# DSGVO-Aspekte der Swarm Perception Plattform und Lösungen

## Unverbindlicher DSGVO-Leitfaden für Systemintegratoren und Endkunden

# Inhalt

# 1 Schlüsselwörter

Die wichtigsten Schlüsselwörter, die in diesem Dokument verwendet werden:

Die Datenschutz-Grundverordnung (kurz **DSGVO**) ist die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

**Personenbezogene Daten** (Art. 4 (1) DSGVO)**:** Die DSGVO definiert personenbezogene Daten als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (**Mensch**) beziehen. Als identifizierbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer (z. B. einem Kfz-Kennzeichen), zu Standortdaten, zu einer Online-Kennung (z. B. IP-Adresse oder Cookie-Kennung) oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, wie etwa einem Bild (Film oder Video), Geschlecht oder Alter.

**Sensible Daten** (Art. 4 (14) DSGVO): Eine besondere Kategorie personenbezogener Daten (z.B. biometrische Daten), deren Verarbeitung nur in den in Art. 9 (2) DSGVO genannten Fällen zulässig ist. Die Verarbeitung solcher sensibler Daten erfordert in der Regel immer die ausdrückliche Zustimmung der betroffenen Person.

**Biometrische Daten** (Art. 4 (14) DSGVO): Sensible Daten, die sich aus einer spezifischen technischen Verarbeitung ergeben und sich auf die physischen, physiologischen oder verhaltensbezogenen Merkmale einer natürlichen Person beziehen, die eine eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie z. B. Gesichtsmerkmale oder Fingerabdrücke.

**Pseudonymisierte Daten** (Art. 4 (5) DSGVO): Daten, bei denen der Personenbezug entfernt (pseudonymisiert) wurde (z. B. durch Verschlüsselung), die aber mit rechtlich zulässigen, vernünftigerweise verwertbaren Mitteln wiederhergestellt werden können, so dass eine Person identifizierbar ist. Pseudonymisierte Daten unterliegen der Datenschutz-Grundverordnung.

**Anonyme/anonymisierte Daten**: Daten, bei denen der Personenbezug von vornherein fehlt (anonyme Daten) oder die entfernt wurden und nicht mit rechtlich zulässigen, vernünftigerweise verwertbaren Mitteln wiederhergestellt werden können (anonymisierte Daten). Anonyme/anonymisierte Daten unterliegen nicht der DSGVO.

**Verarbeitung personenbezogener Daten** (Art. 4 (2) DSGVO)**:** Jeder Vorgang, der an oder mit personenbezogenen Daten durchgeführt wird, wie das Erheben, das Speichern, die Organisation, die Strukturierung, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, die Anpassung oder die Kombination, die Einschränkung, das Löschen oder die Vernichtung.

**Für die Verarbeitung personenbezogener Daten Verantwortlicher** (Art. 4 (7) DSGVO)**:** Eine Person (natürliche oder juristische Person, z. B. ein Unternehmen), die über die Mittel und Zwecke der Verarbeitung personenbezogener Daten entscheidet. Die Person, die die Administratoren und Betreiber eines Online- oder Cloud-Dienstes leitet, ist in der Regel der Verantwortliche für die Verarbeitung personenbezogener Daten im Rahmen des Dienstes.

**Verarbeiter der personenbezogenen Daten** (Art. 4 (8) DSGVO)**:** Jemand (natürliche oder juristische Person, z. B. ein Unternehmen), der personenbezogene Daten im Auftrag eines für die Verarbeitung Verantwortlichen verarbeitet, ohne die Mittel und Zwecke der Verarbeitung personenbezogener Daten zu bestimmen. Der Anbieter eines Online- oder Cloud-Dienstes ist in der Regel der Verarbeiter personenbezogener Daten, die im Rahmen des Dienstes verarbeitet werden.

**Nutzer:** Ein Systemintegrator oder ein Endkunde, der die Swarm Analytics Anwendungen nutzt. Dieser Begriff kommt in der DSGVO nicht vor**.** Es wird davon ausgegangen, dass der Nutzer die Entscheidungsbefugnis hat, welche und wie Daten erzeugt, gespeichert, verarbeitet und in andere Datenverarbeitungssysteme eingespeist werden.

**Benutzerinhalte:** Alle Informationen oder Daten, die von Swarm Analytics Anwendungen erfasst und verarbeitet werden. Dieser Begriff kommt in der DSGVO nicht vor**.**

**Video Stream:** Videodaten, die von der Kamera an andere Netzwerkgeräte gesendet werden, z. B. an eine Swarm Perception Box und/oder an ein Speicher- oder Überwachungsgerät. Das am häufigsten verwendete Protokoll ist RTSP.

# 2 Einführung

## 2.1 Bedeutung der Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten

Der Schutz der Verarbeitung von personenbezogenen Daten ist in der gesamten Europäischen Union von großer Bedeutung. Die DSGVO ist Teil des EU-Rechts und legt die Bedingungen fest, unter denen die Verarbeitung personenbezogener Daten rechtskonform ist und welche Schutzmaßnahmen in diesem Zusammenhang ergriffen werden sollten. Jede unrechtmäßige Verarbeitung personenbezogener Daten kann zu hohen Geldstrafen führen. Aus diesem Grund ist die Rechtmäßigkeit der Verarbeitung personenbezogener Daten so wichtig.

Neben der DSGVO gibt es auch zahlreiche nationale Gesetze, die die Verarbeitung von personenbezogenen Daten regeln. In Österreich ist es zum Beispiel das Datenschutzgesetz (DSG). Dieses muss bei der Verarbeitung personenbezogener Daten beachtet werden.

## 2.2 Über Swarm Analytics

Die Swarm Analytics GmbH (kurz: Swarm Analytics) entwickelt revolutionäre KI-Technologie, um Kameras in **intelligente Sensoren** zu verwandeln. Dies führt zu intelligenteren, schnelleren, einfacheren und vertrauenswürdigen Lösungen und macht sie gleichzeitig erschwinglich. Basierend auf der Swarm

Analytics Sensortechnologie liefern die Lösungspartner eine breite Palette von intelligenten End-to-End Smart City Lösungen für Verkehr, Parken, öffentlichen Nahverkehr und Einzelhandel.

Swarm Analytics arbeitet mit Systemintegratoren aus der ganzen Welt zusammen. Diese Integratoren treffen sich mit den Endkunden, verkaufen ihnen die Produkte von Swarm Analytics und/oder übernehmen das Design, die Integration, die Installation und den Service der Produkte von Swarm Analytics. Normalerweise verkauft, installiert, konfiguriert und kalibriert der Systemintegrator das System für den Endkunden und wartet es auch. Daher besteht in Bezug auf die Swarm Analytics Anwendungen in der Regel keine direkte Rechtsbeziehung zwischen Swarm Analytics und dem Endkunden.

## 2.3 Über die Swarm Perception Plattform (Swarm Analytics Anwendungen)

Die Swarm Perception Plattform besteht aus dem Swarm Control Center und den Swarm Perception Boxen. Zusammen werden sie auch oft als Swarm Analytics Anwendung bezeichnet. Mit dem Swarm Control Center werden die Swarm Perception Boxen konfiguriert und verwaltet, wobei sie den Stream einer IP-Kamera empfangen und sofort die gesuchten Informationen extrahieren. Dies kann die Klassifizierung von Fahrzeugen sein, die Zählung von Personen, die eine bestimmte Zähllinie überqueren, oder die Aufenthaltsdauer von Personen und Fahrzeugen in bestimmten Regionen von Interesse. Diese Informationen werden verwendet, um mehr Einblicke in die Notwendigkeit von Verkehrsplanungsbemühungen sowie die Optimierung von Einzelhandelsumgebungen wie Einkaufszentren und Einkaufsstraßen zu erhalten. Nicht vergessen: Die Überwachung von Personen mit Videogeräten, die einen zugänglichen Stream erzeugen, bedeutet (zumindest im Prinzip) immer die Verarbeitung personenbezogener Daten!

## 2.4 Zweck dieses Dokuments

Der Zweck dieses Dokuments ist es, zu beschreiben, wie die Benutzerinhalte in Swarm Analytics Anwendungen verarbeitet werden, und Ihre Arbeit zur Einhaltung der DSGVO bestmöglich zu erleichtern, unabhängig davon, ob Sie ein Systemintegrator oder ein Endkunde sind.

Es ist nicht der Zweck dieses Dokuments, Rechtsberatung zu Datenschutzfragen im Einzelfall zu leisten oder sie zu ersetzen.

# 3 Die Swarm Perception Plattform und wie sie funktioniert

Die Swarm Perception Plattform besteht aus einer **Swarm Perception Box** und einem **Swarm Control** Center (SCC).

Die **Swarm Perception Box** wird entweder in einer von Swarm Analytics gelieferten dedizierten Hardware (P100, OP100, P101, OP101) oder in einem virtuellen Docker-Container (VPX, SPL) auf einem vom Benutzer bereitgestellten Host-System eingesetzt.

So oder so wird der Videostream der jeweiligen IP-Kamera in die Swarm Perception Box geleitet und diese analysiert die Inhalte entsprechend ihrer Konfiguration (Objekterkennung und Objektklassifizierung).

Diese Konfiguration erfolgt über das **Swarm Control Center**, das alle Swarm Perception Boxes eines bestimmten Bereichs verwaltet. Es bestimmt das Analysemodell und Details wie Eingangs-/Ausgangslinien, Herkunfts- und Zielrichtungen.

Das Swarm Control Center läuft in einem IoT Hub auf MS Azure, der vom **Datenverarbeiter**, d.h. dem Endkunden oder einem Systemintegrator/Dienstleister, der dies im Auftrag des Endkunden tut, gesteuert wird.

Jeder Anwendungsfall besteht aus mehreren neuronalen Netzen, die für die Extraktion von Merkmalen aus dem gegebenen Videostream verantwortlich sind und die Ausgabe mit fallspezifischer Nachbearbeitung (z. B. Verkehrsüberwachung) kombinieren.

Die extrahierten Daten (numerische Informationsausgabe) werden von der Swarm Perception Box an eine vom Benutzer ausgewählte Datenbank übermittelt.

Dies sind typische Beispiele für Wahrnehmungskonfigurationen, die vom Benutzer für die jeweilige Swarm Perception Box über das Swarm Control Center konfiguriert werden können:

| | Traffic insights | People insights | Parking monitoring |
|---|---|---|---|
| **Objekt-Erkennung** | • Fahrzeug<br>• Fahrer<br>• Person | • Person<br>• Kopf<br>• Gesicht | • Fahrzeug<br>• Fahrer<br>• Nummernschild |
| **Objekt-Klassifizierung** | • Auto<br>• Van<br>• Motorrad<br>• Fahrrad<br>• LKW<br>• LKW + Anhänger<br>• Bus<br>• Andere | • Weiblich<br>• Männlich<br>• Alter (kommt 2023) | • Auto<br>• Van<br>• Motorrad<br>• Fahrrad<br>• LKW<br>• LKW + Anhänger<br>• Bus<br>• Andere<br>• Erkennung von Nummernschildern |
| **Wiedererfassung von Objekten** | • Ja | • Ja (kommt 2023) | • K.A. |
| **Ereignis-auslöser** | • Herkunft Bestimmung<br>• Zählende Linien<br>• Heatmap | • Virtuelle Tür<br>• Region von Interesse<br>• Heatmap | • Einzelraum-Zone<br>• Multispace-Zone<br>• Eingangs-/Ausgangszählung |
| **Meta-Informationen** | • Schätzung der Geschwindigkeit<br>• Verweildauer | • Verweildauer | • Verweildauer |

Potenzielle und tatsächliche DSGVO-sensible Konfigurationen:

### Person, Kopf, Gesicht, Geschlecht, Alter

Im Allgemeinen stellen charakteristische Merkmale einer Person wie Geschlecht, Alter, Gesicht usw. personenbezogene Daten im Sinne der Datenschutz-Grundverordnung dar.

Die Swarm Perception Box kann im Videostream erkennen, ob es sich um eine Person, einen menschlichen Kopf oder ein menschliches Gesicht handelt, ohne biometrische Daten zu verwenden. Stattdessen verwendet die Swarm Perception Box die im Algorithmus erstellten Vorlagen und vergleicht sie mit dem allgemeinen Erscheinungsbild der Personen, so dass der Benutzer nicht in der Lage ist, Personen zu extrahieren oder zu verfolgen. So ist es beispielsweise nicht möglich, eine bestimmte Person zu erkennen, die am nächsten Tag wieder in den Verkaufsraum kommt. Die Swarm Perception Box erstellt keine neuen Vorlagen aus dem VIDEO Stream selbst. Daher wird die numerische Ausgabe der Swarm Perception Box selbst als anonymisierte Daten betrachtet.

Wenn Personen mit der IP-Kamera überwacht werden und dieser Datenstrom zur Auswertung an die Swarm Perception Box weitergeleitet wird, stellt dies in jedem Fall eine Verarbeitung personenbezogener Daten im Sinne der DSGVO dar.

Wenn der Nutzer in diesen Fällen die IP-Kamera und die Swarm Perception Box betreibt, ist er auch der für die Verarbeitung personenbezogener Daten Verantwortliche im Sinne der DSGVO.

### Nummernschild-Erkennung

Für die Parkraumbewirtschaftung kann die Swarm Perception Box Nummernschildinformationen extrahieren.

Ein Kfz-Kennzeichen ist eine personenbezogene Information im Sinne der Datenschutz-Grundverordnung. Daher stellt die Kennzeichenerkennung immer eine Verarbeitung personenbezogener Daten dar und erfordert eine Rechtsgrundlage (Artikel 6 DSGVO).

Für die Erkennung einzelner Nummernschilder zur Automatisierung und Beschleunigung des Dienstes für Fahrzeuge, die auf der Whitelist stehen, ist es erforderlich, die Zustimmung aller Nutzer einzuholen und sicherzustellen, dass die Daten nicht für andere als die erforderlichen Dienste verwendet werden.

Statistische Daten über die Herkunft eines Fahrzeugs werden nicht als personenbezogene Daten betrachtet und können daher gesammelt und verarbeitet werden, ohne gegen die Datenschutzbestimmungen zu verstoßen. Die Erfassung und Auswertung eines Kfz-Kennzeichens zur Gewinnung statistischer Daten ist jedoch eine Verarbeitung personenbezogener Daten, für die eine Rechtsgrundlage erforderlich ist (Artikel 6 DSGVO).

ANMERKUNG: Diese Funktionen (Kennzeichen- und Geschlechts-/Altersschätzung) werden voraussichtlich im Jahr 2021 bzw. 2023 verfügbar sein und unterliegen der endgültigen Bestätigung. Die gegenständliche Zusammenfassung dient lediglich dazu, um Sensibilität zu erzeugen, dass individuelle Kennzeichenerkennung eindeutig Daten sind, die der GDPR-Compliance unterliegen.

# 4 Welche Art von Daten werden von der Swarm Perception Plattform erfasst und gespeichert?

Der in die Swarm Perception Box geleitete VIDEO Stream enthält in der Regel personenbezogene Daten (Aussehen/KFZ-Kennzeichen etc.) der von der IP-Kamera überwachten Personen. Das bedeutet, dass die Analyse dieser Inhalte (Objekterkennung und Objektklassifizierung) in der Swarm Perception Box in der Regel personenbezogene Daten verarbeitet. Daher handelt es sich bei den erfassten und in der Swarm Perception Plattform verarbeiteten Informationen (d. h. Benutzerinhalte) in der Regel um personenbezogene Daten.

Für diese Datenverarbeitung ist in der Regel der Nutzer verantwortlich, der das Videoüberwachungssystem und die Swarm Perception Box betreibt (Datenverarbeiter).

Die einzigen Daten, die von der Swarm Perception Plattform gespeichert werden, sind **numerische Informationen**, wie z. B. die Anzahl der Personen, die ein Geschäft/einen Ort während eines bestimmten Zeitraums betreten und verlassen haben, ihr Alter oder Geschlecht. Die Swarm Perception Plattform speichert kein Bild- oder Videomaterial. Es ist auch nicht möglich, die Videostreams über die Swarm Perception Plattform aufzuzeichnen:

```
{
  "Version": "1.0",
  "eventSchema": "https://swarm-analytics.com/schema/event/peopleinsights/1.0",
  "Knoten":{
    "id":"b8ade223-e847-4741-a405-7f62c0403aa2",
    "Name": "Test"
  },
  "capacityMonitoringEvent":{
    "zoneEvent": {
      "Objekte": [
       {
         "Klasse": "Person"
       }
      ],
      "zoneId": "69031920-6239-471e-a3d7-f241b7753fd0",
      "zoneName": "zone1",
      "Zustand": "besetzt",
      "Zeitstempel": "2020-01-02T14:59:27.85136Z",
      "AuslöserTyp": "time"
    }
  }
}
```


*Beispiel für numerische Informationen von Swarm Analytics People Counter im JSON-Format.*

Für die Beantwortung der Frage, ob die ausgegebenen numerischen Informationen pseudonymisierte Daten (die der DSGVO unterliegen) oder anonyme bzw. anonymisierte Daten (die nicht der DSGVO unterliegen) enthalten, ist es relevant, ob der Personenbezug zu den ausgegebenen numerischen Informationen mit rechtlich zulässigen, vernünftig anwendbaren Mitteln wiederhergestellt werden kann oder nicht.

Verbindet der Nutzer die Swarm Perception Plattform mit einer anderen Anwendung oder mit Hard- oder Software in einer Weise, die geeignet ist, Personen zu identifizieren oder identifizierbar zu machen (z.B. mit einem Videoüberwachungssystem), dann könnten die ausgegebenen numerischen Informationen personenbezogene (pseudonymisierte) Daten im Sinne der DSGVO darstellen.

Wenn der Nutzer die Swarm Perception Plattform nicht mit anderen Anwendungen oder mit Hard- oder Software in einer Weise verbindet, die geeignet ist, Personen zu identifizieren oder identifizierbar zu machen, dann könnten die ausgegebenen numerischen Informationen anonymisierte Daten darstellen, die nicht unter die DSGVO fallen.

Bei den ausgegebenen numerischen Informationen kann es sich auch um anonymisierte Daten handeln, wenn der Nutzer technische und rechtliche Maßnahmen ergreift, so dass es keine rechtlich zulässige Möglichkeit gibt, die Daten mit anderen Merkmalen (z.B. mit einem gespeicherten VIDEO Stream oder Daten aus anderen personalisierten Zugangskontrollsystemen) zu verknüpfen und damit bestimmte Personen zu identifizieren. Solche Maßnahmen könnten z.B. eine Verschlüsselung oder die Speicherung von Daten in zwei verschiedenen Datenbanken sein, ohne dass die zuständigen Stellen des Nutzers diese Daten miteinander verknüpfen können.

# 5 DSGVO-Rollen und Verantwortlichkeiten

Die Person, die in den meisten Fällen für die DSGVO-Konformität der Swarm Perception Plattform zur Verarbeitung personenbezogener Daten verantwortlich ist, ist der Nutzer (in der Regel der Endkunde) als

für die Verarbeitung personenbezogener Daten Verantwortlicher. Swarm Analytics trägt im Rahmen der DSGVO keine Verantwortung für eine solche Nutzung der Swarm Perception Plattform.

In solchen Fällen ist der Nutzer verpflichtet, technische und/oder organisatorische Maßnahmen zu ergreifen, um die in der DSGVO festgelegten Datenschutzgrundsätze umzusetzen (privacy by design). Für die Swarm Perception Plattform wären Beispiele für solche Maßnahmen ein restriktiver Zugang zu Verwaltungsschnittstellen und die Vermeidung der Kombination der ausgegebenen numerischen Informationen mit anderen Datenquellen, um Personen zu identifizieren oder sie identifizierbar zu machen.

Der Nutzer, der für die Verarbeitung personenbezogener Daten verantwortlich ist, ist außerdem verpflichtet, technische oder organisatorische Maßnahmen zu ergreifen, die standardmäßig eine möglichst wenig in die Privatsphäre eingreifende Verarbeitung der betreffenden personenbezogenen Daten gewährleisten (privacy by default). Im Zusammenhang mit Swarm Analytics Applications wäre ein Beispiel für solche Maßnahmen die Vermeidung von Videostreaming an ein anderes Ziel als die Swarm Perception Box, die es sofort anonymisiert und löscht.

Die Datenschutz-Grundverordnung verpflichtet Entwickler/Hersteller nicht dazu, "privacy by design" und "privacy by default" einzubauen. Zum Beispiel ist es für den technischen Support und die Konfiguration notwendig, dass der Administrator prinzipiell Zugriff auf das Bild der jeweiligen Kamera hat.

## 5.1 Swarm Analytics' DSGVO-Verpflichtung für die Swarm Perception Plattform

Wie bereits erwähnt, ist in der Regel der Nutzer der Swarm Perception Plattform für die Einhaltung der DSGVO verantwortlich. Nichtsdestotrotz möchte Swarm Analytics die Nutzer bei der Einhaltung der DSGVO so weit wie möglich unterstützen. Das ist auch der Hauptzweck dieses Dokuments. Alle Funktionen in der Swarm Perception Plattform zielen darauf ab, Ihre DSGVO-Compliance und Ihre Compliance mit den Privacy by Design- und Privacy by Default-Bestimmungen der DSGVO zu erleichtern.

### Pseudonymisierung vs. Anonymisierung

Wie bereits oben beschrieben, handelt es sich bei der Videoüberwachung von Personen im Allgemeinen um eine Verarbeitung personenbezogener Daten (Erscheinungsbild von Menschen). Diese Videoüberwachung findet in der IP-Kamera statt, so dass der VIDEO Stream, der an die Swarm Perception Box gesendet wird, personenbezogene Daten enthält. Die Analyse des VIDEO Streams in der Swarm Perception Box stellt die Verarbeitung personenbezogener Daten dar. Das Ergebnis dieser Analyse ist die Ausgabe numerischer Informationen, die entweder pseudonymisiert oder anonymisiert sein können.

Die Unterscheidung zwischen pseudonymisierten und anonymisierten Daten ist wichtig, weil anonymisierte Daten nicht unter die DSGVO fallen. Pseudonymisierte Daten hingegen unterliegen der DSGVO, so dass es eine Rechtsgrundlage für ihre Verarbeitung geben muss.

Ähnlich wie bei der Verarbeitung personenbezogener Daten im Rahmen der Videoüberwachung liegt es in der Verantwortung des Nutzers, die in der numerischen Informationsausgabe enthaltenen Daten zu pseudonymisieren oder zu anonymisieren.

Wenn der Nutzer technische und rechtliche Maßnahmen ergreift, damit die in der numerischen Informationsausgabe enthaltenen Daten nicht mit anderen Daten (wie dem gespeicherten Videostream o.ä.) in Verbindung gebracht werden können, kann es sich bei den in der numerischen Informationsausgabe enthaltenen Daten um anonymisierte Daten handeln.

Die meisten Anwendungen lassen sich so konfigurieren, dass Personen aus der Live-Ansicht der Kamera nicht mehr identifiziert werden können. Die Anonymisierung funktioniert wie folgt: Alle Videostreams und Bilder der Kamera werden blockiert. Die Debug-Ansicht zeigt weiterhin ein unscharfes Bild, d. h. man kann zwar sehen, was vor sich geht, aber man kann keine Personen aus dem Videostream identifizieren.

Als Softwarehersteller nimmt Swarm Analytics die Cybersicherheit ernst und stellt Mittel zur Verfügung, um Produkte und Anwendungen widerstandsfähiger und sicherer zu machen - zum Beispiel durch Authentifizierung, Autorisierung und Passwortdurchsetzung. Dies ist nicht spezifisch für die Swarm Analytics Anwendungen, sondern ein fester Bestandteil unserer Produktentwicklungsstrategie, die darauf ausgerichtet ist, Computer Vision schneller, einfacher, intelligenter, erschwinglicher und vertrauenswürdiger zu machen.

## 5.2 Speziell über die DSGVO-Verantwortung des Nutzers in Bezug auf die Swarm Perception Plattform

Bitte denken Sie daran, zu prüfen, welche genauen rechtlichen Verpflichtungen für Sie oder Ihr Unternehmen gelten, wenn Sie Swarm Analytics Anwendungen verwenden. In dieser Hinsicht übernimmt Swarm Analytics keine rechtliche Verantwortung (siehe den rechtlichen Haftungsausschluss unterhalb des Inhaltsverzeichnisses).

Wie bereits erwähnt, stellt die Nutzung der Videoüberwachung und die Analyse des Videostreams in der Swarm Perception Plattform eine Verarbeitung personenbezogener Daten dar. In solchen Fällen sind Sie (Ihr Unternehmen) als Nutzer dieser Anwendungen ein für die Verarbeitung personenbezogener Daten Verantwortlicher im Sinne der DSGVO. Die Datenschutz-Grundverordnung stellt eine Reihe von Anforderungen an die für die Verarbeitung personenbezogener Daten Verantwortlichen. Sie sollten die folgenden Schritte berücksichtigen, wenn Sie die DSGVO einhalten:

a. Bitte prüfen Sie, ob der beabsichtigte Zweck der Datenverarbeitung (z.B. Objektschutz durch Videoüberwachung) nicht durch mildere Mittel (z.B. Einsatz von Sicherheitspersonal etc.) erreicht werden kann.
b. Bitte geben Sie an, zu welchen Zwecken die Videoüberwachung/Swarm Analytics Anwendungen zur Verarbeitung personenbezogener Daten eingesetzt werden (z. B. Werbung, Objektschutz, Parkraumbewirtschaftung usw.) und bewahren Sie diese Dokumentation zu Beweiszwecken in schriftlicher Form auf.
c. Informieren Sie (z. B. durch ein Informationsschild) die betroffenen Personen (Personen, deren personenbezogene Daten Sie verarbeiten) über die Datenverarbeitung und deren Zwecke. Die Informationen umfassen unter anderem, welche Arten von personenbezogenen Daten Sie erheben und für welche Zwecke Sie die Daten verwenden.
d. Verwenden Sie personenbezogene Daten niemals für einen anderen als den/die von Ihnen angegebenen Zweck(e).
e. Bitte vergewissern Sie sich, dass Sie eine Rechtsgrundlage gemäß Artikel 6 DSGVO für die Verarbeitung personenbezogener Daten haben, z. B. eine Einwilligung der betroffenen Personen, berechtigte Interessen oder die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde.
f. Stellen Sie die Einführung und Aufrechterhaltung effizienter Verwaltungsfunktionen für personenbezogene Daten sicher, um Anfragen, um Anfragen von betroffenen Personen bezüglich der von Ihnen gespeicherten personenbezogenen Daten nachkommen zu können.
g. Ergreifen Sie Sicherheitsmaßnahmen für alle von Ihnen verarbeiteten personenbezogenen Daten (z. B. geregelte Zugangskontrollen, Verschlüsselung, Speicherung in verschiedenen Datenbanken usw.).
h. Wenn Sie mit einem Datenverarbeiter zusammenarbeiten, vergessen Sie nicht, einen Vertrag mit dem Verarbeiter abzuschließen (Art. 28 DSGVO).
i. Vergessen Sie nicht, personenbezogene Daten zu löschen, sobald ihre Verarbeitung für den jeweiligen Zweck nicht mehr erforderlich ist. Die Speicherdauer sollte so kurz wie möglich sein und idealerweise 72 Stunden nicht überschreiten.

j. Denken Sie daran, die in den ausgegebenen numerischen Informationen enthaltenen Daten zu pseudonymisieren oder zu anonymisieren, indem Sie technische und rechtliche Maßnahmen ergreifen (siehe oben).
k. Die systematische Überwachung eines öffentlich zugänglichen Bereichs in großem Umfang erfordert eine Datenschutz-Folgenabschätzung. Die Datenschutzbehörden der EU-Mitgliedsstaaten können jedoch Ausnahmen hiervon machen. In Österreich ist zum Beispiel die Videoüberwachung von Geschäftsräumen mit Kundenverkehr oder von Parkplätzen in Einkaufszentren unter bestimmten Voraussetzungen von der Datenschutz-Folgenabschätzung ausgenommen.[1] Auch Bild- und Tonübertragungen ohne Aufzeichnung (in Echtzeit) sind unter bestimmten Voraussetzungen von der Datenschutz-Folgenabschätzung ausgenommen.[2]

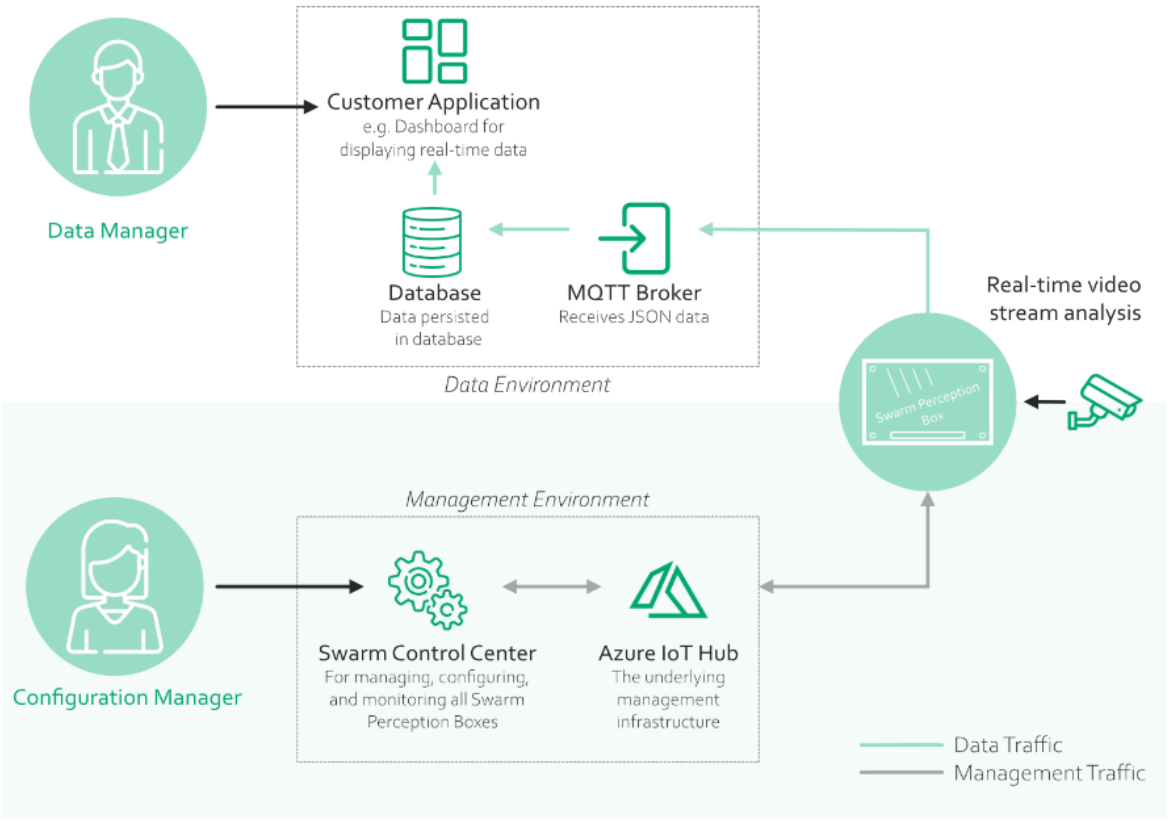
# 6 Einsatzarten

Wir unterscheiden zwischen 3 verschiedenen Einsatzarten, wobei die beiden bestimmenden Parameter sind, ob der Kamerastream für verschiedene Zwecke (z.B. Sicherheitsüberwachung) verwendet wird und ob der Kamerastream in die Swarm Perception Box am Standort jeder Kamera geleitet oder an eine zentralere Stelle im Netzwerk übertragen wird.

| | Dezentrale Analyse | Zentralisierte Analyse |
|---|---|---|
| Dedizierte Kamera | Die Swarm Perception Box wird direkt an die Kamera angeschlossen und extrahiert anonymisierte Informationen in Echtzeit, ohne dass ein Stream an einen anderen Ort weitergeleitet wird. | Die Swarm Perception Box und die Kamera befinden sich an unterschiedlichen Standorten, und die anonymisierten Informationen werden in Echtzeit extrahiert. Der Videostream wird über ein IP-Netzwerk an den anderen Standort weitergeleitet, aber nicht gespeichert, überwacht oder in irgendeiner Weise aufgezeichnet. |
| Mehrzweck-kamera (vorhandenes DVR/CCTV-System) | Die Videostreams werden an ein Überwachungs- und/oder Speichersystem weitergeleitet. Zusätzlich wird der Stream analysiert und anonymisierte Daten werden von einer Swarm Perception Box extrahiert. | |

Für alle Bereitstellungen wird die allgemeine Verwaltungseinrichtung auf die gleiche Weise gehandhabt, d. h. die folgende Zeichnung ist für alle Szenarien anwendbar.

[1] DSFA-A09 Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV)
[2] DSFA-A10 Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV)




# 7 Swarm Perception Plattform als dezentraler, dedizierter Kameraeinsatz

**Funktionsweise**

Die Netzwerkkamera in einem lokalen Netzwerk ist mit einer Swarm Perception Box (IP muss über das Netzwerk erreichbar sein) verbunden, sodass der Videostream direkt angeschlossen werden kann und kein anderes Gerät damit interagieren kann - dies kann entweder über einen PoE-Switch oder direkt an die PoE-Schnittstelle der Swarm Perception Box erfolgen.

Dies ist vor allem dann der Fall, wenn der einzige Zweck des Systems darin besteht, als Sensor zu fungieren. In diesem Anwendungsfall finden alle Aktivitäten im lokalen Netz des Endkunden statt, und die Kamera fungiert als visueller Sensor ohne die Möglichkeit, Videoinhalte aus Gründen der Videoüberwachung zu speichern.

## 7.1 Swarm Perception Plattform als zentralisierter, dedizierter Kameraeinsatz

**Funktionsweise**

Bei größeren Einsätzen kann die Swarm Perception Box auf einem Hostsystem (z. B. einem Server) installiert werden, das sich in Reichweite der Netzwerkkameras befindet, um eine direkte Verbindung über VIDEO ohne CCTV/DVR als Streaming-Quelle herzustellen. Dies ermöglicht den Einsatz von Kameras in großem Umfang mit dem alleinigen Zweck, Textinformationen zu sammeln, anstatt Videoaufzeichnungsfunktionen und -aspekte einzubringen.

Für diese Einrichtung ist ein gesichertes IP-Netzwerk (z. B. durch eine Firewall) erforderlich, in dem der Server installiert ist und mit allen benötigten Kameras verbunden werden kann. Die Kamerastreams werden dann auf dem dedizierten System verarbeitet, ohne gespeichert zu werden oder anderen Diensten zur Verfügung zu stehen. Es ist sicherzustellen, dass das Hostsystem und der Netzwerkpfad durch Standard-Sicherheitsmaßnahmen (Benutzerkonten, Firewall usw.) vor nicht genehmigtem Zugriff geschützt sind.

## 7.2 Swarm Perception Plattform als Erweiterung bestehender CCTV/DVR-Installationen

**Wie es funktioniert**

In einer Einsatzumgebung, in der bereits ein CCTV-System vorhanden ist, wird die Swarm Analytics Anwendung neben der bestehenden Infrastruktur eingesetzt und stellt entweder über das Verwaltungsnetzwerk des CCTV-Systems eine Verbindung zum Server her oder direkt zu jeder Kamera über IP, wenn das Netzwerk erreichbar ist. In einem solchen Einsatzszenario wird der Videostream vom CCTV-System aufgezeichnet, und die Kamera ist daher kein visueller Einzwecksensor, sondern ein Mehrzweckgerät, das Videodaten sowie extrahierte anonymisierte Informationen liefert.

## 7.3 DSGVO-Aspekte bei der Nutzung der Swarm Perception Plattform in jedem Einsatzszenario

Die Videoüberwachung mit der Kamera und die Analyse des Streams in der Swarm Perception Plattform stellen eine Verarbeitung von personenbezogenen Daten dar.

Der Nutzer (für die Verarbeitung personenbezogener Daten Verantwortlicher) sollte technische und rechtliche Maßnahmen ergreifen, um sicherzustellen, dass es keine andere Möglichkeit gibt, die ausgegebenen numerischen Informationen mit den Daten aus dem Videoinhalt zu verbinden. In diesem Fall könnte es sich bei den ausgegebenen numerischen Informationen um anonymisierte Daten handeln, die nicht unter die DSGVO fallen.

Swarm Analytics hat keinen Zugriff auf Ihre Nutzerinhalte, d. h. die von der Swarm Perception Plattform erfassten und verarbeiteten Informationen, es sei denn, Sie gewähren einen solchen Zugriff (in der Standardinstallation ist ein solcher Zugriff ohne die Zustimmung des Azure-Kontoinhabers nicht möglich).

Wenn die Swarm Perception Boxen in einem lokalen Netzwerk installiert sind und nicht mit einem bestimmten Datenendpunkt verbunden sind (entweder durch den Kunden selbst oder einen Systemintegrator), dann ist Swarm Analytics kein Verarbeiter personenbezogener Daten in Bezug auf die von der Swarm Perception Plattform erfassten personenbezogenen Daten. Swarm Analytics stellt diese Anwendungen lediglich zur Verfügung - ohne weitere Beteiligung an der Nutzung und/oder Verarbeitung personenbezogener Daten durch die Anwendung.

Je nach Einrichtung der Swarm Perception Plattform können die Rollen des Datenverarbeiters und des für die Datenverarbeitung Verantwortlichen vom Endkunden auf den Systemintegrator übertragen werden und umgekehrt. Wir empfehlen, dass Sie untersuchen, wie die DSGVO-Verantwortung unter Ihrer spezifischen Einrichtung zugewiesen wird. Wenn Sie sich dafür entscheiden, die Swarm Analyseanwendungen mit anderen Dienstanbietern zu verbinden (z. B. Visualisierungstools von Drittanbietern, Business-Intelligence-Tools usw.), empfehlen wir Ihnen, zu prüfen, wie die DSGVO-Verantwortung im Rahmen dieser spezifischen Dienstkonfiguration zugewiesen wird.

# 8 Beispiele für Anwendungsfälle → mögliche DSGVO-Aspekte

Allgemeine Hinweise: Wenn Sie als Datenverarbeiter personenbezogene Daten zur Wahrung der berechtigten Interessen (Art. 6 (1) (f) DSGVO) verarbeiten, müssen Sie sicherstellen, dass diese berechtigten Interessen nicht durch die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwogen werden (Interessenabwägung). Es ist nicht ausreichend, auf abstrakte Situationen zu verweisen oder sie mit ähnlichen Fällen zu vergleichen. Die folgenden Anwendungsfälle haben daher nur demonstrativen Charakter und ersetzen nicht die vorgeschriebene Interessenabwägung im Einzelfall.

Achtung: Öffentliche Stellen können personenbezogene Daten nicht für die Zwecke der berechtigten Interessen (Art. 6 (1) (f) DSGVO) bei der Erfüllung ihrer Aufgaben verarbeiten.

### Typische Verkehrszählung durch ein privates Verkehrsplanungsbüro

Die Aufzeichnung von Bilddaten bzw. Kennzeichen im Rahmen einer Verkehrszählung durch ein privates Verkehrsplanungsbüro stellt eine Verarbeitung personenbezogener Daten dar, die mit der DSGVO konform sein muss.

Die Rechtsgrundlage für eine solche Datenverarbeitung könnten berechtigte Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten oder die Wahrnehmung einer Aufgabe sein, die im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde.

Nach dem Grundsatz der Datenminimierung sollte die Überwachung so wenig wie möglich oder nötig personenbezogene Daten von Verkehrsteilnehmern betreffen. Der Verantwortliche sollte rechtliche und technische Maßnahmen ergreifen, damit die Videoüberwachung z.B. keine Personen im Fahrzeug erfasst und die Nummernschilder nur aufgezeichnet werden, wenn dies unbedingt erforderlich ist.

Der für die Datenverarbeitung Verantwortliche sollte rechtliche und technische Maßnahmen ergreifen, damit die ausgegebenen numerischen Informationen nicht mit anderen Daten (z. B. Videodateien) in Verbindung gebracht werden können. Wenn diese Anforderungen erfüllt sind, kann die numerische Informationsausgabe anonymisierte Daten darstellen, die nicht unter die DSGVO fallen.

Hinweis: Dies ändert nichts an der Tatsache, dass die Videoüberwachung selbst eine Verarbeitung personenbezogener Daten darstellt und eine Rechtsgrundlage erfordert.

### Typische Verkehrszählung durch eine Straßenaufsichtsbehörde

Die Straßenaufsichtsbehörden haben auch die Aufgabe, bei Bedarf Maßnahmen zur Regelung und Sicherung des Verkehrs zu ergreifen. Solche Maßnahmen können insbesondere in der Anordnung der Verkehrsregelung durch Lichtsignale bestehen. Um die Notwendigkeit solcher Maßnahmen zu klären, bedarf es mitunter entsprechender empirischer Verkehrsdaten, zum Beispiel aus Verkehrszählungen. Unabhängig davon, wer eine kamerabasierte automatische Verkehrszählung sozusagen "technisch" umsetzt, fällt dies in die rechtliche Zuständigkeit der jeweiligen örtlichen Straßenaufsichtsbehörde.

Wie bereits erwähnt, stellt die Aufzeichnung von Bilddaten bzw. von Nummernschildern im Rahmen einer Verkehrszählung durch eine Straßenaufsichtsbehörde eine Verarbeitung personenbezogener Daten dar, die mit der DSGVO vereinbar sein muss.

Die Rechtsgrundlage für eine solche Datenverarbeitung könnte die Wahrnehmung einer Aufgabe sein, die im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde. Eine solche "Aufgabe" muss durch Gesetz oder eine andere Rechtsgrundlage in dem jeweiligen Staat bestehen. Ein Beispiel hierfür wäre § 98f der österreichischen Straßenverkehrsordnung, wonach die Straßenverkehrsbehörden in bestimmten Fällen eine Videoüberwachung des Verkehrs durchführen dürfen, um beispielsweise die Dynamik, den Fluss und die Sicherheit des Verkehrs zu gewährleisten.

Auch in diesen Fällen sollte der für die Datenverarbeitung Verantwortliche rechtliche und technische Maßnahmen ergreifen, damit die ausgegebenen numerischen Informationen nicht mit anderen Daten (z. B. Videodateien) in Verbindung gebracht werden können. Wenn diese Anforderungen erfüllt sind, kann die numerische Informationsausgabe anonymisierte Daten darstellen, die nicht unter die DSGVO fallen.

### Videokontrolle des öffentlichen Raums durch eine öffentliche Behörde

Wie bereits erwähnt, stellt die Videoüberwachung in jedem Fall eine Verarbeitung personenbezogener Daten dar, für die eine Rechtsgrundlage erforderlich ist. Öffentliche Stellen können personenbezogene Daten nicht für die Zwecke der berechtigten Interessen (Art. 6 (1) (f) DSGVO) bei der Erfüllung ihrer Aufgaben verarbeiten.

Allerdings erlaubt die DSGVO den Behörden, personenbezogene Daten im Rahmen ihrer hoheitlichen Aufgaben zu verarbeiten (Art. 6 (1) (e) DSGVO), wobei sich die Rechtsgrundlage für solche Aufgaben, wie oben dargestellt, aus der nationalen Rechtslage ergibt. Solche "Aufgaben" müssen durch Gesetz oder eine andere Rechtsgrundlage in dem jeweiligen Staat bestehen (siehe Anwendungsfall oben).

So sind die Sicherheitsbehörden in Österreich durch das Sicherheitspolizeigesetz ermächtigt[3], öffentliche Plätze (z.B. Parks, Plätze, etc.) zu überwachen, um gefährliche Angriffe auf das Leben, die Gesundheit oder das Eigentum von Menschen zu verhindern. Die Kriminalpolizei und die Staatsanwaltschaft sind berechtigt, unter bestimmten Voraussetzungen Personen visuell zu überwachen.4

Wenn die Behörde aufgrund nationaler Rechtsvorschriften zur Videoüberwachung verpflichtet ist, kann diese Verpflichtung als Rechtsgrundlage gemäß Artikel 6 (1) (c) DSGVO dienen.

Die Datenschutz-Grundverordnung knüpft daher an diese nationale Rechtsgrundlage an, nennt aber keine eigene Rechtsgrundlage für die Videoüberwachung durch den öffentlichen Sektor. Wenn es keine nationale Rechtsgrundlage für die Videoüberwachung gibt, ist die Behörde nicht berechtigt, diese durchzuführen.

Wenn es eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten (Videoüberwachung) und für die Analyse des Videostreams in den Swarm Perception Boxen gibt, muss der für die Verarbeitung Verantwortliche sicherstellen, dass die ausgegebenen numerischen Informationen entsprechend anonymisiert werden, damit sie nicht unter die DSGVO fallen. Die Anonymisierung kann durch rechtliche und technische Maßnahmen erfolgen, so dass der Videostream und die ausgegebenen numerischen Informationen getrennt voneinander gespeichert oder aufbewahrt werden und kein Vergleich zwischen ihnen stattfinden kann. Im Idealfall wird der Videostream überhaupt nicht gespeichert.

### Videokontrolle der öffentlichen Verkehrsmittel

Wenn die Organisation und der Betrieb des öffentlichen Verkehrs nach nationalem Recht eine Angelegenheit der Hoheitsverwaltung ist, gelten für die Verarbeitung personenbezogener Daten die gleichen Bedingungen wie für die Videoüberwachung öffentlicher Räume (siehe oben).

In einigen Ländern wird der öffentliche Verkehr im Rahmen einer privatwirtschaftlichen Verwaltung organisiert und betrieben. In diesen Fällen handelt die Behörde nicht hoheitlich, sondern wie eine Privatperson. Dies ist zum Beispiel in Österreich der Fall.

In diesen Fällen könnte die Rechtsgrundlage für die Videoüberwachung und die Verarbeitung personenbezogener Daten im berechtigten Interesse des für die Verarbeitung Verantwortlichen liegen (Art. 6 Abs. 1 lit. f DSGVO). Die Interessenabwägung sollte erstellt und zu Dokumentations- und Beweiszwecken schriftlich festgehalten werden.

Wenn es eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten (Videoüberwachung) und für die Analyse des Videostreams in den Swarm Perception Boxen gibt, muss der für die Verarbeitung Verantwortliche sicherstellen, dass die ausgegebenen numerischen Informationen entsprechend anonymisiert werden, damit sie nicht unter die DSGVO fallen. Die Anonymisierung kann durch rechtliche und technische Maßnahmen erfolgen, so dass der Videostream und die ausgegebenen numerischen Informationen getrennt voneinander gespeichert oder aufbewahrt werden und kein Vergleich zwischen ihnen stattfinden kann.

[3] § 54 Abs 6 Österreichisches Sicherheitspolizeigesetz

[4] § 136 Österreichische Strafprozessordnung (StPO)

### Typische Einzelhandelssituation (z. B. Einkaufszentrum):

Die Videoüberwachung von Kunden im Eingangsbereich des Geschäfts mit einem Videoüberwachungssystem stellt in jedem Fall eine Verarbeitung personenbezogener Daten dar. Die Kunden müssen über die Überwachung sowie über die Datenverarbeitung und deren Zwecke informiert werden (z. B. durch ein Hinweisschild am Eingang des Ladens). In solchen Fällen ist der Ladenbetreiber höchstwahrscheinlich ein Datenverarbeiter im Sinne der DSGVO.

Wichtig ist auch der rechtliche Grund für die Datenverarbeitung. In den allermeisten Fällen wird dies die Wahrung der berechtigten Interessen des Shop-Betreibers sein (Art. 6 (1) f DSGVO). Dieser Rechtsgrund erfordert in jedem Einzelfall eine Interessenabwägung. Die Gründe für das Überwiegen der Interessen des Betreibers gegenüber den Interessen der betroffenen Kunden sollten schriftlich festgehalten werden.

Körperliche Merkmale von Personen wie das Geschlecht oder das Alter stellen in jedem Fall personenbezogene Daten dar, weil sie geeignet sind, eine Person identifizierbar zu machen. Theoretisch könnte es sich auch um besonders sensible (biometrische) Daten im Sinne von Artikel 9 DSGVO handeln.

Die Antwort auf diese Frage hängt unter anderem vom Zweck der Datenverarbeitung ab:

Wenn der Zweck der Videoüberwachung nicht darin besteht, eine bestimmte Person auf der Grundlage dieser Daten zu identifizieren, sondern nur darin, eine Kategorie von Personen von einer anderen zu unterscheiden (wie im obigen Beispiel), dann handelt es sich nicht um sensible Daten.

Möchte ein Datenverarbeiter eine bestimmte Person (einen Kunden) z.B. als Stammkunde oder Mitglied für maßgeschneiderte Werbung identifizieren, wäre der Zweck der Verarbeitung die eindeutige Identifizierung einer natürlichen Person. In diesem Fall müsste der Shop-Betreiber vor der Nutzung seines Systems die ausdrückliche Einwilligung aller betroffenen Personen einholen (Artikel 9 (2) DSGVO). Der Shop-Betreiber müsste außerdem sicherstellen (z. B. durch zwei getrennte Eingänge usw.), dass das System keine Personen erfasst, die keine Einwilligung gegeben haben.

Unabhängig davon, ob es sich um herkömmliche personenbezogene Daten oder um sensible Daten (Art. 9 DSGVO) handelt, sollte das Videoüberwachungssystem in einem Einkaufszentrum so eingerichtet werden, dass es nur die Kunden und nicht nur die Passanten erfassen kann.

Um die ausgegebenen numerischen Informationen als pseudonymisierte Daten (die der DSGVO unterliegen) oder als anonyme Daten (die nicht der DSGVO unterliegen) zu klassifizieren, ist es wichtig, dass der Nutzer rechtliche und technische Maßnahmen ergreift, um zu verhindern, dass numerische Informationen, die aus anderen Datenquellen ausgegeben werden, zugeordnet werden (insbesondere dem Videostream). Der Nutzer muss daher sicherstellen, dass die ausgegebenen numerischen Informationen keine Identifizierung von Personen zulassen.

Wenn die ausgegebenen numerischen Informationen anonymisiert wurden, können sie aus Sicht der DSGVO wie erforderlich verwendet und verarbeitet werden, da es sich nicht um personenbezogene Daten im Sinne der DSGVO handelt.

### Typische Situation der Parkraumbewirtschaftung

*Beispiel 1: Bewirtschafteter Parkplatz mit individueller Zufahrt durch Kennzeichenerkennung*

Systeme zur Erfassung von Kfz-Kennzeichen, um ein- und ausfahrtberechtigte Fahrzeuge identifizieren zu können, können auf der Grundlage berechtigter Interessen zulässig sein (Art. 6 (1) f DSGVO).

Wichtig ist, dass der Betreiber technische und organisatorische Maßnahmen ergreift, um negative Folgen für betroffene Personen auszuschließen. Diese können z.B. darin bestehen, dass nur die unteren Bereiche von Fahrzeugen aufgezeichnet werden (und nicht die Windschutzscheibe) oder die

Videoaufzeichnungen entweder gar nicht oder nur für einen kurzen Zeitraum (z.B. einen Tag) gespeichert werden.

Der Betreiber sollte rechtliche und technische Maßnahmen ergreifen, damit der Videostream und die ausgegebenen numerischen Informationen getrennt voneinander gespeichert oder aufbewahrt werden und kein Vergleich zwischen ihnen stattfinden kann.

Sobald die ausgegebenen numerischen Informationen nicht mit anderen Daten in Verbindung gebracht werden können (z. B. weil der Videostream nicht mehr existiert), kann es sich um anonymisierte Daten handeln, die nicht unter die DSGVO fallen.

Unter bestimmten Voraussetzungen kann die Videoüberwachung von der Pflicht zur Durchführung der Datenschutz-Folgenabschätzung ausgenommen werden, z.B. wenn die Videoüberwachung in Echtzeit (ohne Aufzeichnung) erfolgt und nur das Firmeneigentum aufgezeichnet wird. Die EU-Mitgliedstaaten legen die Ausnahmen eigenständig fest.

### Beispiel 2: Unbewirtschaftete Parkplätze: Kapazitätsmessungen, Verweildauer, usw.

Auch die Videoüberwachung von unbewirtschafteten Parkflächen (mit freiem Zugang) zur Ermittlung der Belegung der Parkflächen (Kapazitätsmessungen) oder der Parkdauer könnte auf der Grundlage berechtigter Interessen zulässig sein (Art. 6 (1) f DSGVO).

Auch in solchen Fällen ist es wichtig, dass der Betreiber technische und organisatorische Maßnahmen ergreift, um negative Folgen für betroffene Personen auszuschließen. Diese können z.B. darin bestehen, dass nur die unteren Bereiche von Fahrzeugen aufgezeichnet werden (und nicht die Windschutzscheibe) oder die Videoaufnahmen entweder gar nicht oder nur für einen kurzen Zeitraum (z.B. einen Tag) gespeichert werden.

Sobald die ausgegebenen numerischen Informationen nicht mit anderen Daten in Verbindung gebracht werden können (z. B. weil der Videostream nicht mehr existiert), kann es sich um anonymisierte Daten handeln, die nicht unter die DSGVO fallen.

Unter bestimmten Voraussetzungen kann die Videoüberwachung von der Pflicht zur Durchführung der Datenschutz-Folgenabschätzung ausgenommen werden, z.B. wenn die Videoüberwachung in Echtzeit (ohne Aufzeichnung) erfolgt und nur das Firmeneigentum aufgezeichnet wird. Die EU-Mitgliedstaaten legen die Ausnahmen eigenständig fest.

### Beispiel 3: Bereiche für potenzielle Kurzparkzonen (Videoüberwachung durch die Stadtverwaltung)

Wie bereits erwähnt, dürfen die Behörden die Verarbeitung personenbezogener Daten nicht auf berechtigte Interessen stützen. Vielmehr ergibt sich der Rechtsgrund für die Datenverarbeitung in der Regel aus einer gesetzlichen Verpflichtung (Art. 6 (1) c DSGVO) oder einer gesetzlichen Erlaubnis (Art. 6 (1) e DSGVO) zur Datenverarbeitung. In beiden Fällen muss die entsprechende nationale Rechtsgrundlage bestehen, die die behördlichen Rechte und Pflichten bei der Datenverarbeitung festlegt.

In Österreich beispielsweise sind die Straßenverkehrsbehörden nach § 98f der österreichischen Straßenverkehrsordnung befugt, in bestimmten Fällen, etwa zur Gewährleistung der Dynamik, des Flusses und der Sicherheit des Verkehrs oder zur Erfüllung der den Behörden und Straßenerhaltern gesetzlich obliegenden Aufgaben, eine Videoüberwachung des Verkehrs durchzuführen.

Gemäß § 25 Straßenverkehrsordnung sind die Straßenbehörden berechtigt, durch Verordnung Kurzparkzonen einzurichten, wenn und soweit dies zu bestimmten Zeiten aus ortsbezogenen Gründen (auch im Interesse der Wohnbevölkerung) oder zur Verkehrsberuhigung erforderlich ist.

Es ist daher denkbar, dass die Straßenverkehrsbehörden mit Hilfe der Videoüberwachung potenzielle Kurzparkzonen auf diese Rechtsgrundlagen hin untersuchen.

Um sicherzustellen, dass es sich bei den ausgegebenen numerischen Informationen um anonymisierte Daten handelt, sollten rechtliche und technische Maßnahmen getroffen werden (siehe oben).

Wichtig ist auch, dass die Videoüberwachung nach dem Grundsatz der Datenminimierung so wenig wie möglich in die Rechte der Betroffenen eingreift (keine Fahrzeuginsassen erkennbar etc.).