ISS
INTELLIGENT VIDEO. DEFINED.

ISS GDPR Compliance White Paper

Introduction

We live in a connected world, almost every aspect of our lives revolves around data. From online shopping and banking to social media posts, almost every service we use involves the collection and analysis of our personal data. Supplying our names, addresses, and credit card numbers over an internet connection has become commonplace and most of us do not give it a second thought. Recently, the rise of passive video monitoring that captures and records faces, as well as extracts personal metadata (age, race, gender) has become an important topic on the daily news cycle. All of this data that uniquely identifies an individual is collected, analyzed, and perhaps most importantly, stored by organizations. The General Data Protection Regulation (GDPR) adopted by the European Union is designed to reflect the reality of the connected world, and outlines laws and obligations that govern the collection, processing, and use of personal data, across Europe.

Brief History of Data Protection

The rapid growth of the digital information age and the ability to collect and store almost unlimited amounts of data prompted the European Union (EU) to revise the Data Protection Directive (official Directive 95/46/EC) formally adopted in 1995. This directive bolstered the due protection of individuals with regard to the processing of personal data and on the free movement of such data. These protections were a first step in data privacy, but were soon outpaced by technological advancements. In response, the European Parliament and Council passed the General Data Protection Regulation in 2016 to provide civilians the possibility to control their own personal data and to protect personal rights and freedoms.

The GDPR is a new set of rules for personal data processing operations conducted by organizations on EU residents that took effect on May 25th, 2018. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The GDPR enacts rules that aim to protect the privacy of individuals as it pertains to the collection and the use of their personal data. GDPR is the biggest change to the European data protection legal landscape since the EU Data Protection Directive was established in 1995. Although based on the current directive, the GDPR creates complex new obligations for organizations inside and outside of Europe.

GDPR Directives

The central tenet of the GDPR is the right of the individual to control their own personal data. The GDPR states that the individual owns or possesses the data being collected by the Data Controller. Under the regulation, Data Controllers are responsible for assessing the level of risk posed by their data processing operations against the fundamental rights and freedoms of individuals and then modulating their data protection compliance accordingly.

Central to the GDPR is that data is processed lawfully, fairly, and in a transparent manner in relation to the data subject. The transparency of data processing means that data is collected for a specified, explicit, and legitimate purpose, and that the data is not further processed to extract information that goes beyond the intended purpose. In other words, the collection of personal

data is limited to the intent of the original purpose (also called "data minimization"). The collected personal data must also be accurate and kept current, if applicable, while an agency that collects data must take every reasonable step to erase or rectify inaccurate personal data.

The GDPR also stipulates that collecting agencies must impose a limit on the amount of time personal data can be stored and that the data not be stored for longer than necessary. During the time the data is stored, the agency must also ensure the integrity and the confidentiality of personal data. The agency must employ technical and organizational measures to protect personal data from unauthorized or unlawful processing and from accidental loss, destruction, or damage.

Definitions

GDPR uses the following terms when describing the collection, processing, and use of personal data and privacy principles. These definitions are used throughout this document.

Biometric Data: Personal data resulting from specific technical processing relating to the data subject's physical, physiological, or behavioral characteristics, which allow or confirm the unique identification from data collected by scanning facial images, collecting fingerprints, or from any means that collects an individual's physical traits.

Data Controller: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: A natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

Data Subject: A natural person that a Data Controller collects information about, whether knowingly or unknowingly.

Personal Data: Any information that directly or indirectly allows the identification of a natural person ("data subject"). For example, a person's name, identification number, location data, online identifier, or a specific record of the physical, physiological, genetic, mental, economic, cultural, or the social identity of an individual.

Personal Data Breach: A compromise of security protocols leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

Processing: Any operation or set of operations performed on personal data or on sets of personal data. For example, collecting, recording, organizing, structuring, storing, adapting, transmitting, and analyzing personal data.

Supervisory Authority: An independent public authority, which is established by a Member State pursuant to GDPR Article 51.

Implications of GDPR for Video Surveillance

Over the last ten years, video surveillance has proliferated around the world. The availability of inexpensive cameras, the adoption of advanced analytics (including Artificial Intelligence for facial recognition and other video analytics) and the rise of cloud storage allows most home and business owners to install their own systems. Under the GDPR, video surveillance is considered a high-risk operation requiring particular attention, especially monitoring public areas with a large amount of foot traffic. The goal of video surveillance includes determination of vandalism and identifying criminals (but not limited to it), however cameras do not discriminate between criminals and those just going about their daily business. The same technology that aids law enforcement can also be used to identify passers-by and compromise their privacy, without them being aware of the fact.

The Data Controller and Processor are required to perform a data privacy impact assessment (DPIA) with the help of the data protection officer for every surveillance system set up. As part of the DPIA the Data Controller and Processor should list the specific processing activities they want to perform and the reasons why video monitoring is necessary in the first place. The Data Controller and Processor should then consider the risks to the individuals stemming from video surveillance, as well as any remedial measures they can take to reduce these risks. If the risks are excessive and cannot be reasonably reduced, it is best to contact the data protection authority (regulator) directly.

There is a need to strike a fair balance between the interest of privacy and of crime prevention. Most laws permit the operation of CCTV systems in such a way that they create a minimal intrusion into personal privacy. The principle of data minimization applies in all cases. Cameras should cover as little area as possible to fulfill their role. For example, for a bank this includes surveillance of the surrounding walls to prevent vandalism, but not of the pedestrian sidewalk across the street. The Data Controller and Processor should not forget that data handling guidelines apply to the recorded material. They must ensure security and privacy of the data for as long as you retain it, especially if individuals can be recognized on the recordings.

Right and Responsibilities of Video Surveillance under GDPR

The revised GDPR rules are designed to give EU citizens more control over their personal data. A key provision of the GDPR is that it establishes one law across Europe with a single set of rules that apply to companies doing business within EU member states. The reach of the legislation extends further than the borders of Europe itself, and includes:

- EU based Data Controllers and Processors, regardless of whether the processing takes place in the EU or not.
- Foreign-based providers of goods and services in the EU (irrespective of whether payment is required).
- Foreign-based organizations that monitor the behavior of EU residents.

The GDPR considers all information from which an individual can be pointed out with reasonable accuracy as personal data. GDPR defines personal data as any information relating to an identified or identifiable natural person (‘data subject’); a natural person is one who can be identified,

directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Under the terms of GDPR, not only do organizations have to ensure that personal data is gathered legally and under strict conditions, but those who collect and manage it are obliged to protect it from misuse and exploitation, as well as to respect the rights of data owners. Companies that collect personal data are Data Controllers, and they give commands for its processing to Data Processors, who carry out processing activities on behalf of the Data Controller. In most cases, these two will be the same entity, but need not be – cloud providers are an example of third-party Data Processors.

The GDPR outlines several principles relating to processing personal data (GDPR Chapter 2 Articles 5 – 11):

1. **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject.
2. **Purpose limitation** — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
3. **Data minimization** — You should collect and process only as much data as absolutely necessary for the purposes specified.
4. **Accuracy** — You must keep personal data accurate and up to date.
5. **Storage limitation** — You may only store personally identifying data for as long as necessary for the specified purpose.
6. **Integrity and confidentiality** — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
7. **Accountability** — The Data Controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

Use these principles as a guide to decide the type and amount of personal data collected, how you handle it, and what to do with the data after it is no longer needed. Typically, a Data Controller and Processor that handle personal data in a lawful manner and with transparency, in relation to the type of data collected, have a good start to complying with GDPR provisions. These organizations must explicitly specify the legitimate purpose for collecting and processing personal data and collect only that data that is relevant to the specified purpose.

Once an organization collects and processes personal data, it assumes the burden of ensuring the accuracy and protecting the integrity of the data. Organizations must keep data accurate and up-to-date and may only store the data for no longer than is necessary for the purposes for which they are processed. During the time the data is stored, organizations must protect personal data against unauthorized or unlawful processing, accidental loss, or destruction.

For example, a Data Collector and Processor may be a retail location that uses multiple surveillance cameras with facial recognition technology to monitor activity inside and outside the facility and upload the video to a cloud storage provider. To ensure that personal data is collected in the compliance with GDPR, this retail location should install signage that alerts people that video surveillance is in use. In addition, cameras that are positioned on the outside of the building should have a field of view limited to the building entrance to avoid recording people who are simply passing by the location.

Intelligent Security Systems (ISS) and GDPR

Intelligent Security Systems (ISS) offers the following guidelines for Data Controllers and Processors that utilize ISS solutions to help with planning their specific strategy to comply with GDPR directives. These guidelines, however, are not a substitute for a complete and comprehensive review of Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version.

ISS is not responsible for GDPR compliance and does not fall under regulations since ISS is not a Data Collector or Processor. ISS provides tools for the Data Collector/Processor to be able to create a personal data usage policy that will comply.

The table below lists the main GDPR requirements that are relevant to collecting and processing video images that contain personal data and lists the features in the SecurOS Video Management System that will assist with compliance.

GDPR Requirement	Relevance to Video Surveillance	Organizational and Technical
Data Subject Notification	**Lawfulness, fairness and transparency** The controller should notify a data subject that video imaging and recording devices are active in a location where the subject may visit. The notification should be in compliance with GDPR Article 12 and 13. The information should be delivered in a clear and precise manner that is in an easily accessible form.	This requirement does not a have direct impact on the SecurOS VMS. The Data Controller or Processor should provide a textual, graphical, video, voice or other type of notification about video surveillance in the area.

Right to Access/Right to Portability	**Accuracy.** Upon request, organizations need to deliver to a data subject all the personal data collected about them, including video images from a video surveillance system.	SecurOS offers tools to quickly find video and to deliver it to the data subject. • Save/lookup bookmarks • Region of Interest search • Motion Detection event search • Forensic search using SecurOS Tracking Kit, SecurOS FaceX or SecurOS ACS recorded metadata Video can be reviewed directly from a SecurOS client or can be exported and played back via industry standard players (VLC, for example) or the SecurOS native Evidence Manager player.
Right to be Forgotten	**Accuracy. Storage limitation.** Also known as the right to erasure, the GDPR gives individuals the right to ask organizations to delete their personal data when they no longer consent to processing, when there are signifcant errors within the data, or if they believe information is being stored unnecessarily. The GDPR, however, states that this is not an absolute right. Refer to GDPR Chapter 3 Article 17.	SecurOS provides settings to independently configure minimal and maximal video archive storage terms for each camera. In addition, there are retention settings for storing metadata in the database. Both video and metadata are erased completely as the data retention period is over. Metadata stored directly in SecurOS SQL databases, can be deleted if needed, with no negative effect on the functionality of the system.
Personal Data Storing and Processing	**Purpose limitation.** Process data for the legitimate purposes specified explicitly to the data subject when you collected it.	SecurOS provides capabilities to limit the amount of stored data corresponding to data usage. Examples: • Public safety applications need to record video, recognize faces, search for stolen cars, etc... • Convenience of access such as toll roads and gates opened by LPR, and turnstiles opened by facial recognition • Business process automation These use cases are justified by public notifications or rules and standards of corporations/organizations.
	Data minimization. Collect and process only as much data as absolutely necessary for the purposes specified.	SecurOS allows organizations to independently configure video archive parameters for each camera (resolution, frames per second, etc.). The SecurOS Archiver module manages long-term video storage quality and video retention policy. SecurOS provides tools that specify when video is recorded based on events to minimize the amount of data collected. These events include: vandalism to the camera, motion detection or other alarms based on an analytic event, and recording based on a specified schedule (for example, recording during normal business hours). Event-based recording limits the type and amount of video data collected and processed.

Personal Data Storing and Processing *(Continued)*	**Storage limitation.** Store personally identifying data for as long as necessary for the specified purpose.	SecurOS provides settings to independently configure minimal and maximal video archive storage terms for each camera (as well as retention settings for storing metadata). The SecurOS Archiver module manages long-term video storage quality and video retention policy.
	Integrity and Confidentiality. Process data in such a way as to ensure appropriate security, integrity, and confidentiality.	SecurOS Video Archive stores recorded video in a native format that can be encrypted using HDD Self-Encrypting technology. Self-Encrypting AES-256 hard drives keep your data safe even if the drives are lost, stolen, or misplaced. Exported video archive files can be encrypted (AES-256) and protected with a password and a digital signature. SecurOS VMS has built-in user right management that can define user access on an object level. SecurOS VMS supports Windows Active Directory user authentication including user groups. SecurOS VMS stores all passwords in an encrypted state. SecurOS connection restriction settings allow an administrator to set a list of client workstations capable of connecting to the system (based on IP address or NetBIOS name). SecurOS VMS provides logging of all important system events and administrator / user activities to exclude improper system usage.
Personal Data Storing and Processing **Special Use: Biometric Data Usage**	**Purpose Limitation.** Collecting and processing biometric data runs the highest risk of violating an individual's rights and freedoms due to the restrictions placed on this type of data. Refer to GDPR Chapter 2, Article 9 Paragraphs 2, 3, and 4 for specific cases where the GDPR allows collection and processing of biometric data.	The SecurOS face recognition module stores a person's face in an SQL database using digital descriptors. These descriptors have no meaning outside of the system. The 'detection' pictures are cropped out of video frames and stored in a separate database table. Data Subject identification information is stored only when the Data Collector or Processor decides to store it in a watchlist. The Data Collector or Processor decides what information to store in the profile for each entity in the watchlist. For example, the system omits the person's first and last name and only stores an abstract ID number to refer to a person in any database separate from the facial recognition system. If sensitive information is stored in profiles, the watchlist database should be secured in the same way as any other sensitive data would be according to GDPR requirements.

Data Protection and Security of Processing (Cybersecurity)	**Integrity and Confidentiality.** Personal Data must be processed in a manner that ensures appropriate security of the data. This includes protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.	**Encrypted Connectivity:** SecurOS provides a secured HTTPS connection between SecurOS video servers and IP devices as well as connections to SecurOS Mobile and Web Clients applying the following technologies: • Trusted certificates to establish connections over SSL or TLS • Trusted certificate management via Windows Certificate Store • Encrypted video and audio transfer inside an HTTPS-tunnel • Encrypted message exchange to pass authentication credentials, settings, and commands • SecurOS supports digest authentication when connecting to IP devices (actual password is never sent over network) **User Rights:** • SecurOS has a built-in user rights management to provide secure access to the system. Also, SecurOS is able to use Active Directory or LDAP to authenticate into the system **Safe Connection to Public Network:** • Firewalls should be used when possible for local and external connections. Rules can be set if needed to allow trusted connections • SecurOS supports working through VPN over public networks
	Accountability. The Data Controller shall be responsible for and be able to demonstrate compliance with GDPR requirements in relation to video surveillance.	**SecurOS Audit Trail:** • Any system changes, user logins, video exports, and other user activity can be tracked using the SecurOS Audit Trail module

Conclusion

GDPR is a set of rules designed to give EU citizens more control over their personal data by simplifying the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy. The reforms are designed to reflect the modern connected world and bring laws and obligations - including those around personal data, privacy and consent - across Europe up to speed for the Information Age.

GDPR establishes one law across the continent and a single set of rules which apply to companies doing business within EU member states. This means the reach of the legislation extends further than the borders of Europe itself, as international organizations based outside the region but with activity on ‘European soil’ will still need to comply. Under the GDPR provisions that promote accountability and governance, companies need to implement appropriate technical and

organizational measures, including data protection provisions (staff training, internal audits of processing activities, and reviews of HR policies) and documenting processing activities. Countries and regions around the world took note of GDPR and are considering introducing or modifying data protection legislation. Brazil, Japan, South Korea, and India have already signaled that they are revising their own privacy laws since the introduction of GDPR. In addition to these countries, Silicon Valley, California, is also set to introduce its own data privacy laws in the California Consumer Privacy Act, which was put into force on January 1, 2020.

ISS products already have built-in functions to address the impact of GDPR on collecting, analyzing, recording, and archiving corresponding metadata as they relate to personal privacy. ISS SecurOS employs tools that help to minimize the data collected and then maintains the integrity and the accuracy of the data. ISS is positioned to ensure that any Data Collector or Processor has tools at their disposal to comply with GDPR.