GDPR Aspects of The Swarm Perception Platform and Solutions

Non-binding GDPR-Guidelines for system integrators and end customers

Contents

1 Keywords

The most important keywords used in this document:

The General Data Protection Regulation (short **GDPR**) is the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Personal data (Art 4 (1) GDPR)**:** The GDPR defines personal data as any information relating to an identified or identifiable natural person (**human being**). An identifiable person is someone who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number (e.g. vehicle license plate), location data, online identifier (e.g. IP-addresses or cookie identifier), or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person, such as an image (footage or video), gender or age.

Sensitive data (Art 4 (14) GDPR): A special category of personal data (e.g. biometric data), which processing is only permitted in the cases specified in Art 9 (2) GDPR. The processing of such sensitive data generally always requires the express consent of the person concerned.

Biometric data (Art 4 (14) GDPR): Sensitive data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial features or fingerprints.

Pseudonymized data (Art 4 (5) GDPR): Data in which the personal reference has been removed (pseudonymized) (e.g. through encryption), but can be restored with legally permissible, reasonably usable means, so a person is identifiable. Pseudonymized data are subject to the GDPR.

Anonymous/anonymized data: Data in which the personal reference is missing from the beginning (anonymous data) or has been removed and cannot be restored by legally permissible, reasonably usable means (anonymized data).Anonymous/anonymized data is not subject to the GDPR

Processing of personal data (Art 4 (2) GDPR)**:** Any operation performed on or with personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal data controller (Art 4 (7) GDPR)**:** Someone (natural or legal person, e.g. a company) who determines the means and purposes of the processing of personal data. The person who directs the admins and operators of an online or cloud service is typically the personal data controller of personal data processed in the service.

Personal data processor (Art 4 (8) GDPR)**:** Someone (natural or legal person, e.g. a company) who processes personal data on behalf of a personal data controller, without determining the means and purposes of the processing of personal data. The provider of an online or cloud service is typically the personal data processor of personal data processed in the service.

User: A system integrator or an end customer using the Swarm Analytics Applications. This term does not appear in the GDPR. It is understood that the user has the decision authority which and how data is generated, stored, processed and fed into other data processing systems.

User content: Any information or data captured by and processed in Swarm Analytics Applications. This term does not appear in the GDPR.

Video Stream: Video data which is sent by the camera to other network devices, e.g. into a Swarm Perception Box and/or to a storage or monitoring device. The most popular protocol used is RTSP.

2 Introduction

2.1 Importance of the lawfulness of processing of personal data

The protection of the processing of personal data is of great importance across the European Union. The GDPR is a part of the EU-law and sets the conditions under which the processing of personal data is legally compliant and what protective measures should be taken in this context. Any unlawful processing of personal data can result in severe fines. That is why the lawfulness of processing of personal data is so important.

In addition to the GDPR, there are also numerous national laws that regulate the processing of personal data. In Austria, for example, it is the Data Protection Act (Datenschutzgesetz - DSG). This must be kept in mind while processing personal data.

2.2 About Swarm Analytics

Swarm Analytics GmbH (short: Swarm Analytics) develops revolutionary AI technology for transforming cameras into **smart sensors**. This leads to smarter, faster, easier, and trustworthy solutions while increasing affordability. Based on Swarm Analytics sensor technology, the solution partners deliver a broad range of end-to-end smart city solutions for traffic, parking, public transport, and retail.

Swarm Analytics cooperates with system integrators from all over the world. These integrators meet the end customers, sell them Swarm Analytics' products and/or handle the design, integration, installation and service of Swarm Analytics' products. Normally the system integrator sells, installs, configures and calibrates as well services and maintains the system to/for the end customer. Therefore, concerning the Swarm Analytics Applications there is usually no direct legal relationship between the Swarm Analytics and the end customer.

2.3 About Swarm Perception Platform (Swarm Analytics Applications)

The Swarm Perception Platform consists of the Swarm Control Center and the Swarm Perception Boxes. Together they are also often referred to as Swarm Analytics Applications. With the Swarm Control Center the Swarm Perception Boxes are configured and managed, whereas they receive the stream of an IP camera and immediately extracts the information which is looked for. This can be classification of vehicles, counting of people crossing a certain counting line or duration of stay of people and vehicles in certain regions of interest. This information is used to get more insights into the need of traffic planning efforts as well as optimization of retail environments like shopping centers and high street areas. Remember: Monitoring people with video devices generating an accessible stream (at least in principle) always means processing personal data!

2.4 Purposes of this document

The purpose of this document is to describe how the user content is processed in Swarm Analytics Applications and to facilitate your GDPR compliance work in the best possible way, whether you are a system integrator or an end customer.

It is not the purpose of this document to provide legal advice on data protection issues in individual cases or to replace them.

3 Swarm Perception Platform and how it works

The Swarm Perception Platform consists of a **Swarm Perception Box** and a **Swarm Control** Center (SCC).

The **Swarm Perception Box** is either deployed in a dedicated hardware delivered by Swarm Analytics (P100, OP100, P101, OP101) or in a virtual docker container (VPX, SPS, SDS) deployed on a host system provided by the user.

Either way the video stream of the respective IP camera is directed into the Swarm Perception Box and it analyzes the content according to its configuration (object detection and object classification).

This configuration is done with the **Swarm Control Center**, which administers all Swarm Perception Boxes of a certain realm. It determines the analyzing model and details like entry/exit lines, origins and destination directions.

The Swarm Control Center runs in an IoT Hub on MS Azure, which is **controlled by the data processor**, i.e. the end customer or a system integrator/service provider, who does it on the end customers' behalf.

Each use-case consists of multiple neural networks, which are responsible for extracting features from the given video-stream and combine the output with case-specific post-processing (e.g. Traffic Monitoring).

The extracted data (numeric information output) is transmitted from the Swarm Perception Box to a database selected by the user.

These are typical examples of perception configurations, which can be configured by the user for the respective Swarm Perception Box through the Swarm Control Center:

	Traffic Insights	People Insights	Parking Monitoring
Object Detection	• Vehicle • Rider • Person	• Person • Head • Face	• Vehicle • Rider • License Plate
Object Classification	• Car • Van • Motorcycle • Bicycle • Truck • Truck+Trailer • Bus • Others	• Female • Male • Age	• Car • Van • Motorcycle • Bicycle • Truck • Truck+Trailer • Bus • Others • License Plate Number Recognition
Object Re-Recognition	• Yes	• Yes	• N/A
Event Trigger	• Origin Destination • Counting Lines • Heatmap	• Virtual Door • Region of Interest • Heatmap	• Single-Space Zone • Multi-Space Zone • Entry/Exit Counting
Meta Information	• Speed Estimation • Dwell Time	• Dwell Time	• Dwell Time • Parking Time Violation • Image of violation includes with timestamp generated by software

Potential and actual GDPR sensitive configurations:

Person, head, face, gender, age

In general, characteristic features of a person such as gender, age, face etc. represent personal data within the meaning of the GDPR.

The Swarm Perception Box can recognize in the VIDEO stream whether it is a person, a human head or a human face without using biometric data. Instead, the Swarm Perception Box uses the templates created in the algorithm and compares them to the general appearance of the persons, so the user is not able to extract or trace individuals. For example, it is not possible to recognize a certain person who comes back to the retail space the next day. The Swarm Perception Box does not create any new templates from the VIDEO stream itself. Hence the numeric output of the Swarm Perception Box itself is regarded as anonymized data.

If people are monitored with the IP camera and this data stream is forwarded to the Swarm Perception Box for evaluation, this in any case represents processing of personal data within the meaning of the GDPR.

In such cases, if the user operates the IP camera and the Swarm Perception Box, he is also the personal data controller within the meaning of the GDPR.

License plate recognition

For parking management cases the Swarm Perception Box can extract license plate information.

A license plate number is personal data within the meaning of the GDPR. Therefore, the license plate recognition always constitutes a proceeding of personal data and requires a legal basis (Art 6 GDPR).

For recognition of individual license plates to automate and accelerate the service for whitelisted vehicles it is necessary to receive consent of all users and to make sure that the data is not used for anything else than the necessary services.

Statistical data of vehicle origin is not regarded as personal data and can hence be collected and processed without violating privacy regulations. However, recording and evaluating a license plate number to obtain statistical data is processing personal data, which requires a legal basis (Art 6 GDPR).

4 What type of data is collected and stored by Swarm Perception Platform?

The VIDEO stream directed into the Swarm Perception Box contains usually personal data (appearance/license plate number etc.) of people monitored by the IP camera. That means analyzing this content (object detection and object classification) in the Swarm Perception Box is usually processing personal data. Therefore, the information captured (i.e. user content) and processed in the Swarm Perception Platform is generally personal data.

The user who operates the video surveillance system and the Swarm Perception Box normally is responsible for this data processing (data processor).

The only data stored by Swarm Perception Platform is **numeric information output**, such as the number of people entering and exiting a store/location during a period of time, their age or gender. The Swarm Perception Platform does not store footage or video. Nor is it possible to record the video-streams through Swarm Perception Platform:

```
{
  "version":"1.0",
  "eventSchema": "https://swarm-analytics.com/schema/event/peopleinsights/1.0",
  "node":{
    "id":"b8ade223-e847-4741-a405-7f62c0403aa2",
    "name":"test"
  },
  "capacityMonitoringEvent":{
    "zoneEvent": {
      "objects": [
       {
         "class": "person"
       }
      ],
      "zoneId": "69031920-6239-471e-a3d7-f241b7753fd0",
      "zoneName": "zone1",
      "state": "occupied",
      "timestamp": "2020-01-02T14:59:27.85136Z",
      "triggerType": "time"
    }
  }
}
```

Example of numeric information from Swarm Analytics People Counter in JSON-format.

To answer the question of whether the numeric information output contains pseudonymized data (which is subject to the GDPR) or anonymous resp. anonymized data (which is not subject to the GDPR), it is relevant whether the personal reference to the numeric information output can be restored with legally permissible, reasonably applicable means or not.

If the user connects the Swarm Perception Platform with another application or with hardware or software in a way that is suitable for identifying people or making them identifiable (e.g. with a video surveillance system), then the numeric information output could represent personal (pseudonymized) data within the meaning of GDPR.

If the user does not connect the Swarm Perception Platform with another applications or with hardware or software in a way that is suitable for identifying people or making them identifiable, then the numeric information output could represent anonymized data, which is not subject to the GDPR.

The numeric information output could also be an anonymized data, if the user takes technical and legal measures so there is no legally permissible possibility to link the data with other characteristics (e.g. with a stored VIDEO stream or data from other personalized access control systems) and thereby identify certain persons. Such measures could be e.g. an encryption or the storage of data in two different databases without the responsible departments of the user being able to link this data with one another.

5 GDPR roles and responsibilities

The person who in most cases is responsible for the GDPR compliance of the Swarm Perception Platform to process personal data is the user (typically the end customer) as a personal data controller. Swarm Analytics has no responsibility under the GDPR for such use of the Swarm Perception Platform.

In such cases, the user has an obligation to implement technical and/or organizational measures designed to implement the data protection principles set out in the GDPR (privacy by design). For the Swarm Perception Platform, examples of such measures would be restrictive access to admin interfaces and avoidance of combining the numeric information output with other data sources to identify persons or make them identifiable.

The user as a personal data controller also has an obligation to implement technical or organizational measures, which by default ensure the least privacy intrusive processing of the personal data in question (privacy by default). In the context of Swarm Analytics Applications examples of such measures would be avoiding video streaming to any other destination than the Swarm Perception Box, which anonymizes and deletes it immediately.

The GDPR does not obligate developers/ manufacturers to build in privacy by design and privacy by default. For example, for purposes of technical support and configuration it is necessary that in principle the admin has access to the picture of the respective camera.

5.1 Swarm Analytics' GDPR commitment for the Swarm Perception Platform

As mentioned above, the user of the Swarm Perception Platform is usually responsible for ensuring GDPR compliance. Nonetheless, Swarm Analytics would like to support users in achieving GDPR compliance as much as possible. That is also the primary purpose of this document. All functionalities in the Swarm Perception Platform aim to facilitate your GDPR compliance, and your compliance with the privacy by design and privacy by default provisions of the GDPR.

Pseudonymization vs. Anonymization

As already described above, the video surveillance of people is generally a processing of personal data (appearance of human beings). This video surveillance takes place in the IP camera so that the VIDEO stream that is sent to the Swarm Perception Box contains personal data. The analysis of the VIDEO stream in the Swarm Perception Box represents the processing of personal data. The result of this analysis is the numeric information output, which can be either pseudonymized or an anonymized data.

The distinction between pseudonymized and anonymized data is important because anonymized data is not subject to the GDPR. Pseudonymized data, on the other hand, are subject to the GDPR, so that there must be a legal basis for their processing.

Similar to the processing of personal data in the course of video surveillance, it is the responsibility of the user to pseudonymize or anonymize the data contained in the numeric information output.

If the user takes technical and legal measures so that the data contained in the numeric information output cannot be associated with any other data (such as the stored video stream or similar), the data contained in the numeric information output can be anonymized data.

Most of the applications can be configured so that persons can no longer be identified from the live view of the camera. The anonymization works as follows: All video streams and images from the camera are blocked. The debug view still shows a blurred image which means it is possible to see what is going on but you cannot identify people from the video stream.

As a software manufacturer, Swarm Analytics takes cyber security seriously and provides means to make products and applications more resilient and secure - for example by authentication, authorization, and password enforcement. This is not specific to the Swarm Analytics Applications, but an inherent part of our product development strategy, which is committed to make computer vision faster, easier, smarter, more affordable, and more trustworthy.

5.2 Specifically about user's GDPR responsibility in relation to the Swarm Perception Platform

Please remember to check what exact legal obligations may apply to you or your company when you use Swarm Analytics Applications. In this respect, Swarm Analytics has no legal responsibility (see the legal disclaimer below the table of contents).

As mentioned above, using video surveillance and analyzing the video stream in the Swarm Perception Platform constitutes processing of personal data. In such cases, you (your company) as the user of these applications are a personal data controller under the GDPR. The GDPR imposes a number of requirements on personal data controllers. You should take the following steps into account when establishing GDPR compliance:

a. Please check whether the intended purpose of the data processing (e.g. property protection with video surveillance) cannot be achieved by more lenient means (e.g. use of security personnel etc.).
b. Please specify the purposes for using the video surveillance/Swarm Analytics Applications for processing of personal data (e.g. advertising, property protection, parking management etc.) and save this documentation in a written form for evidence purposes.
c. Inform (e.g. by an information sign) the data subjects (persons whose personal data you process) about the data processing and its purposes. The information shall cover, among other things, what types of personal data that you collect and for what purposes you will use the data.
d. Never use personal data for any other purpose than the purpose(s) you informed about.
e. Please make sure that you have legal ground, as provided for in the Art 6 GDPR, for processing personal data e.g. a consent of data subjects, legitimate interests, or performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
f. Implement and maintain efficient management capabilities of personal data to be able to comply with requests from data subjects concerning their personal data that you hold.
g. Undertake safety measures for any personal data that you process (e.g. regulated access controls, encryption, storage in various databases, etc.).
h. If you work with a data processor, do not forget to arrange a contract with the processor (Art 28 GDPR).
i. Do not forget to delete personal data as soon as their processing is no longer necessary for the purpose. The storage period should be as short as possible and ideally not exceed 72 hours.
j. Remember to pseudonymize or anonymize the data contained in the numeric information output by undertaking technical and legal measures (see above).
k. Systematic monitoring of a publicly accessible area on a large scale requires a data protection impact assessment. However, data protection authorities of the EU member states may make exceptions to this. In Austria, for example, the video surveillance of business premises with customer traffic or of parking areas in shopping centers is excluded

from the data protection impact assessment under certain conditions.[1] Image and acoustic transmissions without recording (in real-time) are also excluded from the data protection impact assessment under certain conditions.[2]

6 Deployment Types

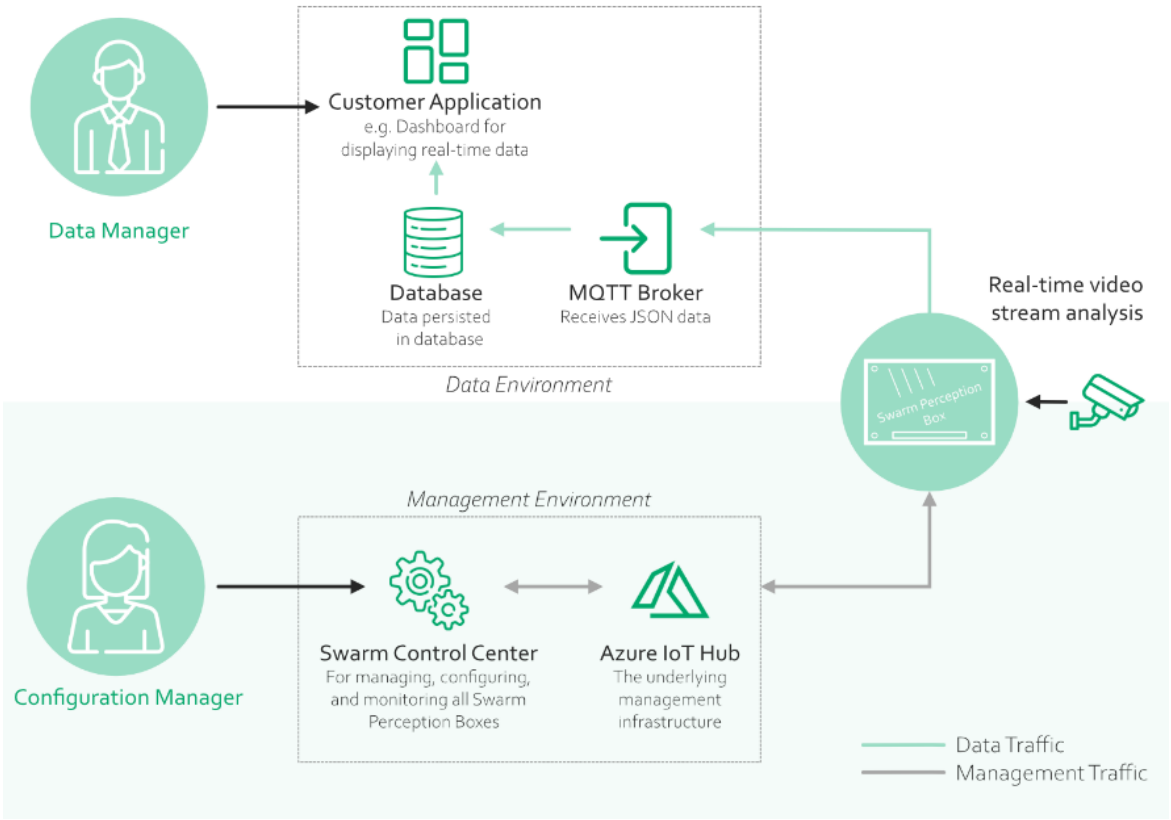
We distinguish between 3 different deployment types, the 2 defining parameters being whether the camera stream is multiply used for different purposes (e.g. security surveillance) and whether the camera stream is directed into the Swarm Perception Box at the location of each camera or transferred to a more centralized place in the network.

	Decentral analysis	Centralized analysis
Dedicated camera	The Swarm Perception Box is directly attached to the camera, extracts anonymized information in real time and no stream is forwarded to any other location.	The Swarm Perception Box and the camera are in different locations and anonymized information is extracted in real time. The video stream is forwarded through an IP network to that other location, but not stored, monitored or captured in any way.
Multi-purpose camera (existing DVR/CCTV system)	The video streams are forwarded to a monitoring and/or storage system. Additionally, the stream is analyzed, and anonymized data is extracted by a Swarm Perception Box.	

For all deployments, the general management setup is handled the same way, which means the following drawing is applicable for all scenarios.

[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)



6.1 Swarm Perception Platform as decentral, dedicated-camera deployment

How it works

The network camera within a local area network and connect to (IP need to be reachable through network) a Swarm Perception Box, so the video-stream can be directly connected and no other device can interact with it - this can either done through a PoE switch or directly to the PoE Interface of the Swarm Perception Box.

This is mostly the case, when the sole purpose of the systems is to be a sensor. In this use case, all activities take place in the local area network of the end customer, and the camera acts as a visual sensor without the possibility of storing any video content for CCTV reasons.

6.2 Swarm Perception Platform as centralized, dedicated-camera deployment

How it works

For larger scale deployments, the Swarm Perception Box can be deployed on a host system (e.g. a server), which is within the range of the network cameras in order to connect directly via VIDEO without a CCTV/DVR as streaming source. This enables the usage of large scale camera deployments with the sole purpose of gathering textual information, rather than bringing in video recording features & aspects.

This setup will require a secured IP network (f.e. by a firewall) in which the server is deployed to and can connect to all needed cameras. The camera streams will then be processed , without being stored or available to other services, on the dedicated system. It is to ensure to secure the hostsystem and the network path against any non-approved access by standard security measurements (user accounts, firewall, etc.).

6.3 Swarm Perception Platform as extension to existing to CCTV/DVR deployments

How it works

In a deployment environment where a CCTV system is already in place, the Swarm Analytics application is being deployed side by side to the existing infrastructure and either connects to the server through the Management Network of the CCTV system or directly to each camera via IP if the network is reachable. In such a deployment scenario the video-stream is being recorded by the CCTV system and therefore the camera is not a single purpose visual sensor, but rather a multi-purpose device used to provide video data as well as extracted anonymized information.

6.4 GDPR aspects of using the Swarm Perception Platform in any deployment scenario

The video surveillance with the camera and the analysis of the stream in the Swarm Perception Platform represent processing of personal data.

The user (personal data controller) should undertake technical and legal measures to ensure that there is no other possibility to connect the numeric information output with the data from the video content. In such case, the numeric information output could be anonymized data, which is not subject to the GDPR.

Swarm Analytics will not access your user content i.e., the information captured by and processed in the Swarm Perception Platform, unless you provide such access (in the default deployment, no such access is possible to gain without the consent of the Azure Account owner).

If the Swarm Perception Boxes are installed in a local network and not connected to a designated data end-point (either by the customer itself or a system-integrator), then Swarm Analytics is not a personal data processor in relation to any personal data captured by Swarm Perception Platform. Swarm Analytics only supplies these applications – without any further involvement in the use and/or processing of personal data through the application.

Depending on the setup of the Swarm Perception Platform, the roles of data processor and data controller can be transferred from the end customer to the system integrator and vice versa. We recommend that you investigate how the GDPR responsibility will be allocated under your specific setup. In addition if you choose to connect the Swarm Analytics Applications to any other service provider (i.e., third party visualization tool, Business Intelligence tools, etc.), we recommend that you investigate how the GDPR responsibility will be allocated under that specific service set up.

7 Use case examples → possible GDPR aspects

General notes: If you are a data processor and process personal data for the purposes of the legitimate interests (Art 6 (1) (f) GDPR) you must assure, that those legitimate interests are not overridden by the interests or fundamental rights and freedoms of the data subject (weighing of interests). It is not sufficient to refer to abstract situations or to compare them with similar cases. Therefore, the following use cases have only a demonstrative character and do not replace the compulsory weighing of interests in individual cases.

Caveat: Public authorities cannot process personal data for the purposes of the legitimate interests (Art 6 (1) (f) GDPR) in the performance of their tasks.

Typical traffic counting by a private traffic planning office

Recording of image data resp. of license plates in the course of a traffic counting by a private traffic planning office constitutes a processing of personal data, which must be compliant with the GDPR.

The legal ground for such data processing could be legitimate interests by the controller or by a third party or performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

According to the principle of data minimization, the monitoring should affect as little as possible or necessary personal data of road users. The person responsible should take legal and technical measures so that the video surveillance e.g. does not include people in the vehicle and the license plates are only recorded if this is absolutely necessary.

The data controller should take legal and technical measures, that the numeric information output is not be able to be related to other data (e.g. video files). If these requirements are met, the numeric information output can represent anonymized data that is not subject to the GDPR.

Note: That doesn't change the fact that the video surveillance itself is processing of personal data and requires a legal basis.

Typical traffic counting by a road inspectorate authority

Road inspection authorities also have the task of taking measures to regulate and secure traffic if necessary. Such measures can consist in particular in the arrangement of the regulation of traffic by means of light signals. In order to clarify the necessity of such measures, corresponding empirical traffic data is sometimes required, for example from traffic counts. Regardless of who implements a camera-based automatic traffic count, so to speak, "technically", this falls under the legal responsibility of the relevant local road inspectorate authority.

As mentioned above, recording of image data resp. of license plates in the course of a traffic counting by a road inspectorate authority constitutes a processing of personal data, which must be compliant with the GDPR.

The legal ground for such data processing could be performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Such a "task" must exist by law or other legal basis in the respective state. Example of this would be § 98f Austrian Road Traffic Act (Straßenverkehrsordnung), according to which road authorities are allowed to carry out video surveillance of the traffic in certain cases, such like ensuring the ease, fluidity and safety of traffic.

Also in these cases, the data controller should take legal and technical measures, that the numeric information output is not be able to be related to other data (e.g. video files). If these requirements are met, the numeric information output can represent anonymized data that is not subject to the GDPR.

Video control of the public space by a public authority

As mentioned above, video surveillance in any case represents processing of personal data that requires a legal basis. Public authorities cannot process personal data for the purposes of the legitimate interests (Art 6 (1) (f) GDPR) in the performance of their tasks.

However, the GDPR allows authorities to process personal data as part of their sovereign tasks (Art 6 (1) (e) GDPR), but the legal basis for such tasks, as shown above, results from the national legal situation. Such "tasks" must exist by law or other legal basis in the respective state (see use case above).

For example, the security authorities in Austria are authorized by the Security Police Act (Sicherheitspolizeigesetz)[3] to monitor public places (e.g. parks, squares, etc.) in order to prevent dangerous attacks against the life, health or property of people. The criminal police and the public prosecutor's office are authorized to visually monitor people under certain conditions.[4]

If the authority is obliged to video surveillance based on national legal provisions, this obligation can serve as the legal basis in accordance with Art 6 (1) (c) GDPR.

The GDPR is therefore linked to this national legal basis, but does not state its own legal basis for video surveillance by the public sector. If there is no national legal basis for video surveillance, the authority is not entitled to do this.

If there is a legal basis for the processing of personal data (video surveillance) and for the analysis of the video stream in the Swarm Perception Boxes, the data controller must ensure that the numeric information output is anonymized accordingly so that it is not subject to the GDPR. Anonymization can be done by legal and technical measures so that the video stream and the numeric information output are stored or kept separately from one another and no comparison can take place between them. Ideally the video stream is not stored at all.

Video control of the public transportation

If the organization and operation of public transport is a matter of sovereign administration under national law, the same conditions apply to the processing of personal data as to video surveillance of public spaces (see above).

In some countries, public transport is organized and operated within the framework of private sector administration. In these cases, the authority does not act sovereign, but like a private person. This is how it is in Austria, for example.

In these cases, the legal basis for video surveillance and the processing of personal data could be in the legitimate interest pursued by the controller (Art 6 Paragraph 1 lit f GDPR). The balance of interests should be drawn up and kept in writing for documentation and evidence purposes.

If there is a legal basis for the processing of personal data (video surveillance) and for the analysis of the video stream in the Swarm Perception Boxes, the data controller must ensure that the numeric information output is anonymized accordingly so that it is not subject to the GDPR. Anonymization can be done by legal and technical measures so that the video stream and the numeric information output are stored or kept separately from one another and no comparison can take place between them.

Typical Retail Situation (e.g. shopping center):

The video surveillance of customers in the entrance area to the shop with a video surveillance system represents processing of personal data in any case. Customers must be informed about

[3] § 54 Abs 6 Austrian Security Police Act (Sicherheitspolizeigesetz)

[4] § 136 Austrian Code of Criminal Procedure (Strafprozessordnung)

the surveillance as well as about data processing and its purposes (e.g. by an information sign at the entrance to the shop). In such cases, the shop operator is most likely a data processor according to the GDPR.

The legal reason for the data processing is also important. In the vast majority of cases, this will be the safeguarding of the legitimate interests of the shop operator (Art 6 (1) f GDPR). This legal ground requires a weighing of interests in each individual case. The reasons for the outweighing the interests of the operator over the interests of the customers concerned should be written down.

Physical characteristics of people such as gender or age represent personal data in any case, because they are suitable for making a person identifiable. Theoretically, it could also be particularly sensitive (biometric) data within the meaning of Art 9 GDPR.

The solution to this question depends, among other things, on the purpose of the data processing:

If the purpose of video surveillance is not to identify a specific person on the basis of this data, but only to distinguish one category of person from another (like in the example above), then it does not constitute sensitive data.

If a data processer would like to identify a certain individual (a customer) e.g. as a regular customer or member for customized advertising, the purpose of the processing would be to uniquely identify a natural person. In this case, the shop operator would have to obtain the express consent of all data subjects before using his system (Art 9 (2) GDPR). The shop operator would also have to ensure (e.g. through two separate entrances, etc.) that the system does not record any persons who have not given their consent

Regardless of whether it is conventional personal data or sensitive data (Art 9 GDPR), the video surveillance system in a shopping center should be set up in such a way that it can only encompass the customers and not just people passing by.

To classify the numeric information output as pseudonymized data (which is subject to the GDPR) or as anonymous data (which is not subject to the GDPR), it is important that the user takes legal and technical measures to prevent numeric information output from other data sources is assigned (especially to the video stream). The user must therefore ensure that the numeric information output does not allow people to be identified.

If numeric information output has been anonymized, it can be used and processed as required from the point of view of the GDPR, because this is not personal data within the meaning of the GDPR.

Typical Parking Management Situation

Example 1: Managed parking area with individualized access with license plate recognition

Systems for recording license plates in order to be able to identify vehicles authorized to enter or exit may be permissible on the basis of legitimate interests (Art 6 (1) f GDPR).

It is important that the operator takes technical and organizational measures to exclude negative consequences for affected data subjects. These can e.g. consist in the fact that only the lower areas

of vehicles are recorded (and not the windshield) or the video recordings are either not saved at all or only for a short period (e.g. one day).

The operator should take legal and technical measures so that the video stream and the numeric information output are stored or kept separately from one another and no comparison can take place between them.

As soon as the numeric information output cannot be linked to other data (e.g. because the video stream no longer exists), it can be anonymized data that is not subject to the GDPR.

Under certain conditions, video surveillance can be exempted from the obligation to carry out the data protection impact assessment, e.g. if the video surveillance takes place in real time (without recording) and only the company property is recorded. The EU member states determine the exceptions autonomously.

Example 2: Unmanaged parking areas: capacity measurements, length of stay, etc.

Video surveillance of unmanaged parking areas (with free access) to determine the occupancy of the parking areas (capacity measurements) or the parking duration could also be permissible on the basis of legitimate interests (Art 6 (1) f GDPR).

Also in such cases it is important that the operator takes technical and organizational measures to exclude negative consequences for affected data subjects. These can e.g. consist in the fact that only the lower areas of vehicles are recorded (and not the windshield) or the video recordings are either not saved at all or only for a short period (e.g. one day).

As soon as the numeric information output cannot be linked to other data (e.g. because the video stream no longer exists), it can be anonymized data that is not subject to the GDPR.

Under certain conditions, video surveillance can be exempted from the obligation to carry out the data protection impact assessment, e.g. if the video surveillance takes place in real time (without recording) and only the company property is recorded. The EU member states determine the exceptions autonomously.

Example 3: Areas for potential short-term parking zones (Video surveillance by the city administration)

As mentioned above, authorities may not base the processing of personal data on legitimate interests. Rather, the legal reason for data processing generally arises from a legal obligation (Art 6 (1) c GDPR) or a legal permission (Art 6 (1) e GDPR) for data processing. In both cases, the corresponding national legal basis must exist, which stipulates the official rights and obligations with regard to data processing.

In Austria, for example, § 98f Austrian Road Traffic Act (Straßenverkehrsordnung) provides the road traffic authorities with the power to carry out video surveillance of the traffic in certain cases, such as ensuring the ease, fluidity and safety of traffic or for the fulfillment of the tasks legally incumbent on the authorities and road maintenance authorities.

According to § 25 Austrian Road Traffic Act (Straßenverkehrsordnung), road authorities are entitled to set up short-term parking zones by ordinance if and to the extent that it is necessary at certain times for location-related reasons (also in the interest of the resident population) or to ease the traffic situation.

It is therefore conceivable that road authorities will use video surveillance to research potential short-term parking zones with reference to these legal bases.

To ensure that numeric information output is anonymized data, legal and technical measures should be taken (see above).

It is also important that video surveillance, in accordance with the principle of data minimization, interferes with the rights of those affected as little as possible (no vehicle occupants can be recognized, etc.).