GDPR Aspects of the Camlytics Software

Non-binding GDPR guidelines for system integrators and end customers

Contents

DISCLAIMER

Spearr LLC created this document to the best of its knowledge and belief, without claiming to be exhaustive and without any obligation, solely for general information purposes. The content of this document and the document itself are not legally binding. The information contained in this document cannot replace specific legal advice in individual cases. Spearr LLC assumes no liability for the accuracy of the information contained in this document.

The use of this document is at the user's own risk. Any liability on the part of Spearr LLC for damage associated with the use of this document is excluded to the extent permitted by law.

This document is not intended to, and shall not, create any legal obligation for Spearr LLC and/or any of its affiliates. Spearr LLC's and/or any of its affiliates' obligations in relation to any Camlytics products are subject exclusively to terms and conditions of the agreement between Spearr LLC and the entity that purchased such products directly from Spearr LLC.

All rights to the document or any intellectual property rights relating thereto (including but not limited to trademarks, trade names, logotypes, and similar marks therein) are protected by law and all rights, title, and/or interest in and to the document or any intellectual property rights related thereto are and shall remain vested in Spearr LLC.

1 Executive Summary

The Camlytics Software is designed to provide anonymized data for a variety of use cases. In its most used standard deployment, the data output is anonymized data and hence not subject to GDPR regulations for further handling.

However, there are major points to consider in order to remain GDPR-compliant:

1. The mere fact that a video stream exists constitutes processing of personal data in almost all use cases. Therefore, careful consideration must be given to ensure that personal data is not stored, accessed, or otherwise processed as originally intended.

This document highlights many edge cases, including hypothetical deployments and configurations, to ensure that the Camlytics Software is not used in unintended ways.

2 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 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 Camlytics Software. 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 the Camlytics Software. This term does not appear in the GDPR**.**

Video stream: Video data which is sent by a camera to other network devices, e.g. into a PC with Camlytics Software and/or to a storage or monitoring device. The most popular protocol used is RTSP.

3 Introduction

3.1 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.

3.2 About Camlytics

Spearr LLC (short or doing-business-as: Camlytics) develops revolutionary AI technology for transforming cameras into **smart analytics devices**. This leads to smarter, faster, easier, and trustworthy solutions while increasing affordability. Based on Camlytics sensor technology, the solution partners deliver a broad range of end-to-end smart city solutions for any kind of people or vehicle traffic and movement (e.g. retail, parking, public transport, tourism, traffic safety).

Camlytics cooperates with system integrators from all over the world. These integrators meet the end customers, sell them Camlytics' products and/or handle the design, integration, installation and service of Camlytics' 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 Camlytics Software, there is usually no direct legal relationship between Camlytics and the end customer.

3.3 About Camlytics Software

The Camlytics Software consists of the desktop PC software that runs on customer's machines and a cloud portal that receives anonymized video analytics events data. Together, they are also often referred to as Camlytics applications. The Camlytics Sofware is used to configure and manage the scene, receiving the stream from an IP camera and immediately extracting the information sought. 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 provide more insight into the need of traffic planning efforts, as well as optimization of retail environments like shopping centers and high street areas. Important notice: Monitoring people with video devices generating an accessible stream (at least in principle) always means processing personal data.

3.4 Purposes of this document

The purpose of this document is to describe how user content is processed in the Camlytics Software and to best facilitate your work to comply with the GDPR, 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, nor to replace such advice.

4 Camlytics Software and how it works

The Camlytics Software consists of a Camlytics Software for desktop PC and cloud portal.

The **desktop software** is deployed in a dedicated PC delivered by end customer. The video stream of the respective IP camera is analyzed by the content according to its configuration (object detection and object classification).

Each use case consists of multiple neural networks responsible for extracting features from the given video stream and combining the output with case-specific post-processing (e.g. Traffic Monitoring). The extracted data (events, or numeric information output) is transmitted from the Camlytics Software desktop PC to a cloud server hosted by Camlytics.

These are typical examples of configurations that can be configured by the user for the particular Camlytics Software setup.

Video Analytics Detection, classification and tracking of objects across the camera frame	**Event Analytics** Configuration of event types and triggers in order to generate event based data for given use cases
Object detection and **classification** in **10+1** standardized traffic **classes** (incl. pedestrian and bicycle)	**Event types:** • **Counting Lines** Provides an event if object crosses the configured line • **Origin-Destination Zones** Provides an event with origin and destination area of an object based on object tracking • **Region of Interest (RoI)** Provides the count of objects in a specified region with different trigger options Option to have dedicated Parking RoI for Single & Multispace parking capacities. • **Virtual door** Provides an event if object appears in the door and leaves outside of the door • **Raw tracks** Provides the pixel coordinates of the track where the object moved along the camera frame or the other way around.
Dedicated model for **person detection** in order to have person countings in tourism areas.	
Object tracking Tracks the object across the camera frame	**Speed estimation** Each counting line supports a speed estimate. Output km/h as parameter within the created Counting Line events.

	Custom Rules Customization of the event triggers. Reducing big data to relevant data with just a few clicks: From simple adjustments to only count bicycles on a given Counting Line to more complex rules to monitor pedestrian crossings by combining Region of Interest status with counting line crossings.

5 What types of data are collected and stored by Camlytics Software

The video stream directed into the Camlytics Software usually contains personal data (appearance/vehicles, etc.) of the persons monitored by the IP camera. This means that the analysis of this content (object detection and object classification) in the Camlytics Software usually processes personal data. Therefore, the information captured (i.e. user content) and processed in the Camlytics Software is generally personal data.

The responsible party for such data processing is generally the user operating the video surveillance system and Camlytics Software (data processor).

The only data stored by Camlytics Software is the **numeric information output**, such as the number of persons entering and exiting a store/location in a certain period of time.

The Camlytics Software does not store footage or video on it's servers. It is possible to record video streams through the Camlytics Software, but the access to the recordings is only possible by the end user (all recordings are stored locally on the user's machine).

Potential and actual GDPR sensitive configurations:

Age/gender recognition

The Camlytics Softare can extract age and gender information. This is typically used for ads marketing targeting purposes.

The age and gender is personal data within the meaning of the GDPR. However, it is stored without attaching it to a particular person and therefore can be collected and processed without violating data protection regulations.

Other Data

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

If the user connects the Camlytics Software to another application or to hardware or software in a way that is likely to identify or make identifiable individuals (e.g. with a video surveillance system), then the numeric information output could constitute personal (pseudonymized) data within the meaning of GDPR.

"If the user does not connect the Camlytics Software to other applications or hardware or software in a way that is likely to identify or make identifiable individuals, then the numeric information output could constitute anonymized data that is not covered by the GDPR."

The numeric information output could also be anonymized data if the user takes technical and legal measures such that there is no legally permissible possibility to link the data to other characteristics (e.g. to a stored video stream or data from other personalized access control systems) and thereby identify specific individuals. Such measures could be, for example, encryption or the storage of data in two different databases without the user's responsible departments being able to link these data.

6 Deployment Types

We distinguish between three different deployment types, with the two defining parameters being whether the camera stream is used multiple times for different purposes (e.g. security surveillance) and whether the camera stream is directed to the Camlytics Software PC at each camera's location or transferred to a centralized location in the network.

	Decentral analysis	Centralized analysis
Dedicated camera	The Camlytics Software machine is directly attached to the camera, extracts anonymized information in real time and no stream is forwarded to any other location.	The Camlytics Software 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 (except for the local recording if enabled).
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 Camlytics Software.	

6.1 Camlytics Software as decentral, dedicated-camera deployment

How it works

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

This is mostly the case when the sole purpose of the systems is to act as a sensor. In this use case, all activity takes place in the local area network of the end customer, and the camera acts as a visual sensor without the ability to store video content for video surveillance reasons (except for local recording, if initiated by user).

6.2 Camlytics Software as centralized, dedicated-camera deployment

How it works

For larger deployments, the Camlytics Software can be installed in an existing network or on a host system (such as a server) that is within range of the network cameras to connect directly via video without a CCTV/DVR as a streaming source. This allows the use of large scale camera deployments with the sole purpose of gathering textual information rather than bringing in video recording features and aspects.

This setup requires a secured IP network (i.e. through a firewall) where the server or Camlytics Software is installed 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 (except for local recording, if initiated by user). It is to ensure to secure the host system and the network path against any non-approved access by standard security measurements (user accounts, firewall, etc.).

6.3 GDPR aspects of using the Camlytics Software in any deployment scenario

Video surveillance with the camera and analysis of the stream in the Camlytics Software constitute processing of personal data.

The user (personal data controller) should take 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 this case, the numeric information output could be anonymized data, which is not subject to the GDPR.

If the Camlytics Software is installed in a local network and not connected to a designated data endpoint (either by the customer itself or a system integrator), Camlytics is not a personal data processor in relation to any personal data collected by Camlytics. Camlytics merely provides these applications – with no further involvement in the use and/or processing of personal data by the application.

Depending on the setup of the Camlytics Software, the roles of data processor and data controller may be transferred from the end customer to the system integrator and vice versa. We recommend that you investigate how GDPR responsibilities are assigned in your specific setup. If you choose to connect the Camlytics Software to any other service providers (i.e., third party visualization tool, Business Intelligence tools, etc.), we recommend that you investigate how the GDPR responsibility is assigned within that specific service setup.

7 Possible GDPR aspects: Use case examples

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.

Various areas of utilization are described below, taking data protection regulations into account.

Typical traffic counting by a private traffic planning office

The recording of image data as part of a traffic counting by a private traffic planning office constitutes a processing of personal data that must be compliant with the GDPR.

The legal basis for such data processing could be legitimate interests of the controller or a third party or the 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, monitoring should involve as little personal data of road users as possible or necessary.

The data controller should take legal and technical measures to ensure that the numeric information output cannot be associated with 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 video surveillance itself constitutes a processing of personal data and requires a legal basis.

Typical retail situation (e.g. shopping center):

The video surveillance of customers in the entrance area to the shop with a video surveillance system constitutes processing of personal data in any case. Customers must be informed about 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 store 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 to protect 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 why the interests of the operator outweigh the interests of the customers concerned should be recorded in writing.

Physical characteristics of people, such as gender or age, represent personal data in any case because they are capable of making a person identifiable. Theoretically, it could also be particularly sensitive (biometric) data within the meaning of Art 9 GDPR. [3]

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 individuals from another (as in the example above), then it is not sensitive data.

If a data processor wants to identify a certain individual (a customer) e.g. as a regular customer or member for tailored advertising, the purpose of the processing would be to uniquely identify a natural person. In this case, the shop operator would need to obtain the explicit consent of all data subjects before using the 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 individuals who have not consented.

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 to capture only the customers and not the passers-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 the attribution of numeric information output from other data sources (especially to the video stream). The user must therefore ensure that the numeric information output does not allow identification of individuals.

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

Typical Parking Management Situation

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. Traditionally this was done by strictly focussing the camera on the lower areas of vehicles (and not the windshield) and storing the video recordings only for a short period of time (e.g. one day). An even better approach is not storing the video recordings at all.

As soon as the numeric information output cannot be associated with license plates or other data (e.g., because the video stream no longer exists), it may be anonymized data that is not subject to the GDPR. Hence statistical information about vehicle classes and time of entry data become anonymous data as soon as the license plate information is deleted.

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 premises are recorded. EU member states determine the exceptions autonomously.

8 GDPR roles and responsibilities

The person responsible in most cases for the GDPR compliance of the Camlytics Software for processing personal data is the user (usually the end customer) as the controller of personal data. Camlytics does not bear any responsibility under the GDPR for such use of the Camlytics Software.

In such cases, the user is required to take technical and/or organizational measures designed to implement the data protection principles set out in the GDPR (privacy by design). For the Camlytics Software, examples of such measures would be restrictive access to administrative interfaces and the avoidance of combining the numeric information output with other data sources in order to identify or make identifiable individuals.

The user as personal data controller also has an obligation to implement technical or organizational measures to ensure, by default, the least privacy-intrusive processing of the personal data in question (privacy by default). In the context of the Camlytics Software, an example of such measures would be to avoid video streaming to a destination other than the Camlytics Software PC, 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 technical support and configuration, it is necessary that the administrator basically has access to the image of the respective camera.

8.1 Camlytics' GDPR commitment for the Camlytics Software

As mentioned above, the user of the Camlytics Software is responsible for ensuring GDPR compliance. Nonetheless, Camlytics would like to assist users in complying with the GDPR as much as possible. That is also the main purpose of this document. All functionalities in the Camlytics Software 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 individuals is generally a processing of personal data (appearance of human beings). This video surveillance takes place in the IP camera, so the video stream sent to the Camlytics Service PC contains personal data. The analysis of the video stream in the Camlytics Service PC represents the processing of personal data. The result of this analysis is the numeric information output, which can be either pseudonymized or anonymized.

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

Most applications can be configured so that individuals can no longer be identified from the still image of the configuration tool. Anonymization works as follows: All video streams and images from the camera are blocked. The configuration view still shows an image, meaning one can see what's going on, but one can hardly identify individuals from the image and it is not stored.

As a software manufacturer, Camlytics takes cybersecurity seriously and provides means to make products and applications more resilient and secure - for example, through authentication, authorization and password enforcement. This is not specific to the Camlytics Software, but an inherent part of our product development strategy to make computer vision faster, easier, smarter, more affordable, and more trustworthy.

8.2 Specifically about user's GDPR responsibility in relation to the Camlytics Software

Please remember to check what exact legal obligations may apply to you or your company when using the Camlytics Software. In this respect, Camlytics 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 Camlytics Software constitutes processing of personal data. In such cases, as a user of these applications, you (your company) are a personal data controller within the meaning of the GDPR. The GDPR imposes a number of requirements on personal data controllers. You should consider the following steps 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 which the video surveillance/Camlytics Software is used to process personal data (e.g. advertising, property protection, parking management etc.) and keep a written record of this documentation for evidentiary 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 must refer, among other things, to the types of personal data you collect and the purposes for which you use the data.
d. Never use personal data for a purpose other than the purpose(s) you disclosed.
e. Please make sure that you have a legal ground under Art 6 GDPR, for processing personal data, such as consent of data subjects, legitimate interests, or the 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 personal data management functions to comply with requests from data subjects regarding the personal data you hold.
g. Undertake safety measures for the 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 and sign 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 respective 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 through 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, the data protection authorities of the EU member states may make exceptions to this.

©2022 Spearr LLC. CAMLYTICS, is a registered trademark or trademark applications of Spearr LLC in various jurisdictions. All other company names and products are trademarks or registered trademarks of their respective companies. We reserve the right to introduce modifications without notice.