Whitepaper

What the GDPR means for Video Surveillance

General Data Protection Regulation (GDPR) for video surveillance applications

Genetec™

Contents

1

Overview of the GDPR

The GDPR is a new set of rules for personal data processing operations conducted by organizations on EU residents that will begin to apply on May 25th, 2018. 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, and it is predicted by Gartner that, by the end of 2018, "more than 50 percent of companies affected by the GDPR will not be in full compliance with its requirements".

"Gartner Says Organizations Are Unprepared for the 2018 European Data Protection Regulation". May 3rd, 2017. http://www.gartner.com/newsroom/id/3701117.

GDPR uses a risk-based approach to data protection that will require organizations to assess the level of risk that their data processing operations pose to the fundamental rights and freedoms of individuals, referred to in the GDPR as 'data subjects'. These rules will govern the collection, use, and sharing of personal data by both data controllers—organizations that collect personal data for their own use—and data processors—organizations that process data (which also includes holding data) on behalf of data controllers, such as cloud service providers. Personal data includes name, home address, photo, bank details, social networking posts, medical information, IP addresses, mobile device ID, and IoT collected data.

The rights of individuals with regards to their data are fundamental to the new regulation. According to the GDPR, the individual still owns or possesses the data being collected by the data controller.

Under the regulation, data controllers are responsible for (1) assessing the level of risk posed by their data processing operations against the fundamental rights and freedoms of individuals and then (2) modulating their data protection compliance accordingly.

One of the goals of this regulation is to protect the data of individuals by forcing data controllers to manage data in a secure manner and to react appropriately in the case of privacy or data breaches. To this end, the GDPR requires data controllers to build data protection into the design and infrastructure of their systems; those data controllers who fail to comply will face large monetary fines, class actions, and damage to their reputations. Consequently, this new paradigm in data protection is an opportunity for data controllers to introduce new systems and promote innovation in connection with the handling of personal data, especially in the areas of management, securitization, anonymization, and delivery, with those that get ahead of the curve potentially gaining a significant competitive advantage.

1.1 What the GDPR means for video surveillance

Data controllers running video surveillance applications in the EU, including public video surveillance systems, need to pay special attention to the provisions in the GDPR relating to the identification, management, and mitigation of risks. While the GDPR does not make specific reference to video surveillance applications, the general data protection principles of the GDPR apply to it. European Data Protection Agencies (DPA) classify video surveillance that involves the monitoring of public areas on a large scale as a 'high-risk processing operation'. As a result, data controllers performing video surveillance in the EU will have to undertake very specific tasks, including conducting risk assessments, ensuring privacy by design in their systems, and developing appropriate signage.

When determining a compliance strategy for their systems, data controllers have the option to either (1) build their own solutions on-premises or (2) outsource the data processing. In either case, data controllers need to find a solution that can help them fulfill their GDPR obligations to deliver any data collected on an individual to that individual upon request.

A trusted partner who understands video surveillance and issues of privacy and data protection can be vital for achieving full GDPR compliance for video surveillance applications. Data controllers looking to build their own compliant video surveillance applications on-premises will need to consider ways to harden their systems and find solutions that offer such built-in functionality as encryption, authentication, and anonymization to ensure compliance. Those looking to outsource their data processing operations to a data processor will need to partner with an organization that offers solutions that can help them become fully compliant with GDPR requirements.

GDPR is the biggest change to the European data protection legal landscape since the EU Data Protection Directive was established in 1995.

2

The implications for video surveillance of the rights and responsibilities in the GDPR

The GDPR is different from the current European Directive in a number of important ways, especially as it pertains to 'high-risk processing operations' like video surveillance. First, the GDPR considerably extends the scope of current EU data protection laws and grants EU individuals an assortment of new rights. Second, it requires greater accountability from data controllers than the current law with regards to such key issues as privacy notices and data breaches and, in certain circumstances, requires data collectors or processors to appoint a Data Protection Officer (DPO). The GDPR also imposes specific obligations on data processors, including cloud service providers, enshrines the concept of privacy by design in legislation, and calls for severe penalties for non-compliance.

2.1 Expanded scope

Extended jurisdiction is one of the most significant changes introduced by the GDPR. In particular, the GDPR applies to the personal data processing operations on individuals by the following organizations:

1. EU based data controllers and data processors, regardless of whether the processing takes place in the EU or not
2. Foreign-based providers of goods and services in the EU (irrespective of whether payment is required)
3. Foreign-based organizations that monitor the behavior of EU residents

2.2 New rights for individuals

Individuals are granted stronger and wider rights under the GDPR, which can be summarized as follows:

2.2.1 Privacy notices and consents

In order to make data controllers more transparent about their collection and use of data, the GDPR requires them to publish privacy notices stating the identity of the data controller and providing information about the nature of the data processing operation being undertaken. Privacy notices must contain extensive, prescribed disclosures, including

- contact details for the data controller
- purpose of the processing
- with whom the data will be shared
- details of any data transfer outside of the EU
- how long the data will be kept
- what an individual's rights are
- how to file a complaint

The notices must be clear and presented in an easy-to-read form; long, illegible terms in legalese will be forbidden.

Notices must also be concise, which clearly presents a challenge for video surveillance notices. European DPAs favor 'layered' notices that provide basic information upfront with links to fuller information for those who want it. Therefore, video surveillance providers who wish to avoid a large sign displaying all the above information could possibly use a small sign setting out who they are and why they are capturing images together with a URL or phone number for individuals interested in obtaining the full notice.

The regulation also applies to video surveillance applications in which a data controller uses another data controller's video management platform to gain greater situational awareness. For example, city surveillance systems are increasingly being built using a collaborative approach that integrates systems and shares the information in those systems with third parties. In such instances, the data collector collecting the initial data will also need to provide contact information for the third parties who have access to the data. In addition, those third parties will also need to appropriately manage and protect the gathered data.

According to the GDPR, an individual's consent, which is one of the numerous legal bases for processing, must be freely-given, specific, informed, and unambiguous. As a result, silence or pre-ticked boxes to infer consent will be forbidden. Under the GDPR, it must be as easy for individuals to withdraw consent as it is for them to give it.

According to the GDPR, an individual's consent, which is one of the numerous legal basis for processing, must be freely-given, specific, informed and unambiguous.

2.2.2 Right to access

The new regulation greatly increases data transparency while also giving greater power to individuals. Under the GDPR, individuals have the right to obtain confirmation as to whether or not their data is being processed, where it is being processed, and for what purpose. In addition, the data controller will be required to remit, free of charge, a copy (including in electronic format) of the personal data to the individual upon request. The GDPR also introduces a new best practice recommendation that, where possible, organizations should be able to provide remote access to a secure self-service system that would provide individuals with direct access to their information.

In the case of video surveillance, data controllers will need to have systems in place to recognize requests, assess their validity, and provide the information within a month. This can be especially challenging for video surveillance systems in cases where an individual requests copies of video in which the identity of other individuals included in the footage will need to be masked or otherwise protected.

2.2.3 Right to erasure (or to be forgotten)

Individuals will be able to ask for their data to be erased, to object to processing, or to restrict the processing of their data. The conditions for erasure include (1) when the data is no longer relevant with regards to the original intent of the processing operations and (2) when processing was originally based on consent and then individuals withdraw their consent.

2.2.4 Right to data portability

Individuals can ask to receive their data and port it to a new data controller. Data controllers must provide the data in a commonly-used, machine-readable format. Individuals can also ask for their data to be transferred directly to a new data controller.

2.2.5 Breach notification

The GDPR imposes a mandatory data breach reporting rule on data controllers. Breaches must be reported to EU DPAs within 72 hours after the data controller first becomes aware of the breach. Data processors will also be required to notify data controllers—who are their customers—about data breaches "without undue delay".

In addition, if a data controller has determined that a data breach is likely to pose a high risk to the rights and freedoms of individuals, the data controller is required to also notify affected individuals "without undue delay". However, the GDPR contains an exception to this requirement to notify affected individuals, and it applies to data controllers that make their data unintelligible to unauthorized persons through the implementation of appropriate technical and organizational protection measures, including encryption and anonymization.

2.3. Accountability and appointment of DPOs

Currently, data controllers must register with their local DPA. While this requirement will disappear, the GDPR imposes new record-keeping requirements on data controllers and processors. Data controllers will also be obliged to conduct a Data Protection Impact Assessment (DPIA) and consult the DPA in cases where processing is high risk. Organizations will also have to appoint a DPO in cases of high-risk data processing, including video surveillance applications involving the systematic monitoring of a public area on a large scale—for example, in the case of city-wide or campus-wide surveillance systems.

2.4 Privacy by design

Under the GDPR, privacy must be by design instead of 'in addition'. The privacy by design obligation in the GDPR requires an approach to systems engineering in which data protection principles, such as encryption and the anonymization of video footage, for example, are included from the outset in any system design.

In addition, data controllers will also be responsible for ensuring that, by default, the minimum amount of data is collected. Video surveillance systems that record constantly and store images indefinitely will be in breach of this provision; as a result, data controllers

will need to adopt video surveillance systems with a feature-rich interface that offers flexibility in video recording operations that would enable them to control how long images are retained.

2.5 Specific obligations for data processors

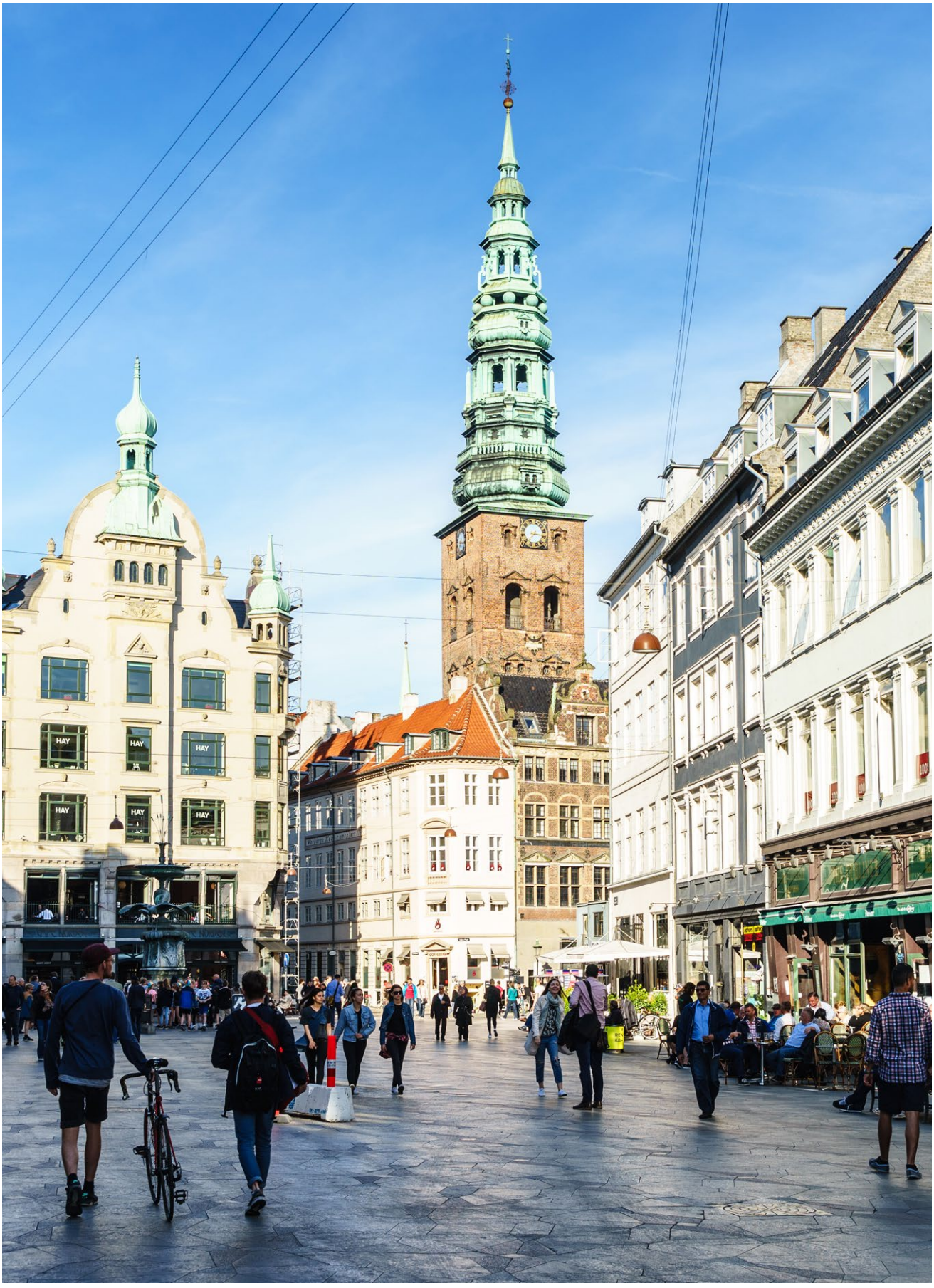
As mentioned earlier, data controllers may decide to outsource their data processing operations using third party solutions. In such cases, the GDPR requires data controllers to put certain terms in place with their data processors, including

1. the obligation to assist the controller to meet its GDPR obligations
2. the obligation to only process according to instructions from the controller
3. the obligation to not engage the services of a sub-processor without permission and to provide the controller with contractual audit rights

2.6 Penalties

The GDPR will also introduce a tiered system of fines for both controllers and processors that can reach 4% of annual turnover or €20 million, whichever is greater. The percentage of the fine will be measured against the entire group's gross revenue rather than against net profits. The GDPR will also allow individuals harmed by a breach to bring civil actions.

The GDPR will also introduce a tiered system of fines for both controllers and processors that can reach 4% of annual turnover or €20 million, whichever is greater.


HAY
HAY
HAY
HAY
HAY
HAY

3

Moving towards a GDPR-compliant video surveillance system

This section (1) provides data controllers with a series of important considerations aimed at making the transition to a GDPR-compliant video surveillance system as operationally efficient as possible and (2) considers different solutions or functionality for making end-to-end video platforms more resilient.

With regards to GDPR compliance, data controllers need to pay special attention to video surveillance as a data processing operation because of its context and scale and because of its intrusive nature. Large scale video surveillance systems will be defined as high-risk processing operations under the GDPR and will require special treatment.

Genetec can provide data controllers with valuable insight into the extent of their GDPR obligations

After assessing the level of risk involved in their video surveillance applications, data controllers should then think about how to protect their systems from data breaches and undertake a thorough assessment of the flow of data through the three stages of their data processing operations—from collection and processing through to restitution.

Data controllers should also review how they will process the rights of individuals, especially around their rights to request captured footage. These requests could prove costly in terms of the time required to both collect and anonymize the data. The right technology could significantly reduce the impact and overall cost of this obligation.

And, finally, data controllers should consider how a data processor could help them achieve compliance for their video surveillance applications by providing the appropriate infrastructure.

As a trusted partner, Genetec can provide data controllers with valuable insight into the extent of their GDPR obligations and on how best to design and develop their video systems to meet those obligations. Genetec also offers on-premises and SaaS end-to-end solutions that can help data controllers achieve GDPR compliance with both their basic and extended responsibilities with regards to the high-risk processing operations of video surveillance data.

3.1 Level of risk

For data controllers undertaking video surveillance applications on EU individuals, the first step towards ensuring GDPR compliance is to conduct a DPIA in order to determine whether processing is "likely to result in a high risk to the rights and freedom of individuals".

Data controllers must first review Article 35 to determine the level of risk associated with their specific video surveillance applications. The types of processing that may result in high risk to the rights and freedom of individuals are those that involve

- a systematic and extensive evaluation of personal aspects relating to natural subjects, which would include facial recognition for profiling purposes and Automatic License Plate Recognition (ALPR)
- a large scale, systematic monitoring of a publicly accessible area, including cities, airports, stores, and hotels

If data controllers are operating such high-risk systems, they will have to appoint a DPO and may require the consent of the DPA before proceeding.

3.2 GDPR data breach obligations

The move towards GDPR compliance starts before the implementation of the video surveillance system itself, and data controllers need to begin by thinking about how to harden their systems against data breaches. Regardless of the sensitivity of the data being collected, a data breach can:

- negatively affect reputation and damage brand recognition
- significantly increase operational costs as data controllers work to close the breach and ensure that their systems are clean
- result in large monetary fines

The ability of data controllers to effectively respond to an intentional or unintentional data breach will be an important part of the risk assessment process since the GDPR requires data controllers to report breaches within 72 hours of their discovery.

Depending on the implementation of a video surveillance system and on who participates in its management, an effective communication process, as well as appropriate tools, will need to be put in place to report data breaches in any component in the system. The traceability of all operations through logs and reports as well as chain of custody when a series of videos become evidential will be important functionalities for achieving compliance. And, to help protect the rights and privacy of the individuals whose data is being collected, data controllers can also implement technical and organizational protection measures, including encryption and anonymization, that make data unintelligible to unauthorized persons. With these processes, tools, and data protection measures, data controllers can effectively investigate the cause of a breach as well as demonstrate their commitment to managing data responsibly.

Genetec on-premises and SaaS solutions: 'Security-of-Security' is at the heart of our proactive strategy to prevent data breaches and unauthorized access to personal information. Genetec products use encryption and claims-based authentication, provide an authorization management functionality, and offer dynamic anonymization that automatically anonymizes individuals in live and recorded video when monitoring actions and movements.

3.3 GDPR compliance and the flow of data

3.3.1 Collection

Collection refers to the actual recording of information, and, at this stage, data controllers are responsible for ensuring that their systems can maintain data integrity. If a data processing operation is high-risk, data controllers should consider encrypting or anonymizing the video stream.

For instance, to protect the rights of individuals enshrined in the GDPR, data controllers can encrypt the data that they collect. When data is encrypted, even if an unauthorized person or entity gains access to the data, it is not readable without the appropriate decryption key. Whether the data is at rest or in transit from a camera, encryption protects sensitive data and enhances the communication between clients and servers. Other effective measures that can help to make a video surveillance system resilient and secure are authentication, authorization, and password enforcement.

A video surveillance system can ensure that the identity of individuals remains anonymous in three ways:

1. Permanent masking, which involves permanently anonymizing individuals in video footage and means that the masking cannot be removed
2. Dynamic anonymization, which is the process through which a software, monitoring actions and movements, automatically anonymizes individuals in live and recorded video
3. Redaction, which involves hiding the identity of only selected people in the video footage and which is usually done after-the-fact when an organization wants to share video with law enforcement

Genetec on-premises solutions: Genetec Security Center offers encryption and authentication methods to ensure that only authorized personnel can gain access to a data controller's security system. With Security Center, data controllers can implement new levels of encrypted communication between all system components and use digital certificates to guarantee trust within their systems. Security Center can also authenticate communications within the system, validating and ensuring that data and video are not exchanged with outside sources.

Offering dynamic anonymization that automatically anonymizes individuals in live and recorded video when monitoring actions and movements, Security Center can also help data controllers achieve compliance when conducting video surveillance of public spaces. KiwiVision™ Privacy Protector™ allows for originally plain video to be cryptographically encrypted and recorded in the background and then later decrypted by authorized personnel. Data controllers can apply Privacy Protector to only those cameras that are involved in high-risk processing and can choose the ideal level of anonymization for every situation. With only a few clicks, they can either pixelate, blur, or completely obscure individuals and objects in a camera's field of view.

Genetec SaaS solutions: Data controllers can achieve GDPR compliance with regards to data integrity during collection by deploying

the Genetec Stratocast™ offering. And, in order to achieve compliance concerning the redaction of video exports, the Genetec Clearance™ Case Management solution as a Service provides data controllers with the tools required to accomplish the task in an efficient and timely way.

3.3.2 Processing

Processing refers to the actual data processing operation carried out by the data collector. A key provision in the GDPR is that data controllers will be responsible for policing access to the data being collected in their systems. This is important for both privacy and for managing possible data breaches as the proper management of access rights can help to reduce the chances of an unintentional data breach.

Authentication and authorization are two ideal ways for data controllers to control who can access the video and data being collected in their systems. Data controllers can protect access to their systems through authentication mechanisms that ensure that personnel access the correct system when they log in. Authentication uses certificates, username/password combinations, and tokens to prevent cyber-criminals from pretending to be a security server in order to penetrate a security system and manipulate, copy, or take control of the data. Authorization involves controlling who sees the data within a system and what they can do with that data. With authorization capabilities, data controllers can restrict the scope of activity within their system by giving access rights to groups or individuals for resources, data, or applications and by defining what users can do with the resources, thereby ensuring the security of the data transmitted and stored within their systems.

Genetec on-premises and SaaS solutions: Genetec solutions offer detailed user access privileges to help protect privacy by clearly defining how authorized personnel are given access to specific data and whether they can modify that data or system behavior.

3.3.3 Restitution

Restitution refers to the lifecycle management of the collected data and to the GDPR requirement that data controllers must, upon request, provide digital copies of personal data to individuals. This is a very important part of the GDPR as individuals have the right to request a copy of their own data.

In most cases, data controllers must provide this service free of charge and they must ensure that, when honoring such requests, they do not impact the rights and freedom of others. One way to achieve compliance when considering data portability would be for data controllers to provide digital copies of information through a

self-serve kiosk. However, since a common issue with video surveillance is the presence of many individuals on any piece of footage, video anonymization that protects the freedom and privacy rights of other individuals will be essential. Also, as a result of an individual's right to erasure, data controllers need to pay careful attention to the management of their archives since they may be required to isolate and erase specific data.

Genetec on-premises and SaaS solutions: To fulfill their obligations for restitution, data controllers will first need to identify the images in which the individual is present. Either through its standard offerings or via technology partners, Genetec offers a series of tools that can greatly facilitate the search, identification, and gathering of an individual's recorded information.

For the restitution itself, data controllers can deploy Genetec Clearance in their video surveillance systems to recognize requests for data from individuals, assess their validity, and provide the information/service within a month. This open architecture cloud-based solution features encryption, centralized video collection, and advanced search that are all essential for efficiently and securely managing 'high-risk' video data. With built-in video redaction capabilities that mask the identity of all individuals captured by video cameras, data controllers can also use Genetec Clearance to develop a remote access, self-service portal where individuals could directly access their personal data.

3.3.4 Tools to support Data Protection Officers (DPOs)

Data controllers might have to appoint a DPO to monitor their compliance with respect to their GDPR obligations. It will be vital for data controllers to have access to the right information, and, if appointed, the DPO will need to be able to show the steps taken by the data controller to protect the collected information.

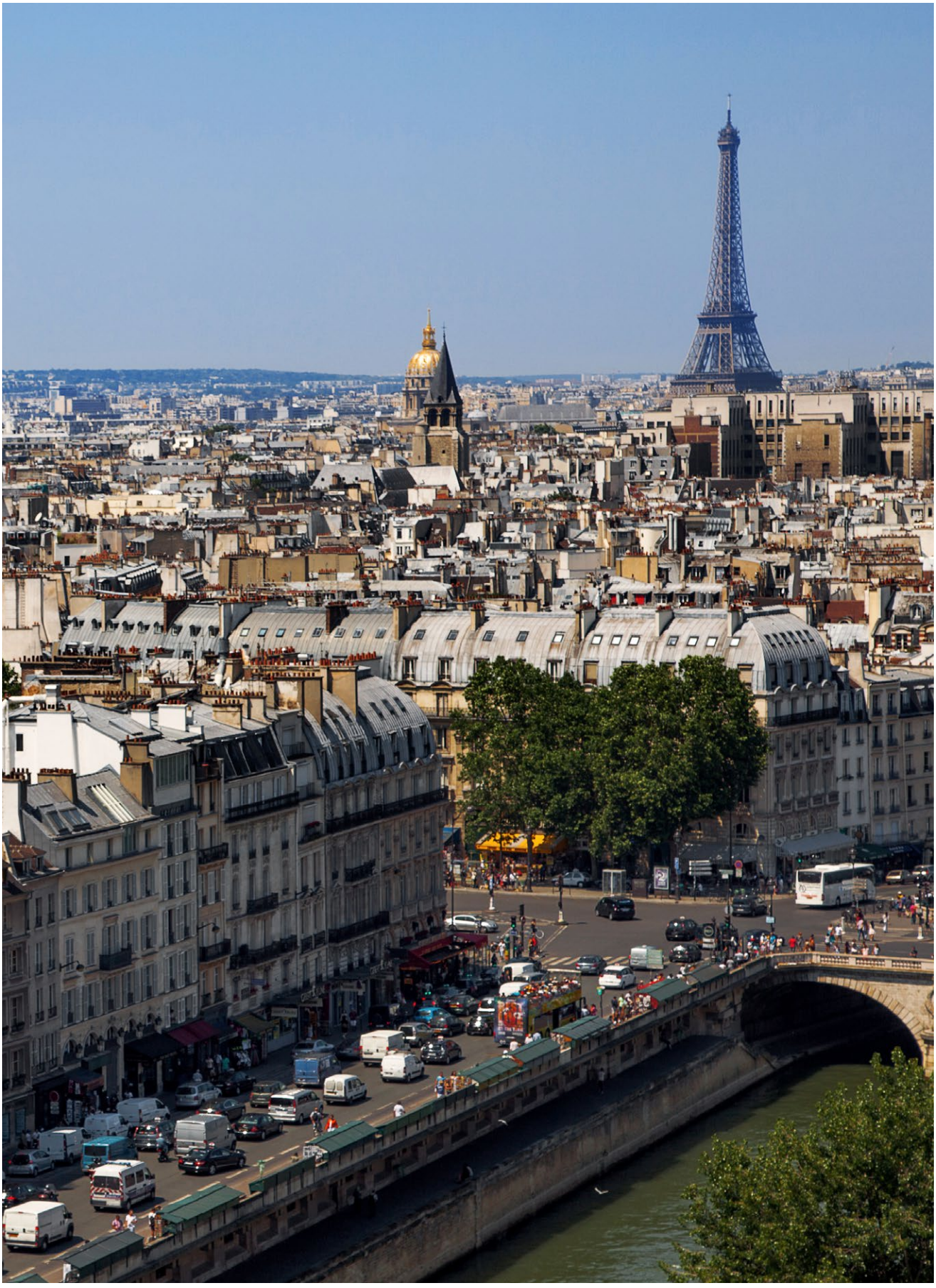
Genetec on-premises and SaaS solutions: Genetec solutions offer numerous logs and, more importantly, a strong reporting platform that can help data controllers and DPOs monitor the state of their video surveillance systems or to conduct research around who had access to, and/or downloaded information from, their systems.

4

Conclusion

The GDPR starts to be applied on May 25th, 2018, and all organizations running video surveillance applications on EU data subjects, especially in public areas, will need to ensure that their systems meet the privacy by design obligations laid out in the regulation. Organizations will also have to respect the rights of individuals as enshrined in the GDPR, including the right of access to their collected information. In addition, organizations will need to monitor and maintain the integrity of the data collected and will need to inform DPAs of a breach within 72 hours. Failure to comply will damage an organization's reputation and will result in large monetary fines.

Genetec can guide organizations towards GDPR compliance with its on-premises solutions or, contracted to act as a data processor, with its portfolio of SaaS solutions. Genetec can also help organizations reduce operational costs associated with their video surveillance applications by providing both search and redaction tools.



Established in 1997, Genetec is the global leader in unified security platforms, with a broad offering across a range of security specialties.

Video surveillance: Achieve greater situational awareness and enhance security within your city with the ability to share cameras across agencies and organizations, providing a common operational picture and improving incident response time.

Access control: Heighten your organization's security, effectively respond to threats, and make clearer and timelier decisions with a unified, IP-ready platform, whether deploying a new access control system or updating an existing installation.

Automatic license plate recognition: Automate the detection of vehicles of interest, increase parking enforcement efficiency and accelerate public safety investigations through the ability to share license plate data with selected agencies and partner organizations, without forfeiting ownership and privacy.

Operational decision support: Create efficiency for incident handling and decision making with advanced workflows that guide operators from situation alerts through policy-based procedures to detailed case compilation export.

Investigative case management: Simplify case management and speed up investigations with a platform that allows you to centralize digital evidence and securely collaborate with investigators, outside agencies and the public.

Cloud services: Extend the capabilities of your on-premises security system and reduce IT costs with highly scalable, on-demand cloud services that allow your city to easily cope with rapidly changing security requirements and operate with greater efficiency.

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

GDPRWP_WPIEN