sie jedoch praktisch und rechtlich nur eingeschränkt nutzbar. Dies gilt insbesondere für Datenverarbeitungen im öffentlichen Raum oder in strukturellen Abhängigkeitsverhältnissen, in denen Zweifel an der Freiwilligkeit bestehen können oder eine Einwilligung erst gar nicht eingeholt werden konnte. Zudem ist zu berücksichtigen, dass Einwilligungen jederzeit widerrufen werden könne, was bei dauerhaft angelegten Infrastrukturen erhebliche organisatorische Herausforderungen mit sich bringt.

### Verarbeitung bei Zweckänderung

Ein besonderes Augenmerk ist auf Zweckänderungen zu richten. Smart-City-Projekte sind oft langfristig angelegt und entwickeln sich technisch und funktional weiter. Die DSGVO erlaubt eine Weiterverarbeitung für andere Zwecke nur unter den engen Voraussetzungen des Art. 6 Abs. 4 DSGVO. Eine vorausschauende und möglichst präzise Zweckdefinition bereits zu Projektbeginn ist daher ein wesentlicher Faktor für die rechtssichere Weiterentwicklung von Smart-City-Anwendungen.

Landesrechtliche Vorschriften enthalten darüber hinaus oftmals weitergehende Pflichten oder spezielle Zweckänderungskataloge (vgl. exemplarisch § 4 SächsDSDG, § 5 LDSG BW, § 9 DSG NRW).

# Datenschutzrechtliche Grundprinzipien und ihre praktische Umsetzung

Die Rechtmäßigkeit von Datenverarbeitungen erschöpft sich nicht in der Wahl einer geeigneten Rechtsgrundlage. Darüber hinaus müssen sämtliche Verarbeitungen den in Art. 5 DSGVO verankerten datenschutzrechtlichen Grundprinzipien entsprechen.

### Grundsatz der Transparenz (Art. 5 Abs. 1 lit. a DSGVO)

Aus Art. 5 Abs. 1 lit. a DSGVO folgt der Grundsatz der Transparenz: Betroffene müssen nachvollziehen können, ob und wie ihre Daten verarbeitet werden. Bürger müssen stets wissen, wer was bei welcher Gelegenheit über sie weiß (vgl. BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83, „Volkszählungsurteil“). Transparenz ist dabei nicht nur rückblickend, sondern auch vorausschauend sicherzustellen, sodass Betroffene bereits im Vorfeld die Datenverarbeitung verstehen können (Erwägungsgrund 39 DSGVO).

Für Smart-City-Projekte bedeutet dies, dass Informationspflichten verständlich, auffindbar und systemgerecht umzusetzen sind. In der Praxis sind häufig mehrstufige Informationskonzepte sinnvoll, etwa durch Hinweise vor Ort (z. B. Schilder, QR-Codes) und ergänzende digitale Informationen. Ziel ist es, die wesentlichen Zwecke und Funktionsweisen der Datenverarbeitung klar zu vermitteln, ohne Betroffene mit technischen oder juristischen Details zu überfordern.

### Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO)

Wichtig ist darüber hinaus der Grundsatz der Zweckbindung. Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden.

Für Smart-City-Projekte bedeutet dies, dass die Zwecke der Datenverarbeitung klar benannt und gegenüber den betroffenen Personen transparent gemacht werden müssen. Allgemeine Formulierungen wie „Optimierung städtischer Prozesse“ oder „Verbesserung der Lebensqualität“ genügen hierfür regelmäßig nicht. Vielmehr ist zu definieren, welche konkreten Steuerungs-, Analyse – oder Verwaltungsaufgaben mit welchen Daten erfüllt werden sollen. Gerade bei modular aufgebauten Systemen und Plattformlösungen ist darauf zu achten, dass neue Nutzungsszenarien nicht automatisch von bestehenden Zweckdefinitionen gedeckt sind (vgl. Schantz in: BeckOK Datenschutzrecht, 54. Ed, 01.11.2021, DS-GVO, Art. 5, Rn. 15). In der Praxis sollten Projektverantwortliche daher prüfen, ob neue Verarbeitungen noch vom ursprünglichen Zweck erfasst sind oder ob eine neue Zweckfestlegung und gegebenenfalls eine neue Rechtsgrundlage erforderlich wird.

### Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)

Eng mit der Zweckbindung verknüpft ist der Grundsatz der Datenminimierung. Danach dürfen nur solche personenbezogenen Daten verarbeitet werden, die für den jeweiligen Zweck erforderlich sind. Die DSGVO verlangt jedoch keine maximale Datensparsamkeit um jeden Preis, sondern eine am Zweck orientierte Begrenzung (*Schantz* in: BeckOK Datenschutzrecht, 54. Ed., 01.11.2021, DS-GVO, Art. 5, Rn. 25).

In der Praxis bedeutet dies, dass Datenerhebungen und -verarbeitungen kritisch zu hinterfragen und technisch so auszugestalten sind, dass überflüssige Detailtiefe, unnötige Speicherungen oder zu lange Aufbewahrungsfristen vermieden werden. Konkret ist der Grundsatz verletzt, wenn weniger intensive Datenverarbeitungen bei gleicher Interessenwahrnehmung zur Verfügung stehen, z.B. durch Bildaufnahme eines Parkverstoßes unter Unkenntlichmachung des Fahrzeugführers mittels Verpixelung (so OLG Dresden, Urt. v. 09.09.2025, Az. 4 U 464/25).

### Grundsatz der Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO)

Der Grundsatz der Richtigkeit verpflichtet Verantwortliche, personenbezogene Daten sachlich richtig und, soweit erforderlich, auf dem neuesten Stand zu halten.

### Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO)

Der Grundsatz der Speicherbegrenzung verlangt, dass personenbezogene Daten nicht länger gespeichert werden, als es für die jeweiligen Zwecke erforderlich ist.

In Smart-City-Projekten, die häufig mit Echtzeitdaten, historischen Analysen und langfristigen Prognosen arbeiten, ist dies eine besondere Herausforderung. Es bedarf klarer Lösch- und Archivierungskonzepte, die zwischen

kurzfristig benötigten operativen Daten und langfristig erforderlichen, möglichst anonymisierten Auswertungsdaten unterscheiden. Globale unbegrenzte Speicherfristen sind mit den Vorgaben der DSGVO nicht vereinbar.

### Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO)

Der Grundsatz der Integrität und Vertraulichkeit erfordert, dass personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung geschützt werden. In Smart-City-Projekten ist dieser Grundsatz vor allem bedeutsam, da die Vernetzung zahlreicher Systeme, Sensoren und Plattformen die Angriffsfläche erhöht.

### Grundsatz der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO)

Schließlich ist der Grundsatz der Rechenschaftspflicht zu beachten. Verantwortliche müssen nicht nur die Einhaltung der datenschutzrechtlichen Vorgaben sicherstellen, sondern diese auch nachweisen können. Dies erfordert eine sorgfältige Dokumentation von Zweckfestlegungen, Rechtsgrundlagen, technischen und organisatorischen Maßnahmen sowie von Abwägungsentscheidungen.

### Anonymisierung und Pseudonymisierung

Anonymisierung und Pseudonymisierung sind zentrale Instrumente zur Reduzierung datenschutzrechtlicher Risiken. Anonymisierte Daten fallen nicht mehr in den Anwendungsbereich der DSGVO, allerdings nur dann, wenn eine Re-Identifizierung dauerhaft und realistisch ausgeschlossen ist (Erwägungsgrund 26 DSGVO). Diese Hürde ist in Smart-City-Projekten hoch: Gerade Bewegungs-, Verkehrs- oder Verbrauchsdaten können trotz technischer Bearbeitung häufig wieder einzelnen Personen oder Haushalten zugeordnet werden, etwa durch zeitliche oder räumliche Muster oder die Verknüpfung mit weiteren Datenquellen. Zudem ist zu beachten, dass auch die Anonymisierung selbst eine Verarbeitung im Sinne der DSGVO darstellt. Pseudonymisierte Daten hingegen bleiben personenbezogen (Art. 4 Nr. 5 DSGVO). Ihr Nutzen liegt vor allem in der Risikominimierung, etwa zur Unterstützung von Datenminimierung und Datensicherheit.

Für die Praxis bedeutet dies: Technische Maßnahmen wie Aggregation, Hashing oder Maskierung führen nicht automatisch zu einer Anonymisierung. Entscheidend ist stets eine Gesamtbetrachtung des Verarbeitungskontexts, insbesondere bei granularen, langfristigen oder plattformübergreifenden Auswertungen. Anonymisierung sollte daher als eigenständiges Verarbeitungskonzept bereits in der Projektplanung verankert werden, mit der klaren Entscheidung, wo personenbezogene Daten erforderlich sind und wo frühzeitig aggregierte oder anonymisierte Daten genügen. Ergänzend ist zu berücksichtigen, dass die aufsichtsbehördliche Bewertung im Detail variieren kann, da die DSGVO selbst keine abschließende Definition der Anonymisierung enthält (vgl. § 2 HDSIG, § 4 DSG NRW). In Zweifelsfällen ist daher eine vorsichtige Einordnung und Dokumentation empfehlenswert.

### Transparenz, Information und Betroffenenrechte

Die DSGVO verpflichtet Verantwortliche, betroffene Personen klar, verständlich und leicht zugänglich über die Verarbeitung ihrer personenbezogenen Daten zu informieren (Art. 12 ff., insbesondere Art. 13 und 14 DSGVO). In Smart-City-Projekten ist dies besonders relevant, da viele Verarbeitungen im öffentlichen Raum stattfinden oder

ohne aktive Mitwirkung der Betroffenen erfolgen. Transparenz erfordert hier mehr als klassische Datenschutzhinweise: Betroffene müssen nachvollziehen können, zu welchen Zwecken, auf welcher Rechtsgrundlage und durch wen ihre Daten verarbeitet werden sowie welche Rechte ihnen zustehen. Gerade bei Projekten mit mehreren beteiligten Akteuren ist eine klare Darstellung der datenschutzrechtlichen Verantwortlichkeit unerlässlich.

Für die Praxis bedeutet dies, dass mehrstufige Informationskonzepte regelmäßig erforderlich sind, etwa durch Hinweise vor Ort (Schilder, Piktogramme, QR-Codes) mit Verweis auf vertiefende digitale Informationen. Zugleich müssen funktionsfähige Prozesse zur Wahrnehmung der Betroffenenrechte nach Art. 15 bis 21 DSGVO vorgehalten werden, auch wenn Daten in verteilten oder automatisierten Systemen verarbeitet werden. Dies setzt klare Zuständigkeiten, abgestimmte Abläufe zwischen den Beteiligten und eine technische Ausgestaltung voraus, die Auskunft, Löschung oder Widerspruch tatsächlich ermöglicht. Besonderes Augenmerk ist dabei auf das Widerspruchsrecht nach Art. 21 DSGVO zu legen, das in der Projektkonzeption von Anfang an mitgedacht werden sollte.

### Datenschutz durch Technikgestaltung (Privacy by Design & by Default)

Art. 25 DSGVO verpflichtet Verantwortliche, Datenschutz durch Technikgestaltung („Privacy by Design“) und datenschutzfreundliche Voreinstellungen („Privacy by Default“) von Beginn an umzusetzen. Datenschutz muss bereits bei der Planung und Auswahl der Systeme berücksichtigt werden und darf nicht erst nachträglich ergänzt werden. Ziel ist es, die Datenschutzgrundsätze – insbesondere Datenminimierung und Zweckbindung – technisch und organisatorisch wirksam umzusetzen, unabhängig von der konkret gewählten Rechtsgrundlage.

Für Smart-City-Projekte bedeutet dies, dass Systeme so konzipiert werden sollten, dass standardmäßig nur die für den jeweiligen Zweck erforderlichen Daten verarbeitet werden. In der Praxis helfen etwa modulare Systemarchitekturen, getrennte Datenhaltung und abgestufte Zugriffskonzepte. Wichtig ist zudem, dass datenschutzfreundliche Voreinstellungen auch bei Erweiterungen, Updates oder neuen Modulen erhalten bleiben. Datenschutzanforderungen sollten daher verbindlich in Projektvorgaben, Ausschreibungen und Verträge aufgenommen und ihre Umsetzung regelmäßig überprüft werden.

### Technische und organisatorische Maßnahmen (TOM)

Die Sicherheit der Verarbeitung ist ein zentraler Bestandteil des Datenschutzes und in Art. 32 DSGVO ausdrücklich geregelt. Danach müssen Verantwortliche unter Berücksichtigung von Risiko, Stand der Technik, Implementierungskosten sowie Art und Zweck der Verarbeitung geeignete technische und organisatorische Maßnahmen treffen, um ein angemessenes Schutzniveau zu gewährleisten. In Smart-City-Projekten ist diese risikobasierte Betrachtung besonders wichtig, da Risiken nicht nur aus einzelnen Datenarten, sondern vor allem aus der Vernetzung, Systemkomplexität und Vielzahl von Zugriffspunkten entstehen.

Für die Praxis bedeutet dies, dass Sicherheitsmaßnahmen von Anfang an systematisch eingeplant werden müssen. Dazu zählen insbesondere Zugriffsbeschränkungen, Rollen- und Berechtigungskonzepte, Verschlüsselung bei Übertragung und Speicherung, Protokollierung sowie der abgesicherte Umgang mit Schnittstellen und Drittanbindungen (vgl. Art. 32 Abs. 1 DSGVO). Da jede Schnittstelle ein potenzielles Einfallstor darstellt, sind klare technische Absicherungen und organisatorische Kontrollen erforderlich. Zudem sind Sicherheitsmaßnahmen

laufend zu überprüfen und anzupassen, da Art. 32 DSGVO keine einmalige Umsetzung, sondern eine kontinuierliche Risiko- und Wirksamkeitsprüfung verlangt.

### Datenschutzfolgenabschätzung (DSFA)

Die Datenschutzfolgenabschätzung (DSFA) nach Art. 35 DSGVO dient dazu, hohe Risiken für die Rechte und Freiheiten betroffener Personen frühzeitig zu erkennen und zu steuern. Sie ist immer dann erforderlich, wenn eine Datenverarbeitung voraussichtlich ein hohes Risiko mit sich bringt. Smart-City-Projekte erfüllen diese Voraussetzungen häufig, etwa durch die Verarbeitung großer Datenmengen, die Überwachung öffentlich zugänglicher Bereiche, den Einsatz neuer Technologien oder die Zusammenführung verschiedener Datenquellen, oft über längere Zeiträume und ohne aktive Mitwirkung der Betroffenen.

In der Praxis ist die DSFA weniger ein formales Dokument als vielmehr ein strukturierter Entscheidungsprozess, der die Projektgestaltung beeinflusst. Sie beschreibt die geplante Verarbeitung, bewertet deren Erforderlichkeit und Verhältnismäßigkeit und legt konkrete Maßnahmen zur Risikominderung fest. Wichtig ist eine klare Abstimmung zwischen allen Projektbeteiligten, insbesondere bei Kooperationen oder gemeinsamer Verantwortlichkeit. Der Datenschutzbeauftragte ist einzubinden und seine Stellungnahme zu dokumentieren. Bleibt trotz geplanter Maßnahmen ein hohes Restrisiko bestehen, muss vor Projektstart die Aufsichtsbehörde konsultiert werden (Art. 36 DSGVO).

## KI in Smart Cities

Der Einsatz von KI ist für viele Smart-City-Anwendungen inzwischen von großer Bedeutung. Konkrete kommunale Beispiele sind KI-gestützte Wärme-Prognose-Modelle, Analyseplattformen für Bürgerfeedback oder Systeme zur Erkennung von Infrastrukturdefiziten (vgl. Künstliche Intelligenz in smarten Städten und Regionen: Innovative KI-Anwendungen für die Stadtentwicklung).

### DSGVO vs. KI-VO

Neben der DSGVO ist für den Einsatz von KI zunehmend die europäische KI-VO zu berücksichtigen. Diese regelt die Zulässigkeit, Risikobewertung und Zertifizierung von KI-Systemen abhängig von ihrer Risikoklasse und kann auch Smart-City-Anwendungen wie Verkehrssteuerung, Mustererkennung oder prädiktive Analysen beeinflussen. Die KI-VO gibt Anforderungen an Transparenz, Qualitätssicherung und Risikomanagement für KI-gestützte Systeme vor. Verantwortliche sollten frühzeitig prüfen, ob und in welchem Umfang KI-Komponenten unter die KI-VO fallen und die DSGVO-Pflichten (z. B. Transparenz, Betroffenenrechte, Dokumentation) parallel erfüllen müssen (vgl. hierzu auch Künstliche Intelligenz in smarten Städten und Regionen: Innovative KI-Anwendungen für die Stadtentwicklung).

Die KI-VO schafft jedoch keine eigene Rechtsgrundlage für eine Datenverarbeitung. Jede KI-Anwendung muss daher weiterhin DSGVO-konform sein.

In der Praxis besonders relevant wird die Trennung von Trainings- und Einsatzdaten. Das Trainieren einer KI stellt ebenfalls eine Datenverarbeitung dar. Werden hierbei personenbezogene Daten verarbeitet oder enthält das

trainierte KI-Modell weiterhin personenbezogene Daten oder kann diese rekonstruieren, bedarf es dafür im Einzelfall ebenfalls einer Rechtsgrundlage, selbst wenn spätere KI-generierte Inhalte keinen Personenbezug (mehr) aufweisen. Hier ist genau zu prüfen, welches KI-Modell verwendet wird und wie dieses personenbezogene Daten erhebt und verarbeitet.

### Transparenzanforderungen

Eine datenschutzrechtliche Herausforderung beim Einsatz von KI in Smart Cities bildet die Frage der Nachvollziehbarkeit und Transparenz der Datenverarbeitung. Art. 5 Abs. 1 lit. a DSGVO verlangt eine rechtmäßige und transparente Verarbeitung. KI-Systeme, insbesondere solche, die auf komplexen Modellen oder maschinellem Lernen beruhen, können jedoch Entscheidungs- und Analyseprozesse aufweisen, die für Außenstehende nur eingeschränkt erklärbar sind. Verantwortliche müssen daher sicherstellen, dass die Funktionsweise der KI zumindest in ihren Grundzügen verständlich beschrieben werden kann und dass die Zwecke, für die KI eingesetzt wird, klar definiert sind. Die DSGVO verlangt dabei keine Offenlegung von Algorithmen, aber eine nachvollziehbare Beschreibung von Logik, Datenkategorien und Auswirkungen auf die Betroffenen (vgl. Art. 5 Abs. 1 lit. a, 13, 14 DSGVO).

### Automatisierte Entscheidungen (Art. 22 DSGVO)

Ein weiterer Schwerpunkt liegt auf der Abgrenzung zwischen unterstützenden Analysen und automatisierten Entscheidungen gegenüber betroffenen Personen. Allgemein gilt, dass zur Vermeidung von Art. 22 DSGVO (Schutz vor automatisierten Entscheidungen) eine wirksame menschliche Kontrolle stets gegeben und nicht nur formal möglich sein sollte. Allerdings stellt nicht jede KI-Nutzung eine automatisierte Entscheidung im Sinne von Art. 22 DSGVO dar. Die Vorschrift greift unter anderem nur bei ausschließlich automatisierter Verarbeitung und rechtlicher oder vergleichbar erheblicher Wirkung. Verkehrsprognosen, Entscheidungsunterstützung und Priorisierungsvorschläge, bei denen die Entscheidung letztendlich nicht von der KI getroffen wird, gehören z.B. nicht dazu. Dagegen können eine automatisierte Zuteilung knapper Ressourcen oder der Ausschluss von Leistungen ohne menschliche Prüfung unter Art. 22 DSGVO fallen.

### Zweckänderungen

KI-Anwendungen sind zudem besonders anfällig für Zweckverschiebungen. Modelle, die einmal trainiert wurden, lassen sich oftmals auch für andere Anwendungsfälle weiterverwenden. Datenschutzrechtlich ist jedoch sicherzustellen, dass Trainings- und Einsatzdaten nur für die festgelegten Zwecke verwendet werden und dass eine Weiterverwendung der Modelle oder der zugrunde liegenden Daten nicht zu einer unzulässigen Zweckänderung führt. Dies gilt insbesondere dann, wenn Trainingsdaten personenbezogen sind oder sich aus den Modellen Rückschlüsse auf einzelne Personen ziehen lassen.

### Datenqualität

Ein weiterer datenschutzrechtlich relevanter Aspekt ist die Qualität der Daten (Art. 5 Abs. 1 lit. d DSGVO). Verzerrte oder unvollständige Datensätze können bei KI-Systemen zu fehlerhaften Analysen oder diskriminierenden Ergebnissen führen. Auch wenn Diskriminierungsfragen über den Datenschutz hinausgehen, können sie datenschutzrechtlich relevant werden, wenn sie die Rechte und Freiheiten betroffener Personen beeinträchtigen. Verantwortliche sind daher gehalten, Datenquellen, Trainingsprozesse und Ergebnisse kritisch zu überprüfen.

### DSFA

Schließlich ist der Einsatz von KI regelmäßig in die Risikobewertung im Rahmen der DSFA einzubeziehen. Der Einsatz neuer oder besonders komplexer Technologien kann das Risiko für die betroffenen Personen erheblich erhöhen und zusätzliche Schutzmaßnahmen erforderlich machen. In Smart-City-Projekten sollte der Einsatz von KI daher stets als eigenständiger Risikofaktor betrachtet und entsprechend dokumentiert werden. Dies gilt insbesondere, wenn KI für Profiling, im öffentlichen Raum oder bei Entscheidungen mit Verteilungswirkung verwendet wird.

Zur datenschutzrechtlichen Bewertung von KI-Systemen in öffentlichen Kontexten wird zudem auf die Handreichung ‚KI in Behörden – Datenschutz von Anfang an mitdenken' des Bundesbeauftragten für Datenschutz und Informationsfreiheit verwiesen.

# Typische Anwendungsfälle aus der Praxis

## Zentrale urbane Datenplattformen

Zentrale urbane Datenplattformen bündeln Daten aus verschiedenen Smart-City-Anwendungen, etwa aus den Bereichen Verkehr, Energie, Umwelt oder Verwaltung, und stellen diese für Auswertungen, Steuerungsprozesse oder weitere Nutzungsszenarien bereit. Ihr Mehrwert liegt in der Zusammenführung und Analyse bislang getrennter Datenquellen.

Datenschutzrechtlich kann durch die Datenbündelung und -verknüpfung ein Personenbezug entstehen oder verstärkt werden. Auch vermeintlich technische oder aggregierte Daten sind daher im Gesamtzusammenhang der Plattform regelmäßig als personenbezogen zu bewerten. Maßgeblich ist nicht die einzelne Datenquelle, sondern die Funktion der Plattform als zentraler Auswertungs- und Verknüpfungspunkt.

Wichtig ist zudem die Klärung der datenschutzrechtlichen Verantwortlichkeit. Häufig entscheiden mehrere Akteure gemeinsam über Zwecke und Mittel der Plattformnutzung, sodass eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO naheliegt. Diese ist transparent zu regeln. Die Zweckbestimmung der Plattform muss hinreichend konkret erfolgen. Offene oder beliebig erweiterbare Nutzungszwecke sind unzulässig und bedürfen bei Erweiterungen einer erneuten datenschutzrechtlichen Bewertung.

Schließlich sind klare Zugriffs- und Berechtigungskonzepte erforderlich. Personenbezogene Daten dürfen nur berechtigten Stellen zugänglich gemacht werden. Aufgrund der strukturellen Risiken ist regelmäßig zu prüfen, ob für den Betrieb der Plattform eine DSFA nach Art. 35 DSGVO erforderlich ist.

Soweit KI-gestützte Auswertungen eingesetzt werden, sind die Vorgaben der KI-VO (vgl. B. XI. 1.) parallel zu prüfen.

## Verkehrsanalyse mittels Kameras und KI

Bei der Verkehrsanalyse mittels Kameras und KI werden Bilddaten aus dem öffentlichen Verkehrsraum erfasst und automatisiert ausgewertet, um Verkehrsflüsse, Fahrzeugdichten oder Störungen zu analysieren und

Verkehrssteuerungsmaßnahmen zu optimieren. In der Regel steht dabei nicht die Identifizierung einzelner Personen oder Fahrzeuge, sondern die statistische Auswertung des Verkehrs im Vordergrund.

Gleichwohl wird in der Aufsichtspraxis oftmals eine Verarbeitung personenbezogener Daten angenommen. Bildaufnahmen im öffentlichen Raum können Personen, Fahrzeuge oder Kennzeichen erfassen und lassen zumindest mittelbar Rückschlüsse auf identifizierbare Personen zu. Der Einsatz von KI verstärkt dieses Risiko, da automatisierte Erkennungs- und Klassifizierungsverfahren detaillierte Auswertungen ermöglichen. Die Datenverarbeitung bedarf daher einer tragfähigen Rechtsgrundlage, in der Regel auf Basis einer Aufgabe im öffentlichen Interesse nach Art. 6 Abs. 1 lit. e DSGVO, und muss strikt zweckgebunden auf Verkehrsanalysen beschränkt bleiben.

Der Fokus sollte hier auf Maßnahmen zur Datenminimierung liegen. Soweit möglich, sollte eine Auswertung in Echtzeit ohne Speicherung personenbezogener Bilddaten erfolgen oder eine frühzeitige Anonymisierung bzw. Verpixelung vorgesehen werden. Funktionen, die über eine reine Verkehrsanalyse hinausgehen, etwa die Identifikation einzelner Fahrzeuge oder Personen, sind datenschutzrechtlich besonders eingriffsintensiv und regelmäßig nicht von der Zweckbestimmung gedeckt. Aufgrund der systematischen Beobachtung des öffentlichen Raums ist für solche Anwendungen zu prüfen, ob eine DSFA nach Art. 35 DSGVO erforderlich ist.

Im Hinblick auf die KI-VO ist zu beachten, dass KI-Systeme im öffentlichen Raum als hochrisikobehaftet eingestuft werden können. Es sollte daher geprüft werden, ob das System lediglich statistisch arbeitet oder auch klassifiziert (z.B. Fahrzeugtypen, Verkehrsteilnehmer). Ist dies der Fall, sind die strengen Anforderungen der KI-VO zusätzlich zu beachten.

### Automatisierte Kennzeichenerfassung

Bei der automatisierten Kennzeichenerfassung werden Fahrzeugkennzeichen mittels Kameras erfasst und technisch ausgewertet, etwa zur Verkehrssteuerung, Parkraumbewirtschaftung oder zur Durchsetzung verkehrsbezogener Regelungen. Anders als bei rein statistischen Verkehrsauswertungen steht hier regelmäßig die Erfassung einzelner Fahrzeuge im Vordergrund.

Datenschutzrechtlich handelt es sich bei Kfz-Kennzeichen um personenbezogene Daten, da sie zumindest mittelbar einer natürlichen Person zugeordnet werden können. Die automatisierte und flächendeckende Erfassung von Kennzeichen im öffentlichen Raum stellt daher einen besonders intensiven Eingriff in die Rechte der Betroffenen dar. Eine Verarbeitung ist nur zulässig, wenn eine klare, spezifische und tragfähige Rechtsgrundlage besteht. Allgemeine Zwecke der Verkehrsoptimierung oder Effizienzsteigerung reichen hierfür regelmäßig nicht aus.

Zudem sind strenge Anforderungen an Zweckbindung, Speicherbegrenzung und Datenminimierung zu stellen. Eine dauerhafte Speicherung oder weitergehende Nutzung der erfassten Kennzeichendaten ist nur zulässig, soweit sie für den konkret festgelegten Zweck erforderlich ist. Angesichts der hohen Eingriffsintensität ist bei automatisierten Kennzeichenerfassungssystemen regelmäßig eine DSFA nach Art. 35 DSGVO durchzuführen.

Die Aufsichtspraxis der verschiedenen Bundesländer kann sich bei der Beurteilung deutlich unterscheiden, so z.B. im Zuge der Parkraumbewirtschaftung. Hierbei gibt es insbesondere verschiedene Ansätze zur Frage der Verantwortlichkeit zwischen Parkraumbewirtschafter und Eigentümer, wenn letzterer Einfluss auf Zwecke und

Mittel der Kennzeichenerfassung nimmt. Der Landesbeauftragte für Datenschutz in NRW nimmt beispielsweise eine reine Verantwortlichkeit des Parkraumbewirtschafters an (vgl. KFZ-Kennzeichenerfassung auf Parkplätzen | LDI - Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen), während die Aufsichtsbehörde des Saarlandes zu einer gemeinsamen Verantwortlichkeit tendiert (32. Tätigkeitsbericht Datenschutz, S. 144 f., abrufbar unter 32. Tätigkeitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit).

Auch die Transparenzanforderungen können unterschiedlich beurteilt werden. So schlägt der Landesbeauftragte für Datenschutz des Saarlandes allgemein eine Hinweisbeschilderung zum Zeitpunkt des Befahrens des befassten Bereichs vor (32. Tätigkeitsbericht Datenschutz, S. 144), in NRW wird ein Symbol für Videoüberwachung als intransparent gesehen, da Betroffene dieses Symbol mit konventionellen Videoüberwachungsanlagen in Verbindung bringen können (vgl. KFZ-Kennzeichenerfassung auf Parkplätzen | LDI - Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen).

### Sonderfall: Parkplatzüberwachung

Ein Sonderfall der Verkehrsanalyse stellen Smart-Parking-Lösungen dar, bei denen mittels optischer Sensoren oder Kameras der Belegstatus von Parkplätzen in Echtzeit ermittelt wird. Ziel ist dabei nicht die Identifikation von Fahrzeugen und deren Haltern, sondern die bloße Anzeige freier oder belegter Stellplätze. In Abgrenzung zur automatisierten Kennzeichenerfassung dienen diese Systeme also gerade nicht der Identifizierung des Halters (z.B. im Falle eines Parkraumverstoßes).

Datenschutzrechtlich ist entscheidend, ob bei der Datenerhebung ein Personenbezug entsteht und ob dieser im weiteren Verarbeitungsprozess fortbesteht. Werden Bild- oder Sensordaten zunächst erfasst, aber innerhalb kürzester Zeit technisch so anonymisiert, dass ein Rückschluss auf Fahrzeuge, Kennzeichen oder Personen dauerhaft ausgeschlossen ist und ausschließlich anonymisierte Daten weiterverarbeitet werden, liegt keine Verarbeitung personenbezogener Daten vor. Voraussetzung ist, dass die Anonymisierung bereits vor der eigentlichen Verarbeitung erfolgt und ein Zugriff auf nicht anonymisierte Rohdaten ausgeschlossen ist.

In der Praxis ist zu berücksichtigen, dass Aufsichtsbehörden bereits die kurzfristige Erfassung von Fahrzeugen oder Kennzeichen als datenschutzrechtlich relevanten Vorgang bewerten können. Dies wurde vor allem durch die Entscheidung des Bundesverfassungsgerichts zur polizeilichen Kennzeichenkontrolle zwecks Abgleichung mit Fahndungsfahrzeugen in Bayern verdeutlicht (BVerfG, Beschl. v. 18.12.2018, Az. 1 BvR 142/15). Die Kennzeichen wurden per Kamera fotografiert, durch Software in digitale Daten umgewandelt und dann mit Fahndungsdateien abgeglichen. Lag kein Treffer vor, wurde die Information gelöscht. Diese automatisierte Löschung erfolgte zum Teil jedoch fehlerhaft, weshalb auch eine manuelle Kontrolle durch die Polizei stattfand. Das BVerfG sah hierin einen Eingriff in das Recht auf informationelle Selbstbestimmung. Über die Rechtmäßigkeit der Datenverarbeitung entschied es nicht. Dennoch lassen sich aus dem Fall wichtige datenschutzrechtliche Erkenntnisse entnehmen: werden unveränderte Aufnahmen der Kameras verwendet - wenn auch nur kurzzeitig - oder diese vor Verarbeitung lediglich pseudonymisiert, liegt eine Verarbeitung personenbezogener Daten vor, auch wenn diese nach der Verarbeitung anonymisiert werden. Die Verarbeitung muss dann durch Art. 6 Abs. 1 DSGVO gerechtfertigt sein. In der Regel wird hier auf ein öffentliches (Art. 6 Abs. 1 lit. e DSGVO) oder berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO) verwiesen. Werden die personenbezogenen Daten nur so lange gespeichert,

wie unbedingt erforderlich für den jeweiligen Zweck (z.B. schnelle Parkplatzfindung) und wird auf die Datenverarbeitung vor der Parkplatzeinfahrt auf einem Schild hingewiesen, ist ein berechtigtes Interesse in der Regel anzunehmen. Aufgrund des Einflusses des jeweiligen Landesdatenschutzrechts auf die Auslegung öffentlicher oder berechtigter Interessen, die Verhältnismäßigkeitsprüfung, sowie die Erwartungshaltung der Aufsichtsbehörden ist jedoch stets eine Einzelfallbetrachtung erforderlich.

Da bei einer Echtzeitanonymisierung dagegen keine personenbezogenen Daten verarbeitet werden, sollten Smart-Parking-Systeme technisch möglichst so gestaltet sein, dass eine Echtzeitanonymisierung unmittelbar am Erfassungsort erfolgt und keine personenbezogenen Daten gespeichert oder zugänglich gemacht werden. Bei einer nachträglichen, manuellen Kontrolle liegt bereits keine Echtzeitanonymisierung mehr vor.

### Videoüberwachung mit KI-Funktion

Videoüberwachung mit KI-Funktion wird in Smart Cities eingesetzt, um öffentliche Räume zu beobachten und automatisiert auszuwerten, etwa zur Erkennung von Gefahrensituationen, zur Analyse von Personenströmen oder zur Unterstützung operativer Maßnahmen. Die KI ermöglicht dabei über die bloße Bildaufzeichnung hinausgehende Analysen, etwa durch Muster- oder Verhaltensauswertungen.

Datenschutzrechtlich handelt es sich um eine besonders eingriffsintensive Verarbeitung personenbezogener Daten. Videoaufnahmen im öffentlichen Raum erfassen regelmäßig identifizierbare Personen. Der Einsatz von KI verstärkt den Eingriff, da aus den Bilddaten zusätzliche Informationen gewonnen werden können. Die Zulässigkeit setzt daher eine klare und spezifische Rechtsgrundlage voraus. Eine allgemeine Zielsetzung wie die „Erhöhung der Sicherheit“ genügt hierfür regelmäßig nicht. Der Einsatz muss strikt zweckgebunden und verhältnismäßig ausgestaltet sein.

Wichtig sind hierbei vor allem Maßnahmen zur Datenminimierung und Transparenz. Soweit möglich, sind Echtzeitauswertungen ohne Speicherung personenbezogener Daten vorzusehen oder frühzeitige Anonymisierungen umzusetzen. Funktionen, die über die ursprünglich festgelegten Zwecke hinausgehen, sind unzulässig. Aufgrund der hohen Risiken für die Rechte der Betroffenen ist bei Videoüberwachung mit KI-Funktionen häufig eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich.

Soweit KI-gestützte Auswertungen eingesetzt werden, sind die Vorgaben der KI-VO (vgl. B. XI. 1.) parallel zu prüfen.

### Fahrgastzählsysteme im ÖPNV

Fahrgastzählsysteme im öffentlichen Personennahverkehr erfassen die Anzahl der ein- und aussteigenden Fahrgäste, um Auslastungen zu analysieren und den Betrieb effizienter zu steuern. Zum Einsatz kommen dabei unterschiedliche Technologien, etwa Infrarotsensoren, Kameras oder funkbasierte Verfahren.

Datenschutzrechtlich ist entscheidend, ob die eingesetzte Technik einen Personenbezug herstellt oder zumindest ermöglicht. Während rein zählende Sensoren ohne Identifizierungs- oder Wiedererkennungsfunktionen in der Regel keinen Personenbezug aufweisen, können kamerabasierte oder funkbasierte Systeme personenbezogene Daten verarbeiten. In diesen Fällen ist eine klare Rechtsgrundlage erforderlich, und die Verarbeitung muss auf die reine Zählfunktion beschränkt bleiben.

Besondere Bedeutung kommt der Datenminimierung zu. Systeme sind so auszugestalten, dass keine individuellen Bewegungsprofile entstehen und personenbezogene Daten nicht gespeichert oder weiterverwendet werden. Soweit technisch möglich, sind anonymisierte oder aggregierte Verfahren zu bevorzugen. Je nach eingesetzter Technologie und Umfang der Verarbeitung ist zu prüfen, ob eine DSFA nach Art. 35 DSGVO erforderlich ist.

### Passantenfrequenz-Messung

Bei der Passantenfrequenz-Messung werden Bewegungen und Anzahl von Fußgängerinnen und Fußgängern in bestimmten Bereichen des öffentlichen Raums erfasst, um Nutzungsmuster zu analysieren und städtische Planungs- oder Steuerungsentscheidungen zu unterstützen. Zum Einsatz kommen insbesondere Sensoren, Kameras oder funkbasierte Erfassungsmethoden.

Ähnlich wie bei den Fahrgastzählsystemen ist maßgeblich, ob die eingesetzten Systeme einen Personenbezug herstellen oder ermöglichen. Während rein zählende Sensoren ohne Wiedererkennungsfunktion regelmäßig datenschutzrechtlich unkritisch sind, können kamerabasierte oder funkbasierte Verfahren personenbezogene Daten verarbeiten, insbesondere wenn Geräte, Bewegungen oder Aufenthaltszeiten individualisierbar sind. In diesen Fällen ist eine tragfähige Rechtsgrundlage erforderlich.

Zu berücksichtigen sind insbesondere eine strenge Zweckbindung und Datenminimierung. Die Erfassung muss auf die reine Frequenzmessung beschränkt bleiben. Weitergehende Auswertungen, insbesondere die Erstellung von Bewegungsprofilen, sind meist unzulässig. Soweit möglich, sind auch hier anonymisierte oder stark aggregierte Verfahren einzusetzen. Aufgrund der Verarbeitung im öffentlichen Raum ist zudem zu prüfen, ob eine DSFA nach Art. 35 DSGVO erforderlich ist.

Soweit KI-gestützte Auswertungen eingesetzt werden, sind die Vorgaben der KI-VO (vgl. B. XI. 1.) parallel zu prüfen.

### Smart-City-Apps und zentrale Nutzerkonten

Smart-City-Apps und zentrale Nutzerkonten dienen als digitale Schnittstelle zwischen Stadt und Bürgerinnen und Bürgern. Sie ermöglichen den Zugriff auf unterschiedliche städtische Dienstleistungen, Informationen und Beteiligungsangebote und bündeln diese häufig in einem einheitlichen Nutzerkonto.

Solche Anwendungen verarbeiten in der Regel personenbezogene Daten, darunter Registrierungsdaten, Nutzungs- und Interaktionsdaten sowie gegebenenfalls Standort- oder Präferenzinformationen. Die Datenverarbeitung erfolgt typischerweise nutzerbezogen und dauerhaft, was erhöhte Anforderungen an Rechtsgrundlage, Zweckbindung und Transparenz stellt. Je nach Ausgestaltung kommen insbesondere Art. 6 Abs. 1 lit. b DSGVO bei vertraglich bereitgestellten Diensten oder Art. 6 Abs. 1 lit. e DSGVO bei öffentlich-rechtlichen Angeboten in Betracht.

Besondere Bedeutung kommt der Zwecktrennung zu. Werden über ein zentrales Nutzerkonto mehrere Dienste angebunden, müssen die jeweiligen Zwecke klar abgegrenzt und technisch voneinander getrennt werden. Eine pauschale Zusammenführung aller Nutzungsdaten ist unzulässig. Zudem sind hohe Anforderungen an

Datensicherheit, Zugriffskontrollen und die Wahrung der Betroffenenrechte zu stellen. Aufgrund der Bündelung personenbezogener Daten ist zu prüfen, ob eine DSFA nach Art. 35 DSGVO erforderlich ist.

# Rechtsfolgen von Datenschutzverstößen

Verstöße gegen DSGVO-Pflichten können zu erheblichen rechtlichen, finanziellen und faktischen Folgen führen.

## Aufsichtsrechtliche Maßnahmen und Projektstopps

Die Aufsichtsbehörden verfügen über weitreichende Befugnisse, um auf DSGVO-Verstöße zu reagieren. Sie können u.a. Verarbeitungen beanstanden, Anpassungen anordnen, Datenlöschungen verlangen oder den Betrieb ganz oder teilweise untersagen (Art. 58 Abs. 2 DSGVO). Dies kann, vor allem bei Datenplattformen und Verkehrs- oder Sensorsystemen im öffentlichen Raum, zu erheblichen Projektverzögerungen, Systemabschaltungen oder Nachbesserungskosten führen.

## Bußgeld

Verstöße können zudem auch mit empfindlichen Geldbußen in Höhe von bis zu mehreren Millionen Euro sanktioniert werden (Art. 83 DSGVO). Für öffentliche Stellen sieht Art. 83 Abs. 7 DSGVO allerdings vor, dass die Mitgliedstaaten regeln können, ob und in welchem Umfang Behörden mit Geldbußen belegt werden. In Deutschland wird gegenüber Behörden regelmäßig auf die Verhängung von Bußgeldern verzichtet (§ 43 Abs. 3 BDSG). Stattdessen stehen aufsichtsrechtliche Anordnungen im Vordergrund. Dies gilt jedoch nicht für öffentliche Stellen, die am Markt wirtschaftlich tätig sind (z.B. Stadtwerke, kommunale Verkehrsbetriebe).

Gleichwohl besteht auch für Behörden ein mittelbares Bußgeldrisiko, wenn kommunale Unternehmen oder private Projektpartner als (Mit-)Verantwortliche eingebunden sind und gegen diese Geldbußen verhängt werden, die das Gesamtprojekt wirtschaftlich und organisatorisch belasten können.

## Schadensersatz

Verantwortliche haften zudem auf Schadensersatz für materielle und immaterielle Schäden (Art. 82 DSGVO). Dieses Risiko ist im Smart-City-Kontext besonders relevant, da Verarbeitungen eine große Zahl von Personen betreffen (z.B. Kamera-, Mobilitäts- oder Nutzungsdaten). Schon einzelne Defizite bei Transparenz, Zweckbindung oder Datensicherheit können zu vielen parallelen Ansprüchen führen. Bei gemeinsamer Verantwortlichkeit können zudem interne Ausgleichs- und Regressfragen entstehen (Art. 26, Art. 82 DSGVO).

## Vertrauens- und Akzeptanzschäden

Neben formalen Sanktionen drohen Kommunen erhebliche Reputations- und Vertrauensverluste. Datenschutzverstöße werden oftmals öffentlich wahrgenommen und können die Akzeptanz von Smart-City-Diensten nachhaltig beeinträchtigen. Dies kann sich in geringerer Nutzung, politischem Widerstand oder erhöhtem Kommunikations- und Beteiligungsaufwand niederschlagen. Gerade weil Smart-City-Anwendungen oft

im öffentlichen Raum stattfinden, wirken sich Defizite bei Transparenz oder Verarbeitungssicherheit (Art. 12 ff, 32 DSGVO) besonders sichtbar aus.

# Fazit

Allgemein gilt, dass Smart-City-Projekte datenschutzrechtlich nicht als Ausnahme- oder Sonderfälle zu behandeln sind, sondern den allgemeinen Anforderungen der DSGVO in besonderem Maße unterliegen. Die datengetriebene Vernetzung urbaner Infrastrukturen erhöht regelmäßig die Eingriffsintensität und erfordert eine frühzeitige Klärung von Personenbezug, Verantwortlichkeiten, Rechtsgrundlagen und Risiken. Datenschutzkonforme Smart Cities entstehen nicht durch nachträgliche Korrekturen, sondern durch eine vorausschauende, transparente und technisch wie organisatorisch integrierte Gestaltung der Datenverarbeitung. Wird Datenschutz von Beginn an berücksichtigt, kann dies nicht nur rechtliche Risiken minimieren, sondern auch Vertrauen schaffen und den nachhaltigen Erfolg von Smart-City-Projekten unterstützen.

**Koordinierungs- und Transferstelle Modellprojekte Smart Cities**

Heinrich-Konen-Straße 1 | 53227 Bonn
Telefon: +49 30 / 67055 – 9999

E-Mail: SmartCities@dlr.de
Webseite: www.smart-city-dialog.de