

WISeNET

White paper

GDPR (General Data Protection Regulation) for Video Surveillance System

May. 8th 2018

Contents

1. Preface : Impact of GDPR on CCTV Video Surveillance

2. Overview of GDPR

2.1. Key Details of GDPR

2.1.1. Principles Related to Processing of Personal Data

2.1.2. Protection of the Rights of Data Subjects

2.1.3. Increased Responsibility of Controller and Processor

2.2. Sanctions for GDPR Violations and Ripple Effects

3. GDPR Compliance Efforts

3.1. Principles Related to Processing of Personal Data, Privacy by Design and Default

3.1.1. Storage Period Limitation and Safe Destruction

3.1.2. Audio Recording Restriction

3.1.3. Restriction of PTZ Recording Beyond Scope of Purpose

3.1.4. De-identification

3.2. Protection of the Rights of Data Subjects

3.2.1. Right to Access

3.2.2. Right to Be Forgotten

3.2.3. Hanwha Techwin Video Analysis Solution

3.3. Cyber Security Issue Management

3.3.1. Management of Access Permissions

3.3.2. Access Control

3.3.3. Safe Transmission

3.3.4. Safe Storage

3.3.5. Safe Release (Backup)

3.3.6. Prevention of Forgery and Tampering

4. Conclusion

Hanwha Techwin Co., Ltd. strives to deliver the latest information about GDPR through this GDPR white paper. However, Hanwha Techwin Co., Ltd. makes no warranty as to the accuracy or business suitability of the information described in this white paper. Please note that you must consult with a professional advisory body or attorney to confirm and respond to your rights and obligations under applicable statutes. Hanwha Techwin Co., Ltd. shall not be liable for any consequences of believing and applying the contents of this white paper without such consultation.

Despite the positive aspects such as social safety and improved security, the CCTV industry suffers from a negative image throughout society due to the spread of surveillance lacking operational reliability and concerns of personal privacy breaches. As new technologies such as Internet (IoT), cloud, Big Data, and AI are applied and converged with IP-based CCTV systems and new possibilities are created, risks of network security vulnerabilities (e.g., unauthorized access and acquisition of personal data) and related legal risks of network CCTV systems are also rising.

In an effort to cope with this situation, the European Union (EU) has enacted the GDPR (General Data Protection Regulation), which ensures the free movement of personal data between EU member states while strengthening privacy protection rights of the data subject (person). This regulation was introduced on May 25, 2016 to vitalize the digital economy within the EU, and it will be enforced from May 25, 2018.

GDPR significantly strengthens the rights of the subjects of personal data as well as the obligations and responsibilities of personal data controllers and processors. In this regard, CCTV system users and service providers should bear in mind that they are legally responsible for security vulnerabilities caused by the network CCTV system they manage or serve the customer.

Therefore, when installing new CCTV systems or upgrading existing systems, a Privacy Impact Assessment (PIA) should be performed before processing any personal data to determine any security risks and establish the necessary safety measures to protect privacy and personal data, even on existing CCTV systems on which PIA was never performed. For example, serious security issues such as initial password settings, periodic analysis of vulnerabilities in technology and equipment, maintenance of acceptable standards (critical bug fixes and software updates), awareness about the Code of Conduct and compliance and breach notification training for employees should be included in the PIA and rectified.

In addition, when consigning a cloud-based CCTV image storage or analysis service to a third party, the processor's management responsibilities from consigning information processing has strengthened and legal liabilities for violations has increased.

However, the background of Europe's GDPR legislation focuses on encouraging initiative and preemptive accountability, instituting such requirements as the Privacy Impact Assessment or Privacy by Design/Default, rather than passive

formal compliance with strengthened regulations. In other words, it encourages natural improvement in the awareness of GDPR compliance processes by rewarding controller's or processors innovative efforts for GDPR compliance while adopting appropriate mechanisms such as enforcing the Code of Conduct and certifications.

If GDPR compliance is achieved by implementing appropriate technical and organizational measures with preemptive accountability under the leadership of the user or service provider of the CCTV system, it would lead to restoring the reliability and transparency of CCTV video surveillance. This would then result in the growth of the CCTV industry and ultimately serve as a catalyst for promoting the digital economy, including the utilization of big data. Furthermore, companies handling personal data of Europeans are subject to GDPR compliance and enormous fines, regardless of whether the company is located within the EU. This practically enforces GDPR compliance and has significant impact on companies in non-EU countries.

Unlike the existing legislative guideline for EU member states, the GDPR holds direct legal binding over all EU member states. It also applies to foreign entities not located in EU, but who provide goods or services to EU residents or processes personal data of EU residents. A serious violation of GDPR is subject to a fine of up to 4% of annual global revenue or €20 million, whichever is greater. In addition, a violation of the GDPR may be subject to class action or civil law suits against individuals. As a result, it requires extreme caution of companies operating in or expanding to the EU.

In addition to general personal data such as names and phone numbers, the GDPR considers a wider scope of personal data such as online identifiers (IP addresses and cookies), as well as genetic information and biometric information. Large-scale, systematized monitoring of public spaces using CCTV systems is categorized as personal data processing with high potential risks of privacy invasion.

The following are key elements that controllers and processors (CCTV monitoring consignment body and executing body) must keep in mind when monitoring or processing personal data using CCTV systems (surveillance cameras, storage devices, and monitoring software).

2.1. Key details of GDPR

2.1.1. Principles Related to Processing of Personal Data

Principles of lawfulness, fairness, and transparency

Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.

Principle of Purpose Limitation

Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Principle of Minimization

Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

Principle of Storage Limitation

Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Principles of Integrity and Confidentiality

Personal data must be processed in a manner that ensures proper security, including protection against unauthorized or illegal processing, accidental loss, destruction, or damages through appropriate technical and organizational measures.

Principle of Accuracy

Processing of personal data must be accurate, and reasonable measures to keep it up-to-date must be taken. Lastly, the controller is responsible for complying with and proving such compliance with the six principles above.

2.1.2. Protection of the Rights of Data Subjects

GDPR strengthens the rights of the data subject with the addition of right to erasure ("right to be forgotten"), data portability, and automated individual decision-making (profiling).

Right to Provision of Information

The controller shall provide information related to the processing of personal data to the data subject in a concise, clear, and understandable form.

Right to Access

The data subject shall have the right to request

- i. confirmation of his/her personal data being processed and
- ii. access to his/her personal data.

Right to Rectification

The data subject shall have the right to request rectification of any inaccurate or incorrect personal data.

Right to Be Forgotten

The data subject shall have the right to request the controller to delete his/her personal data.

Right to Restriction of Processing

The data subject shall have the right to restrict or limit processing of his/her personal data.

Right to Data Portability

The data subject shall have the right to request transfer of personal data so that it can be reused in other services.

Right to Object

The data subject shall have the Right to Object at any time, on grounds relating to his/her particular situation, to processing of personal data concerning him/her.

Rights Related to Automated Individual Decisionmaking, including Profiling

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her or significantly affects him/her in a similar way.

2.1.3. Increased Responsibility of Controller and Processor

As a natural person, corporation, public organization, or agency that determines the purpose and means of personal data processing, the controller shall be responsible for implementing appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR, taking into account the nature, scope, context, purposes and risks of personal data processing.

As a natural person, corporation, public organization, or agency that processes personal data on behalf of the controller, the processor shall process personal data in accordance with the instructions of the controller.

Records of Processing Activities

To demonstrate compliance with GDPR, the controller and processor shall maintain a record of personal data processing activities performed under its responsibility. The obligation to maintain records of processing activities does not apply to corporations with fewer than 250 employees. However, such obligations apply regardless of the number of employees if

- i. personal data processing poses risks of infringing the data subject's rights or freedom or
- ii. when processing sensitive data.

A Privacy Impact Assessment should be conducted in cases of large-scale, systematized monitoring of public spaces. If the Privacy Impact Assessment concludes that there is risk of infringing the rights and freedom of a data subject, processing activities should be recorded regardless of the number of employees.

Data Protection by Default

The controller shall review personal data protection in the engineering and development of IT systems and processes and implement appropriate technical and organizational measures to demonstrate that personal data protection has been implemented in personal data processing activities.

Appropriate technical and organizational measures include pseudonymization of personal data, de-identification, and minimization of personal data processing. Necessary safeguards should also be implemented in personal data processing to comply with the GDPR.

Furthermore, the controller shall review and ensure that the default settings of products, services, or applications that process personal data are privacy-friendly. Video surveillance cameras used in public transportation systems are among the applications that require such review. For instance, necessary technical and organizational measures must be implemented to ensure compliance in

- i. the amount of personal data collected,
- ii. extent of personal data processing,
- iii. storage period,
- iv. accountability

Data Protection Impact Assessment (DPIA)

If data collection or processing in any form is likely to result in a high risk to the rights and freedoms of individuals, such as CCTV systems conducting large-scale, systematized monitoring of public spaces, then it is required to carry out a data protection impact assessment. This is because CCTV systems collect personal data while the data subject doesn't know who is collecting their personal data and how that data will be used. It is difficult for individuals to avoid becoming subject of such processing in public areas.

The purpose of a Data Protection Impact Assessment is to identify and minimize the risks to the privacy infringement and violation of personal data protection, and must be performed before personal data processing takes place.

The Data Protection Impact Assessment should include

- i. an evaluation of scheduled processing and purpose of processing
- ii. the necessity of personal data processing and principle of fairness
- iii. risks to rights and freedom of data subject

iv. safeguards to mitigate such risks

The Data Protection Impact Assessment shall also include the opinion of the affected data subject or their representatives. For CCTV systems, it applies to employees or the general public, who are the subjects of monitoring.

Position of the Data Protection Officer (DPO)

Public organizations or organizations that require large-scale, periodic, and systematized monitoring of data subjects must appoint a DPO. According to EU Article 29 Working Party, this also applies to companies that provide CCTV surveillance as a service (SaaS) in public areas, such as shopping centers. On the other hand, it may not apply to private corporations that use CCTV systems to monitor the inside or vicinity of their buildings. If a DPO is not designated because it is not required, then the reasons for this decision should be documented.

It is recommended that the DPO provide advice regarding whether or not to perform DPIA, execution methodologies, executing bodies (in-house or outsourced), safety measures to mitigate risks, and follow-up assessments.

The independence of the DPO from the controller or processor in performing his/her duties must be guaranteed, and the controller is ultimately responsible for DPIA.

Responsibilities of Processors and Outsourced Processors

The controller may have the processor process personal data on behalf of the controller, provided that compliance with the GDPR and adequate technical and administrative safeguards are guaranteed. The controller shall be held liable for the processor's actions, and the processor bears the obligations and responsibilities to respond to requests regarding the rights of the data subject. Therefore, it is essential for the controller to specify the processor's scope of tasks and responsibilities in the personal data processing consignment contract entered into with the processor.

If the processor outsources personal data handling to a secondary processor, then the original processor must acquire written consent from the controller. The obligations arising from the contract with the controller shall be included in the outsource contract. This also ensures that the controller bears responsibilities for the actions of outsourced processors.

Organizations that consign or outsource their CCTV surveillance service should particularly take note of this fact. In addition, organizations seeking to employ

processors that perform cloud-based processing of CCTV surveillance videos should also take note of the above responsibilities of the controller.

Cyber Security Measures to Ensure Adequate Security

The controller is responsible for complying and demonstrating compliance with the principles of integrity and confidentiality, in other words, ensuring adequate security measures against unauthorized/illegal processing, accidental loss/destruction, or damages.

In addition, the controller must implement the necessary security measures within the personal data processing process to ensure compliance with GDPR in the engineering and development process of IT systems. The controller must also implement technical and organizational measures to ensure that the default settings of products, services, application processes (access, transfer, store, release, use, destroy, etc.), and the personal data processing itself is within the minimum scope for the specific purpose of the personal data processing.

As more CCTV system configurations utilize IP-based network cameras, network storage devices; and VMS, leakage, forgery, tampering, loss, and abuse of personal data by hackers or malicious insiders is rising. This increase will naturally result in an escalating risk in breaches of privacy and violations of personal data protection. Therefore, in order to comply with GDPR, the controller must establish or upgrade to CCTV systems that provide enhanced network security, control of internal users, and anti-abuse features.

Actions Taken in Case of Personal Data Breach

Upon becoming aware of a personal data breach, the processor must notify the controller without delay. The controller must then notify the supervisory authority without undue delay and certainly within 72 hours. The controller must also notify the data subject without delay, excluding when

- i. personal data is adequately protected by security measures such as encryption,
- ii. the breach does not significantly affect the rights of the data subject, or
- iii. notifying the data subject involves disproportionate effort.

2.2. Sanctions for GDPR Violations and Ripple Effects

In case of material violation of Principles Related to Processing of Personal Data, consent to collection of personal data, protection of rights of data subjects, or restrictions on transfers to third countries, the greater amount between 4% of the annual global revenue or €20 million will be imposed as a penalty.

For less severe violations, such as violation of responsibilities of notification, the higher amount between 2% of annual global revenue and €10 million will be imposed as a penalty.

For violations on which such penalties are not imposed, other sanctions such as criminal charges may be imposed. In addition, data subjects whose personal data has been breached may claim compensation for damages. Therefore, companies that fail to comply with the GDPR may face significant drops in brand reputation and even potential shutdown of operations. Failure to comply with GDPR may also lead to loss of jobs on an individual level.

That's why all companies, including those already operating in Europe as well as those planning to expand to Europe, must be thoroughly prepared for GDPR compliance. As there is a strong possibility that GDPR will become the global standard of personal data protection, any company that seeks to operate in the global market should pay close attention in the long term.

It is important to note that public CCTV and video cloud services requiring personal data and privacy protection are categorized as a high-risk group, and they may potentially be subject to large fines if violation occurs. Therefore, controllers or processors that provide video surveillance services on European residents within or outside Europe must be thoroughly prepared.

3.1. Principles Related to Processing of Personal Data, Privacy by Design, and Default

3.1.1. Storage Period Limitation and Safe Destruction

In accordance with the principle of the storage period limitation, people, who are in videos that have passed the storage period, shall be unidentified to prevent identification.

To do so, it is advisable to obligate the setting storage period of videos to the storage period specified by law or personal data collection consent agreement to prevent videos from being stored indefinitely and provide an auto-delete feature for videos whose set storage period has expired. Likewise, recording and managing the set storage period, name of video file deleted, deletion time and date, and name of person who set the storage period will ensure transparency in personal data processing.

To ensure lawfulness and transparency of personal data processing, the permission to change the set period or cancel the storage period should only be given to the administrator. The history of matters related to the storage period, such as the newly set storage period, date and time of changes or cancellation of storage period, and person who made such changes, should be recorded and managed.

Hanwha Techwin products provide related features to ensure that videos are not collected or stored beyond the storage period specified by relevant laws or guidelines. For example, in case of network video storage devices, the storage period of video data can be set to a specific number of days (1 - 400) since the day of recording, and video data are auto-deleted sequentially as their set storage period expires.

3.1.2. Audio Recording Restriction

In compliance with the principle of minimization of personal data processing, recording audio using video surveillance systems is restricted. Recording of conversations between individuals poses a high risk of invasion of privacy, so their audio recording is not permitted. However, video surveillance systems on which recording audio data is permitted for public safety reasons require video and audio recording.

Therefore, it is advisable that the audio recording feature be disabled by default, but it should be separately controllable from audio recording. If audio recording

is required, the permission to enable this feature should only be given to a certified administrator.

Changing settings should only be allowed when recording is justifiable. Warnings regarding the audio feature should be displayed, and the history of setting changes, time and date of changes, and person who made changes should be recorded and managed.

In accordance to the Privacy by Default principle, the audio recording feature is disabled on Hanwha Techwin products by default. However, as audio data is an important source that may provide useful information to the CCTV system users, Audio Detection, Sound Classification, Audio Echo Cancellation, and Audio Noise Reduction features are provided by default.

Audio Detection and Sound Classification features are processed in the camera itself without actually recording the audio, and Hanwha Techwin plans to develop intelligent audio analysis technologies such as Sound Location Tracking using multi-channel microphones to cope with customer's various demands. Of course, the restriction of audio for purposes other than audio analysis will be restricted, and the principle of minimization of personal data processing will be maintained.

3.1.3. Restriction of PTZ Recording Beyond Scope of Purpose

According to the principle of minimization of personal data processing, recording and collection of videos in CCTV video surveillance applications should be restricted to relevant situations that meet the purpose of CCTV video surveillance.

Unlike fixed cameras, PTZ cameras are capable of changing direction and even zooming in, which may pose a risk of privacy breaches. Therefore, providing a feature that restricts the panning (horizontal rotation) and tilting (vertical rotation) scope in accordance with the intended purpose to prevent privacy breaches is required.

To ensure transparency and lawfulness of collection and the storage of videos using PTZ cameras, it is recommended that the permitted panning and tilting scope be set by a certified administrator at the time of installation. Furthermore, it is advisable that the permission to change or remove panning and tilting range settings only be given to a certified administrator. The set/cancel history, set/cancel date and time, and person who changed settings must also be recorded and managed. Furthermore, setting the cameras to stop recording or mask videos when the panning and tilting range exceeds the range set by the certified administrator should also be considered.

Just like all our products, Hanwha Techwin's PTZ cameras offer world-leading performance while complying with the principle of minimization of personal data processing. By supporting up to 24 privacy masks, Hanwha Techwin's PTZ cameras maintain high accuracy with privacy masks synchronized to the pan, tilt, and zoom operation, preventing the collection of videos that don't meet the purpose of the video surveillance. Furthermore, PT Limit, which allows camera to only pan and tilt within the range set by the user, is provided by default, preventing the recording of videos beyond the permitted range.

3.1.4. De-identification

The need for de-identification (masking, blurring, mosaic, etc.) of objects (people or vehicle license plates) within CCTV videos varies according to the purpose of video collection and processing environment.

The GDPR does regulate that if it is possible to achieve the objective by processing de-identified data, such as storing video data for the purpose of public interest, scientific, historical research, or statistics, as well as when using the video data without the consent of the data subject for purposes other than the original purpose of collection.

On the other hand, if the request to access is legitimate (e.g., in an emergency or with authorization of law enforcement/judiciary bodies, etc.), but providing the video as-is is deemed to pose risks of infringing the privacy of third parties included in the video, then de-identification of third parties within the video may be necessary.

To minimize personal data processing and maximize privacy protection, ways to provide de-identified videos when monitoring in real time or playing recorded videos depending on access permissions, such as allowing video as-is for administrators (admin account) and only showing de-identified videos for CCTV monitoring personnel (guest/user account), should also be considered. The advantages of such measures provide various benefits including being free from the Personal Data Processing Principle of GDPR, lowering the risks of data subject's execution of rights, and easier compliance and demonstration of compliance with data protection responsibilities by de-identifying the video as soon as possible.

GDPR requires implementation of appropriate technical and organizational measures, such as pseudonymization or de-identification from the design stage to

comply with the principle of Privacy by design and by default. It also requires technical and organizational measures to ensure adequate security in personal data processing. However, the controller should implement appropriate technical and organizational measures by considering the latest technology, cost of implementation, nature and scope of personal data processing, circumstances, purpose, potential impact, severity, and risks of personal data processing on the rights and freedom of the data subject.

For CCTV video surveillance applications, recognizing and de-identifying individuals in every frame of the video poses significant technical, performance, and cost challenges. Therefore, whether or not de-identification is mandatory for achieving the purpose of the CCTV system needs to be determined. If it is not mandatory, the advantages and costs of de-identification should be weighed to determine the need for de-identification.

To protect the privacy of data subjects and achieve the optimal balance of safety and security in CCTV videos, Hanwha Techwin will collaborate with partners to provide a product that streams real-time masked videos when monitoring and products capable of masking people or specific zones when providing backup copies to fulfill access rights.

3.2. Protection of the Rights of Data Subjects

3.2.1. Right to Access

A customer who thought the CCTV cameras installed in a department store felt uncomfortable enquires via their website to confirm that CCTV videos are processed legitimately and to check if he/she was recorded. In response, unless the request of the data subject lacks clear grounds or is excessive, the controller must be able to provide the information necessary to verify proper processing of personal data, as well as the recorded videos of the data subject in an electronic form within one month.

To do so, the controller may ask the requester for information necessary to verify whether he/she is a data subject with the rights to such requests, and detailed information for locating the subject video, such as date, time and location.

In order to easily ensure right to access, the user of the storage device (NVR / DVR or VMS) should access the stored video after authenticating permissions, use an interface and smart search feature for locating the corresponding video accurately and quickly must be provided, and check the video displayed on the

screen and determine if it should be provided as-is or if third parties excluding the requested data subject should be de-identified (masking, blurring, mosaic, etc.).

If the corresponding video only contains the requested data subject, the video can be provided as-is. If third parties exist in the video, then whether there is a risk of privacy breach for the third parties if the video is provided as-is should be determined. As a result of this determination, de-identification should be implemented if it is deemed necessary.

Additionally, information required to verify legitimate processing of personal data includes the recipient of the personal data (recorded video) and storage period. To cope with such requests easily, it is advisable that the storage device creates and stores a list of all users with access to the video, processing history of each video (such as a log recording copying, backup of videos, users who performed such actions, time and date of such actions, the storage period of the video, etc) and a user interface that allows permitted users to easily perform searches and generate electronic files should be utilised.

If it takes a significant period to provide the video data after receiving the request, then it is advisable to take necessary measures to prevent auto deletion when the storage period of the subject video data expires.

3.2.2. Right to Be Forgotten (Right to Erasure)

In CCTV video surveillance applications, while the right to erasure is similar to the right to access in that videos of the individual must be searched, the difference is that complying with the right to access involves retaining the original copy of CCTV video, whereas in the case of the right to erasure requests the original copy of CCTV video is destroyed. Another difference is that right to erasure requests will likely be made after a breach of privacy has already occurred by CCTV video being disclosed to the outside, such as the Internet, by someone.

One example of a right to be forgotten request is as follows. Let's presume that Celebrity A, who lives in a luxury villa, was recorded entering the house with another Celebrity B by the CCTV cameras in the parking lot, and the video was leaked. In this case, A can request erasure of videos containing himself/herself to the CCTV administrator on the basis of breach of privacy. The CCTV administrator must respond to A's request unless it falls into five cases* that can deny the removal request.

5 circumstances where erasure request can be denied

- for exercising rights to freedom of speech and information
- for execution of duties in public interest or execution of legal obligations for exercising duties
- for health-related public interests
- for archiving a purpose in public interest, scientific or historical research, or statistical purposes
- for exercising or defending legal claims

However, if a CCTV image is collected according to a legitimate purpose (e.g., crime prevention and investigation) and processed according to legitimate procedures, the video must be stored for a set period of time to achieve that purpose. Therefore, if an erasure request is made without the CCTV video being leaked first, the response may differ depending on whether the interests, rights and freedom of the data subject is greater than the legitimate reason for storing the video.

If the request based on right to erasure is still deemed legitimate and necessary, it is advisable that the user of the storage device (NVR or VMS) be able to access the stored video after authentication permissions and that the storage device provides a user interface and smart search features for finding the corresponding video quickly and accurately. The user shall check the video displayed on the screen and determine whether to erase it or just mask the requested data subject. If the video only contains the requested data subject, then the video can be deleted. However, if third parties are included and video must be preserved to achieve the purposes of collection and storage, then masking only the requested data subject may be necessary.

On the other hand, if a copy of the video is already leaked on the internet, the data subject may request for any copies of the video to be erased. In this case, the controller must notify the administrator of the website and ensure deletion of the copy.

To cope with such requests easily, it is advisable that the storage device creates and stores the processing history of each video (such as a log recording copying, backup, and erasure of videos, users who performed such actions, and time and date of such actions) and a user interface should be provided to allow permitted users to easily perform searches. Using such systems, the user will be able to track when, by whom, and through which route the video was leaked, making it possible to fulfill the notification responsibilities easily.

3.2.3. Hanwha Techwin Video Analysis Solution

Hanwha Techwin provides a set of tools that ensure easy searching, identification, and collection of individually recorded data through standard products or technology partners.

Using the Facial Recognition, Face Detection, Motion Detection, Video Summary, and Smart Search features provided by Hanwha Techwin, the controller can handle an individual data subject's right to access or right to erasure requests, encrypt the searched results, and forward it to the requester. The next-generation image processing chip set being developed by Hanwha Techwin will feature deep learning-based video analysis technology for identifying a wider range of objects such as people, vehicles, and animals, making it possible to cope with the needs of controllers and processors more quickly.

3.3. Cyber Security Issue Management

3.3.1. Management of Access Permissions

Using only an administrator account with the highest permissions on the system may weaken the security of the entire system if the account is compromised, leading to unauthorized processing, illegal processing, accidental loss, destruction, or damage of personal information. To prevent this, a feature for adding user accounts and restricting the permissions of each account is essential.

In addition, if an intruder attempts to infiltrate or does successfully infiltrate the network device, security incidents such as logging in with administrator permissions, creating unauthorized user accounts, or granting excessive permissions may occur.

To prevent this, Hanwha Techwin provides features for creating users or user groups with various levels and permissions for accessing the camera, recording device, or VMS. Using this feature, the administrator can provide only the minimum functions required by the user, guaranteeing adequate security that prevents abuse of excessive permissions and misuse of personal data.

Hanwha Techwin also provides a variety of log storage and log checking features, including logs about permission grants, changes, and deletions, so that controllers and processors can analyze the intrusion path using device logs or determine how security incidents took place, thus providing an adequate level of security for minimizing personal data breach risks.

3.3.2. Access Control

Various equipment is required to prevent access to devices by intruders. This equipment should include countermeasures against brute force attacks. If the user purchases and uses a password-protected device without changing the default password, then the password can be easily acquired online from user manuals. Users should keep this in mind to avoid critical security breaches.

If the video surveillance equipment is connected to a public network, then the automatic forwarding feature, which enables easy searches in products, can be used as a route for hijacking personal data. If an intruder intentionally factory resets the device to delete logs, it may be difficult to analyze or trace the intrusion route in the future. Therefore, features for storing the access logs is one of the essential features in access control.

In addition, the firmware provided for the video surveillance equipment contains essential information of the equipment and as a result, it should not be possible to analyze from the outside, and a device for verifying the integrity of the firmware distributed by the manufacturer should be included.

Password Policy

To prevent the use of easily predictable passwords, Hanwha Techwin enforces a minimum complexity level of combining letters, numbers, and special characters repetitions (e.g., 1111, aaaa, etc.) and sequences (e.g., 1234, abcd, etc.) are not permitted. By enforcing this password rule, Hanwha Techwin prevents access by intruders through guessing or brute force attacks.

Unauthorized Access Restriction

In order to prevent unauthorized access to equipment, Hanwha Techwin supports IP filtering, which defines the permitted or prohibited network IP range for accessing Hanwha Techwin cameras or recording devices.

Password input is temporarily restricted after 5 unsuccessful login attempts to prevent access through brute force attacks. The system also doesn't allow remote password resets without authentication of administrator rights (local access-only), thus preventing unauthorized access to the equipment.

Safe Connection to Public Network

Hanwha Techwin's policy does not allow arbitrary remote service ports that can be used for shell access such as Telnet, SSH, and FTP server on cameras, recording devices, or VMS. Hanwha Techwin utilizes secure coding without back-

doors in the software codes and conducts continuous testing and monitoring. UPNP Discovery's automatic port forwarding (NAT Traversal) feature, which makes it easy to search for products on a public network, can also be a route to personal data hijacking, so it is also prohibited. It should be noted that the automatic port forwarding feature is permitted on home cameras connected to the cloud to provide services, however it uses random video streaming ports to enhance security.

Storage and Checking of Connection Logs

Hanwha Techwin products log any changes to device's settings, including cameras, recording devices, and VMS, making it possible to find out what changes were made, and by whom, simply by checking the log. Most log entries include both the previous settings and new settings for easy rollback.

In case of cameras and recording devices, the logs are preserved even after a factory reset. The feature that doesn't allow resetting of logs prevents intruders from hiding their tracks by resetting the device, and it can be useful when analyzing and tracing infiltration routes.

Malware Prevention

Firmware used in Hanwha Techwin cameras and recording devices is encrypted, so that the critical information included in the firmware cannot be arbitrarily analyzed, forged, or tampered with. VMS and mobile apps (iOS) are signed with Hanwha Techwin's private key, issued from a trustworthy CA institution. This guarantees that the subject application is distributed by Hanwha Techwin and is free of forgery or tampering by malware. Moreover, the firmware of Hanwha Techwin home cameras is automatically updated to the latest version using a dedicated server, making it easy to improve security and stability.

3.3.3. Safe Transmission

To protect the personal data (user authentication information, video streams) shared within the CCTV system (surveillance cameras, storage devices, and monitoring software), a safeguard for the information transmitted over the network must be implemented.

Hanwha Techwin uses HTTP Digest authentication during HTTP transmissions from cameras, recording devices, and VMS to the server and client to protect the user's password. Use of HTTPS protects the user's password and video streams transmitted via RTSP. However, as HTTPS mode only protects the data

sent in HTTP protocol, such as user authentication information, additional configuration of tunneling RTSP to HTTPS is required on the client end to protect video streams transmitted via the RTSP protocol. Home cameras connected to the cloud use SRTP, a secure media communications protocol based on RTP, to protect the video streams.

3.3.4. Safe Storage

Important system information (including user authentication information) stored in the surveillance cameras, storage devices, and monitoring software must be protected against potential security vulnerabilities or lack of physical security to prevent unauthorized use. Hanwha Techwin uses one-way encryption by hashing user authentication information (password) of cameras, storage devices, and VMS, and stores it safely using two-way encryption if needed.

3.3.5. Safe Release (Backup)

Personal data (video files) stored in CCTV systems (surveillance cameras, storage devices, and monitoring software) should be protected so that it cannot be played or abused arbitrarily by unauthorized users, even if it is released (backed up) from the system.

Hanwha Techwin applies password protection when backing up files to SEC file formation, which is a proprietary backup format, from the storage devices and VMS, and also encrypts the video files. Once the file is encrypted, it cannot be played by unauthorized users, safely protecting personal data even if the video file is leaked. Also, the player (Backup Viewer) required for playing the file is automatically included in the SEC file, which means that users can play the file just by double-clicking on the SEC file without the need to install any additional players.

3.3.6. Prevention of Forgery and Tampering

Personal data (video files) stored in CCTV systems (surveillance cameras, storage devices and monitoring software) should be protected so that it cannot be arbitrarily forged or tampered with by unauthorized users, even if it is released (backed up) from the system.

When files are backed up from Hanwha Techwin's storage devices or VMS in SEC file format, it cannot be opened with normal editing software, preventing

forgery and tampering of the files. Even if a file is forged or tampered with, the video's hash information is watermarked in every frame, which makes it possible to identify specific frames that have been tampered with. And when extracting the video as an SEC file from SSM, which is Hanwha Techwin's VMS, the electronic signature feature is supported. It verifies that the subject video is extracted from Hanwha Techwin SSM and can be used as proof that the video is free of forgery or tampering. The watermarking and electronic signature can be verified by using the Backup Viewer included in the SEC file.

Due to its extra-territorial applicability, expanded scope of personal data, strengthened lawful processing standards, expanded rights of data subjects, personal data breach notification obligations, DPO designation requirements, stronger accountability of corporations, strengthened governance, and enormous fines to prepare for the demands of the times by promoting digital economy, including big data, the impact of GDPR is expected to be significant.

As CCTV video surveillance applications are categorized with high-risk personal data processing that systematically monitors large volumes of personal video data captured in public spaces, Data Protection Impact Assessments (DPIA) must be performed and a Data Protection Officer (DPO) must be designated. For CCTV users or CCTV video surveillance service providers, who operate and manage CCTV video surveillance applications to comply with GDPR, measures must be established to prove their compliance with the principle of accountability, which means compliance with the six principles of personal data processing based on a correct awareness of GDPR.

It must be noted that when the controller and processor of personal data are required to prove compliance with the principle of accountability, it isn't requiring the controller or processor to provide guarantees against personal data breaches, just by implementing the necessary technical and organizational measures. In other words, while controllers or processors bear the initial responsibility for personal data breaches, if they prove the fulfillment of their accountability and become subject to sanctions such as a fine for personal data breaches, the accountability may be transferred to the provider of the CCTV video surveillance system. This would particularly be the case if the provider has guaranteed the safety of systems or technology, but the claim was found to be untrue.

As you can see, from the CCTV video surveillance application point of view, compliance with GDPR isn't an issue that only affects the end users. To effectively prepare for personal data breaches or leaks caused by cyber security issues, the end users, system integrators, and CCTV manufacturers must work closely together.

At Hanwha Techwin, we will continue our unceasing efforts provide privacy-friendly products that process information related to the user and the system and critical video data recorded in a safe manner, based on a correct understanding of and compliance with GDPR (General Data Protection Regulation).

WISENET

Hanwha Techwin Co.,Ltd.

13488 Hanwha Techwin R&D Center,
6 Pangyoro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do
TEL (82) 70.7147.8771-8
FAX (82) 31.8018.3715
<http://hanwha-security.com>

Copyright © 2018 Hanwha Techwin Co., Ltd. All rights reserved

