Honeywell

THE POWER OF **CONNECTED**

GDPR AND ELECTRONIC SECURITY SYSTEMS

2018 White Paper

Table of contents

1/ What is GDPR?

The General Data Protection Regulation (GDPR) is an European regulation under the EU law on the protection of individuals with regard to the processing of their personal data, and on free movement of such data. It replaces the Data Protection Directive 95/46/EC, and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizen's data privacy, and to reshape the way organizations across the region need to approach data privacy. The GDPR is considered the most important change in data protection and privacy legislation in 20 years.

The GDPR is enforceable since May 25, 2018, and its implications will reverberate far beyond the continent itself. It seeks to ensure that personal data is protected against any misuse (including identity theft) and to give back to individuals in the European Union control over how data relating to them is being used. Any entity that is established in the European Union or that processes the personal data of individuals in the European Union to offer them (online) goods or services, or to monitor their behavior—whether as customers, employees, or business partners—will be affected. Any failure to comply with the regulation could, amongst other penalties, incur severe reputational damage as well as financial fines of up to 4 percent of annual worldwide revenues.

This document sets out an overview of the key elements of the GDPR requirements and how these requirements will be applicable for end users of Honeywell security solutions (acting as data controllers) or for installers and integrators, when processing individuals' personal data.

.

1-1/ Personal Data and Processing

The GDPR only applies when processing personal data. "Personal data means any information relating to an identified or identifiable natural person (called the data subject); an identifiable 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" (Article 4, GDPR). This implies that personal data is any information that could be used to identify a person.

Examples of personal data are identification data such as name, picture, email address, phone number, physical address or personal ID numbers, like a bank account number or a social security number. But also, any information that could be used to identify a person such as location data, mobile device IDs, IP address, and biometric data are to be defined as personal data. In addition, data that can be re-identified with reasonable effort by combining it with additional information is considered personal data.

Biometric data is a special category of personal data requiring a stricter data protection regime. Biometric data is personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (identification by comparison of fingerprints) data.

Biometric data processing is now often used in automated authentication or verification and identification procedures, in particular, for the control of entry to both physical and virtual areas as used in some of our Honeywell security solutions. Biometrics includes physiological characteristics of a person and behavioral-based characteristics.

- **Physiological characteristics:** fingerprint verification, finger image analysis, iris recognition, retina analysis, face recognition, outline of hand patterns, ear shape recognition, body odor detection, voice recognition, DNA pattern analysis, and sweat pore analysis, etc.
- **Behavioral-based characteristics:** hand-written signature verification, keystroke analysis, gait analysis, etc.

Other types of special personal data are genetic data and health data, but these are not covered by this paper as they are not relevant to our security solutions. In addition to the concept of personal data, there must always be a processing operation to trigger the GDPR requirements. Data Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (Article 4, GDPR). Most end users will carry out some amount of data processing as part of their security systems.

1-2/ Controller and Processor

The two most important roles within the GDPR are for the Data Controller and Data processor

Data Controller

A **Data Controller** is the natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. (Article 4, GDPR). Most end users of security systems will be data controllers under this definition. They will need to identify and codify the purpose of their security systems, the reasons for capturing and processing personal data and the controls and processes they have in place to safeguard and manage that data appropriately. Honeywell security solutions have features and functionalities which can help support end users to put in place GDPR compliant systems.

Data Processor

A **Data Processor** is a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller (Article 4, GDPR). Integrators or manufacturers providing on-premise security solutions could be considered data processors if they directly handle data under the (written) instructions and on behalf of the end user. For example, if an integrator accesses an end user's video recording data for maintenance purposes, the integrator may be considered a data processor under the GDPR. Cloud security solution providers who host and store personal data on behalf of an end user are also likely to be considered data processors. Honeywell has taken specific care with the MAXPRO® Cloud hosted solution to ensure it can provide a GDPR compliant offering as a data processor.

1-3/ Guiding Principles

The GDPR is based on principles rather than exact rules. The onus is on individual companies or organisations to determine implementation in their particular context. So an end user, as a data controller, needs to consider these aspects with regard to their own particular circumstances and requirements.

Lawfulness: Data should be processed only when there is a lawful basis for such processing (e.g., consent, contract, legal obligation, or the Data Controller's legitimate interest).

Fairness: The organization processing the data should provide data subjects with sufficient information about the processing and the means to exercise their rights.

Transparency: The information provided to data subjects should be in a concise and easy to understand format and cannot be buried in a lengthy document of terms and conditions).

Purpose limitation: Personal data may be collected only for a specific, explicit, and legitimate purpose and should not be further processed.

Data minimization: The processing of personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which those data are used.

Accuracy: Data should be accurate and kept up to date.

Storage limitation: Data should not be held in a format that permits personal identification any longer than necessary.

Security: Data should be processed in a manner that ensures security and protection against unlawful processing, accidental loss, damage, and destruction.

Accountability: The data controller is responsible for demonstrating compliance with all GDPR principles and obligations (as further set out below).

2/ Rights and Obligations under GDPR

In view of the accountability principle, you need to respect, as a Data Controller, the data subjects' privacy rights and other Data Controller obligations.

2-1/ Data subject rights

The GDPR dedicates a whole chapter to data subjects' rights which controllers are required to honour. The intention is to strengthen and expand data subjects' rights compared to rights granted to them under the old Data Protection Directive. Infringements of the provisions relating to data subjects' rights are subject to the maximum level of fines under the GDPR. Controllers would, therefore, be prudent to prioritize compliance with these obligations.

The GDPR expands data subjects' rights existing under the Directive such as the right to access, right to rectification and right to object. In addition, it introduces important new rights for data subjects, including the right to erasure (or the right to be forgotten), the right to data portability and certain rights in relation to profiling. However, note that these rights are not always absolute. In accordance with the GDPR, controllers will, in any case, be required to provide significantly more information about their processing activities to data subjects.

Set out below is an overview of the different data subjects' rights.

2-1-1/ Information rights

In order to guarantee fair and transparent processing, the GDPR explicitly requires data controllers to communicate with data subjects and provide them, before the actual data processing, information about their data processing activities in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

More specifically, controllers must provide the following information to concerned data subjects (Article 13 GDPR):

- The identity and the contact details of the controller and data protection officer, where applicable;
- The processing purposes and legal basis for processing (and where applicable a description of the data controller's legitimate interest);
- The categories of recipients of the personal data, if any;
- The intention of transferring the personal data outside the EU;
- The period for which personal data will be stored;
- The data subjects' rights, including the rights to request from the data controller access to and rectification or erasure of personal data, or restriction of processing concerning the data subject or to object to data processing in certain cases (such as direct marketing), as well as the right to data portability;
- The right to withdraw consent at any time (if applicable);
- The right to lodge complaints with the competent supervisory data protection authority;
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether data subjects are required to provide the data and the possible consequences for failing to provide data;
- The existence of automated decision making (including profiling), as well as the logic involved and the significance and envisaged consequences of such processing for the data subject.

As data controllers, End users need to set out the above information requirements in a privacy policy or prior statement to be communicated to the concerned staff, visitors, customers, and other impacted parties. In addition, the data controller should also verify whether no (additional) national information requirements apply, such as the required use of pictograms when installing a camera surveillance system.

2-1-2/ Access requests

Data subjects have the right to request access to their personal data that is being processed by a data controller. In this case, the GDPR sets out a list of information that controllers must provide (Article 15 GDPR), including a copy of the personal data undergoing processing (if possible and not adversely affecting the privacy rights of others). When dealing with access requests, under Article 12 GDPR, data controllers must:

- Put in place processes for facilitating the data subject's exercise of their rights, including processes for making requests electronically;
- Deal with access requests free of charge, subject to an exception for manifestly unfounded or excessive requests;
- Respond to access requests without undue delay, and at the latest within one month, subject to a two-month extension for complex requests or for a large number of requests;
- Use all reasonable measures to verify the identity of data subjects requesting access before granting access.

2-1-3/ Right to rectification

Data subjects also have the right to rectification under the GDPR. This requires data controllers to rectify inaccurate personal data and complete incomplete personal data upon a data subject's request (Article 16 GDPR).

2-1-4/ Right to object

Under the GDPR, data subjects will have broader rights to object at any time to data processing activities on grounds relating to his, her or their particular situation, if the data processing is based on his, her or their consent, or the data controller's legitimate interest. In this case, the controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defense of legal claims. In addition, data subjects retain their right to object to processing of their personal data for direct marketing purposes (Article 21 GDPR).

2-1-5/ Right to erasure

The GDPR also contains a right to erasure (also referred to as a 'right to be forgotten'). Data controllers will be required to erase personal data upon request and without undue delay if:

- The data is no longer necessary for the purpose for which it was collected or otherwise processed;
- The processing is based on the data subject's consent and the data subject withdraws his, her or their consent;
- The processing includes any automated decision-making (such as profiling) and there are no overriding legitimate grounds for the processing;
- The personal data has been unlawfully processed;
- The personal data has to be erased for compliance with other EU legal obligations to which the controller is subject (Article 17 GDPR).

2-1-6/ Right to data portability

The GDPR also introduces a new right to data portability. To the extent data subjects have provided their personal data to a controller, and the controller processes that data by automated means and on the basis of consent or a contract, data subjects may require the controller to provide them with their personal data in a structured, commonly used and machine-readable format- and, where technically feasible, transmit that data directly to another controller (Article 20 GDPR).

2-1-7/ Right to restriction of processing

Data subjects also have the right to restrict the processing of personal data if:

- a data subject contests the accuracy of personal data and the controller is in the process of verifying the accuracy of the data;
- the processing is unlawful and the data subject requests the restriction of the processing rather than an erasure of the data;
- the controller no longer needs the personal data for the purposes of the processing, but it is required by the data subject for the establishment, exercise or defence of legal claims;
- the processing is based on the controller's legitimate interest to which the data subject has objected and the data controller is in the process of verifying whether its legitimate grounds override those of the data subject (Article 18 GDPR).

2-2/ Data controller obligations

2-2-1/ Be accountable

Accountability is the big hype word introduced by the GDPR and it's all about documentation. In practice, accountability means that a data controller needs to be able to show compliance with the GDPR by documenting all data protection requirements in different processes and procedures. More specifically, data controllers will amongst others, as from May 25th, 2018, need to implement and document how they implement the principles "data protection by design" and "by default" (Article 25 GDPR), keep a record of their processing activities (Article 30 GDPR), assess and document their technical and organizational security measures (Article 32 GDPR), register any personal data breaches (Article 34) and conduct data protection impact assessments where applicable for more risky data processing activities (Article 35 GDPR).

2-2-2/ Implement Privacy by Design and Privacy by Default

The principle of data protection (or privacy) by design, is that privacy controls are to be embedded in the design of business operations, processes, products, and services. The principle of data protection by default contemplates controllers applying the strictest privacy settings, for example, to a product or service and that only the data which is necessary to achieve the defined purposes can be processed (i.e. data minimization). The aim is that controllers prevent, as far as possible, privacy risks from occurring (Article 25 GDPR).

2-2-3/ Take care when using third parties

One of the key changes in the GDPR is that data processors have direct obligations for the first time. These include an obligation to: maintain a written record of processing activities carried out on behalf of each controller; designate a data protection officer where required; appoint a representative in certain circumstances; and notify the controller on becoming aware of a personal data breach without undue delay.

In addition, the GDPR provides for a minimum set of mandatory wording that needs to be included in a contract concluded between a data controller and a data processor (Article 28 GDPR).

2-2-4/ Keep records of processing

- Each data controller is required to maintain a record of processing activities under his or her responsibility;
- Each record needs to contain a minimum set of information, including, amongst others, the purposes of the processing;
- A description of the categories of data subjects and of the categories of personal data;
- The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries outside the EU;
- Where applicable, transfers of personal data to a third country outside the EU, including the identification of that third country and the related documentation of suitable safeguards;
- Where possible, the envisaged time limits for erasure of the different categories of data;
- Where possible, a general description of the technical and organisational security measures;
- All records need to be made available to the supervisory data protection authority on first request (Article 30 GDPR).

2-2-5/ Inform the data subjects

Data controllers must provide transparent information to data subjects. This must be done at the time when the personal data is obtained. For example, the information to be provided is more comprehensive than previously and must inform the data subject of certain rights (such as the ability to withdraw consent) and the period for which the data will be stored. Controllers will need to consider their forms of fair processing notice with these new obligations in mind, and check that they are providing the information in a clear way and in an easily accessible format (Article 13 and 14 GDPR).

2-2-6/ Ensure appropriate data security

In accordance with Article 32 of the GDPR, controllers (and also processors) will be required to implement appropriate technical and organisational security measures ensuring a level of data security which is proportional to the risks inherent in the data processing for the rights and freedoms of individuals. Complying with this obligation will require a detailed security assessment of various factors, including the purposes of data processing activities, potential risks, the state of the art of security, and implementation costs.

72 hours

2-2-7/ Notify Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. The controller must notify the competent EU supervisory authority about personal data breach without undue delay and no later than 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk for the data subjects (Article 33 GDPR). The controller must also send a notice about the breach to the data subjects when the personal data breach is likely to result in a high risk for the data subjects (Article 34 GDPR). This is, however, not needed in cases where the controller has taken measures to prevent any risk involved in the breach to the data subjects, for example, by encrypting the data. The processor must notify the controller about any personal data breach without undue delay.

2-2-8/ Conduct Data Protection impact assessments (DPIA)

Controllers may be required to undertake pre-processing **Data Protection Impact Assessments** (DPIA), which are required if the processing is likely to result in a high risk to an individual's rights (Article 35 GDPR), and which may require pre-processing consultation with the relevant supervisory authority (Article 36 GDPR). Such high-risk processing includes profiling, large scale processing of sensitive categories of personal data, and may arise where there is a systematic monitoring of a publicly accessible area on a large scale (in the case of camera surveillance systems) and innovative use of technological solutions.

2-2-9/ Appoint a Data Protection Officer where specified

In certain circumstances, data controllers (and processors) must designate a Data Protection Officer (DPO) as part of their accountability program. The designation of a DPO is needed in any case where :

(i) the processing is carried out by a public authority;

(ii) the core activities of the controller (or processor) consist of processing operations which, by their nature, scope or purposes, require regular and systematic monitoring of data subjects on a large scale, or;

(iii) the core activities consist of processing on a large scale of special categories of personal data (such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation) or personal data relating to criminal convictions and offences.

The DPO will need sufficient expert knowledge. This will depend on the processing activities for which he or she will be responsible (Article 37 GDPR).

2-2-10/ Fines

The GDPR establishes a tiered approach to penalties for breach enabling the competent data protection authorities (DPA's) to impose fines for some infringements of up to the higher of 4% of annual worldwide turnover and €20 million (e.g.: for breach of requirements relating to international transfers or the basic principles for processing, such as conditions for consent). Other specified infringements would attract a fine of up to the higher of 2% of annual worldwide turnover and €10 million.

upto 4% 20€ MILLION

3/ A GDPR Compliant Video Surveillance System

As all video surveillance systems can capture and collect identifiable information in the form of video footage and images, organizations deploying video surveillance systems are required to be GDPR compliant.

In accordance with the GDPR, Video Surveillance End Users are in most cases to be considered as data controllers. Cloud providers storing personal data (including video images) on behalf of an end user are likely to be data processors. Integrators or manufacturers could also be considered data processors if they directly handle video recording data on behalf of the end user. For example, if an integrator accesses an end user's video recording data for maintenance purposes, the integrator may be considered a data processor under the GDPR. In a video surveillance system, personal data includes not only video footage, but also video analytics results such as facial or age recognition. The Data Subjects are the people being recorded on camera.

Before implementing a video surveillance system

Being compliant with the GDPR starts with GDPR awareness, the understanding of data subject rights, choosing the proper legal ground for lawful processing of all data processing activities and implementing the GDPR principles. In this connection, the data controller should first assess the main data protection requirements for a video surveillance application before implementing the system. This assessment should cover key areas such as:

- Defining the purposes of the envisaged data processing operation;
- Choosing the correct legal ground to process the personal data concerned;
- Defining the minimum set of necessary data to be processed;
- Setting retention periods;
- Support for the data subjects' rights, including informing the data subjects before implementing the video surveillance system;
- Implementing Privacy-by-design;
- Keeping a record of the concerned data processing activity;
- Conducting a Security risk assessment;
- Evaluating third-party risks.

In addition, a video surveillance system which includes systematic monitoring of a publicly accessible area on a large scale (Article 35, GDPR) is subject to high-risk processing operations, and has additional requirements under GDPR. In this case, a data protection impact assessment is required, and a DPO needs to be appointed.

After the assessment, the controller will be able to identify and prioritize the risks, and plan the strategy for GDPR compliance related to their video surveillance system.

Key GDPR points for a video surveillance system

Honeywell provides a range of video surveillance solutions covering both on-premise and cloud-based solutions. These start with our Performance range targeted at the small to medium business market, extend through our ADPRO XO offerings all the way to our high-end MAXPRO® VMS and MAXPRO® NVR Enterprise level solutions. Working with equipment from reliable partners such as Honeywell, can greatly improve the ease with which a data controller can ensure their video surveillance system is GDPR compliant.

Listed below you will find an overview of the key requirements and areas where Honeywell equipment can assist end users to implement GDPR compliant video systems. Cloud-based systems, including the Honeywell MAXPRO® CLOUD solution, are discussed in more detail in section 6.

3.1/ Privacy by design

Honeywell is building privacy and data protection requirements, as well as controls into the core development, architecture, and functionality of its products and solutions rather than just adding privacy and data protection controls to an existing application. For this, Honeywell has collaborated with third-party consulting partners to review all its product offerings, and has set up a separate privacy impact assessment process – to protect privacy throughout the whole life cycle of new products and solutions. In addition, Honeywell is also focusing on the development of new features to protect personal data processed by its products and solutions – based on the latest AI and IT technologies.

One approach which can reduce privacy risks and assist end users to fulfill their GDPR requirements, is the use of IT security techniques – "pseudonymization" and "anonymization" – available within some Honeywell offerings. More specifically, Honeywell includes in its MAXPRO VMS IP video solutions like "people blurring" and "people pixelization", and capabilities to support the principle of privacy by design. In this type of application, the video system blurs people's faces in live-view to preserve privacy during the normal course of events. However, with appropriate '4-eye' dual authentication, the playback video can be seen in the original format – if there is a legitimate reason to reveal people's identity (e.g.: if a crime has been committed). The Honeywell '4-eye' dual authentication control mechanism is designed to achieve a high level of data protection and security for especially critical operations. Under this mechanism, all playback of the video in the original format requires the presence of two authorized people from two different groups. This type of control mechanism helps to ensure the privacy of individuals, especially during investigations – or when access or rectification is requested by the data subject.

3.2/ Response to data subject rights

As already indicated, the GDPR consists of a range of different rights for data subjects. When video surveillance applications and services are being used, individuals have the right to protect their own personal data and control the digital footprints they leave behind in those systems.

End users need to address these rights by informing their staff, visitors, customers, and other impacted parties through appropriate signage and prior notification – in order to ensure that all concerned individuals are aware that video footage is being taken in a particular area.

In addition, the end user needs to set up a procedure to deal with and manage any type of access request. In case such an access request is valid and the images recorded on the video system need to be provided, it first needs to be checked whether other individuals are visible in the footage. If so, in the future they can be blurred or made unrecognizable by pixelization (if needed) through the Honeywell footage redaction solutions.

Honeywell IP video solutions offer the function to export video clips to help ensure easy and appropriate response to any access request. The Honeywell planned smart search function in the MAXPRO series goes further in terms of improving incident investigation. For example, the smart search feature allows data controllers to search for a person's relevant appearances across multiple camera recordings by using a face photo or a snapshot, and find all relevant video clips for the specific person automatically – saving significant amounts of time, sifting through video by hand. When data subjects request access to or want to erase their personal data, the smart search feature can help to quickly locate the video clips in response to the data subject's request.

3.3/ Data Collection

GDPR has a significant effect on how video surveillance systems collect, store and secure personal data. Any personal data collected by a video surveillance system should be processed in a fair and lawful way, and only for specified, explicit and legitimate purposes implying that this data cannot be further processed in a manner that is incompatible with those purposes (purpose limitation). Video surveillance systems should thus only collect personal data that is adequate and relevant, and should minimize the collection of any useless or irrelevant data (data minimization). These principles of purpose limitation and data minimization are relevant not only to reduce privacy intrusions, but also can facilitate more intelligent and efficient use of video surveillance resources. Honeywell solutions offer three types of recording:

1- Continuous recording: cameras can record all the action 24/7, so you can rewind any camera to any minute of any day and catch everything you missed.

2- Event recording: many events inherently trigger recording in the Honeywell MAXPRO NVR and other Honeywell video solutions, including motion, PTZ operations, video loss, etc. And the events can be configured based on customer requirements.

3- Scheduled recording: this allows you to program the recorder, so that it starts at a specific time, performs a required task (such as record or playback a file), and closes automatically.

- Using an appropriate mixture of continuous, event recording and scheduled recording provides the data controller with the ability to minimize the processing and storage of unnecessary personal data, and be compliant with the data minimization principle.
- Event based recording, where there is only recording upon an intrusion (for example in perimeter protection applications), is very clearly following an approach which is based on both the legitimate purpose and data minimization principles.

3.4/ Technical and organisational security measures – including data security

In order to protect the data collected through a CCTV system, the end user must, as the data controller, implement appropriate technical and organizational security measures to ensure a level of data security, taking into account: the state of the art technology, the costs of implementation and the nature, scope, context and purposes of processing, as well as the varying likelihood and severity of risk for the rights and freedoms of natural persons. Honeywell solutions can assist the end user in implementing such measures. The organizational security measures which Honeywell can assist with include log management, account management, verification procedures, and access management.

Log management: With Honeywell IP video solutions, the end user is able to keep a record of any data processing operation performed within the system and to safely store these so-called 'log files' with encryption (in order to prevent any breach of sensitive information). Log files also contain personal data. Consequently, all GDPR requirements also apply to any log file.

Account management: Honeywell IP video solutions provide adaptability to different environments empowering organizations to choose which user or group of users can have access to and manage different profiles. As part of their system set-up process, the end user needs to define appropriate levels of access to the system for different users or user groups. Honeywell solutions then enable the controller to easily grant users the appropriate level of permission to view, access, search, export, delete, or make corrections (as required).

Verification procedures: Within Honeywell IP video solutions, user account and password information are kept secure using appropriate encryption and pseudo-random technologies. In some solutions, like MAXPRO VMS, end users can also deploy Honeywell four-eye password settings as an extra level of security to determine the legitimacy of log-ins, and keep personal data safe.

Access management: Data should only be disclosed on a "need-to-know" basis. Honeywell IP video solutions protect access to personal data through well-designed privilege control systems (including password and account management controls). The end users can set up the system so that they get notification if there has been an attempted access by a non-authorized account (user). In addition, Honeywell solutions require authentication for the export of data from SD cards in cameras, as well as from the core network or digital video recorders.

In addition to the organizational security measures to be taken, Honeywell solutions provide assistance in implementing the appropriate ***technical security measures***.

Data encryption is one of the most important technical security measures suggested by GDPR. In this connection, the GDPR can punish organisations that fail to leverage appropriate protection as a part of their overall security posture. Honeywell has developed a robust system for considering data security at the outset of product conception and ensures this flows through the whole development process. Some examples are shown below:

- **Secure Data Transmission:** In a video system, data may transfer through an untrusted or unsafe network. Honeywell uses the HTTPS protocol to provide bidirectional, encrypted communication between devices and systems. Please check the Honeywell web page https://mywebtech.honeywell.com/Account/Login for the latest list of products supporting HTTPS encryption. For products without HTTPS encryption capability, care should be taken to avoid use in untrusted networks, or to install them behind firewalls to mitigate potential risks. Honeywell also offers password protection on RTSP and video streaming over TCP TLS to ensure data security.

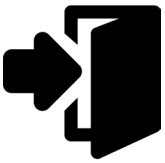
- **Data encryption:** Honeywell leverages the Advanced Encryption Standards (AES) specification to protect IP communications. AES is a specification for data encryption which has been adopted by the U.S. government to protect classified information and has since been adopted worldwide. In the AES specification, 128-bit and 256-bit keys are used for encryption and decryption to protect critical data. 128-bit keys create 3.4×10^{38} possible combinations and 256-bit keys create 1.1×10^{77} possible combinations. Fifty supercomputers which could check a billion billion (10^{18}) AES keys per second would require about 3×10^{51} years to exhaust the number of possible 256-bit key combinations.

- **Crypto Chipset:** Amongst its range of IP video solutions, Honeywell offers cameras with hardware-based ultra-secure key storage to ensure that a product with the consumables it uses, firmware it runs, accessories that support it, and the network nodes it connects to, are not cloned, counterfeited, or tampered with. With the Crypto Chipset, attackers cannot see the secret keys that are stored in the protected hardware. This helps to prevent third-party attacks, and data breaches – ensuring the confidentiality and integrity of the data.

3.5/ Data Retention

A retention period is the period of time which a business or organization identifies as necessary for its purposes to keep personal data. This may be driven by industry regulations or business requirements. Although the installation of cameras might be clearly justified for security purposes, the timely and automatic deletion of the footage is still essential. Where personal data is concerned, the basic data retention rule is that data cannot be longer kept than is necessary for the purposes for which this data is processed. Consequently, end users should have clear policies regarding the use of video surveillance on their premises including retention periods. In general, the national camera surveillance laws foresee a legal retention period, which typically is around 30 days. If you believe that you need to retain video data for longer, then you should first check whether this is legal and if so, document for which purpose, how long and the (business) rationale for this.

With Honeywell IP video solutions, the storage duration for video footage can be set by end users, based on their different requirements. End users can set retention limits when setting up the system to ensure best practice. They can also remove recorded files automatically based on storage duration settings. This all helps the end user to better comply with their data retention obligations.



4/ A GDPR Compliant Physical Access Control System

Before implementing an access control system

The same approach towards GDPR as taken with video surveillance systems needs to be taken with access control systems. As with video, Honeywell also provides a range of "on-premise" and cloud-based access control solutions. The cloud-based solution, MAXPRO CLOUD is discussed in more detail in section 6. The "on-premise" solutions (which meet various market segments) are: IQ-MultiAccess, NetAXS, Pro-Watch, and WIN-PAK. While NetAXS serves access control applications with no need for a computer, the IQ-MultiAccess, Pro-Watch and WIN-PAK solutions are computer-based systems that can provide integration to intrusion and video systems.

Before implementing an access control system, the end user will need to do a similar assessment to that for a video surveillance solution – again considering all the GDPR principles including data subjects' rights and the proper legal ground for lawful processing of all data processing activities.

4.1/ Privacy by design

In principle, Honeywell access control systems do not require the processing of personal data (as defined by the GDPR) by the system, to provide their integrated security functions. All access control and/ or security functions can operate on a purely numerical basis, with only a cardholder number being given permissions to specific features and functions of the system.

However, an end user may choose to enter specific data to meet their business and security needs. For example, if the end user chooses to enter personal data into a cardholder record, it is the responsibility of the end user to ensure that it has a legal ground (such as the end user's legitimate interest), to do so. In all cases, the end user will be required to inform the concerned individuals in advance on the processing of their data, including amongst others, the type of data being processed and how this data will be used (reports, emergency notifications, sending access credentials to an email supported by a mobile device etc).

4.2/ Response to data subject rights

Upon receipt of a request from a data subject, the end user can use the Honeywell access control system to generate a cardholder report showing the data associated with the data subject. The report can be printed or provided electronically (emailed) to the data subject. As with video systems, it is the responsibility of the end user to set up and manage a system to validate and then process data subject requests appropriately.

The above report can be used by the data subject for means of data portability or to review for data accuracy. If the data subject requests the end user to make data corrections (again the requesting process for corrections is the responsibility of the end user), the end user can edit any of the existing cardholder data fields in the access control system and repeat the above report to provide to the data subject confirmation of the requested changes.

The data subject can request the end user to delete their personal data in accordance with the right to be forgotten (the requesting process is the responsibility of the end user). The end user can delete data fields or delete the entire card holder from the system. Appropriate processes need to be set up to ensure this is managed in an effective and appropriate way.

4.3/ Data Collection

As highlighted under section 4.1 above, personal data does not need to be used in Honeywell access control systems. If the end user chooses to enter personal data into a cardholder record, they need to ensure that they minimize the collection of data and focus on data which is sufficient and relevant for purpose.

4.4/ Technical and organisational security measures – including data security

As with video, Honeywell access control solutions protect data through well-designed password and account management controls. Data encryption is also standard. Upon entering card holder data in the access control system, this card holder data, (including printing of photo(s) and signature(s) on a card) is automatically encrypted by the system. In addition, the related database and communication to user interfaces or web browsers are also encrypted. Where video integration is used, both live and retrieved video images can be configured for "four eyes" permission to unmask people faces (as already explained under Section 3.1).

4.5/ Data Retention

Once the end user has defined their data retention approach, Honeywell access control systems' scheduler tools enable the end user to work on their documented plan. Data retention and deletion can be accomplished by the end user using the scheduler configured to purge deleted records and/ or History on a schedule definable from 1 to 999 days. The schedule can be run hourly, daily, weekly, once per two weeks, or monthly and multiple schedules can be created to run in a staggered manner.

Similarly, video recorders used in integrated systems can be configured to overwrite after xx amount of days to ensure the right to be forgotten. It is recommended for the end user to purge deleted records and history before 30-days to minimize risks associated with GDPR compliance. The NetAXS solution automatically meets the right to be forgotten requirement as soon as the user data is deleted, leaving only card history events containing the card holder's last name until the history event buffer is overwritten.

IQ-MultiAccess Cardholders that have not used their badges for a configurable amount of days can be deleted automatically by a scheduler. The access control log of IQ-MultiAccess can be configured to store all events in a format which is automatically anonymized

As with video systems, Honeywell access control solutions provide significant functions and features which can support an end user in the implementation of a GDPR compliant system. However, these need to be part of a wider application of appropriate systems and processes clearly linked back to the GDPR principles.

5/ A GDPR Compliant Intruder Detection System

Before implementing an intrusion detection system

The processing of personal data within the Honeywell Electronic Intruder Detection Systems is also subject to the GDPR. Before implementing an intrusion detection system, the end user needs to do a similar assessment to that of a video surveillance or access control system - considering the data subjects' rights, the proper legal grounds for lawful processing of all data processing activities and the GDPR principles to be implemented.

Honeywell provides a range of "on-premise" intruder solutions including both physical on-site products and PC solutions that can be used on site or off site. Honeywell Intruder products also connect to our cloud-based solution MAXPRO Cloud as discussed in section 6. The "on-premise" solutions (which meet various market segments) are: Galaxy and MB. Both Galaxy and MB systems are supported by PC and Mobile App based software solutions for configuration and end user management (Galaxy Remote Service and User Management Suite, MB IQ Panel Control and IQ-SystemControl, GX Remote Control and MB Remote apps).

The areas where Honeywell equipment can assist end users to implement GDPR compliant intrusion detection systems are very similar to that of Access control. In many instances, no personal data will be processed at all, so GDPR compliance requirements could be very limited.

5.1/ Privacy by design

In principle, there is no processing of personal data (as defined by the GDPR) required to operate Honeywell intruder control systems, except for the GX Remote app push notification service.

The Honeywell GX Remote Control app push notification service, used with Galaxy systems, stores a unique identifier for each end user's mobile devices for the period of usage. Although this unique identifier is not directly linked to any end user identification data, it might be possible for the end user to indirectly identify the individual using the GX Remote Control app push notification service behind this unique identifier. Once the end user turns off the notification service the data will, however, be deleted or anonymised. Honeywell will also not distribute the data to any third parties.

Users of MB systems, through IQ-SystemControl, may additionally choose to enter specific data to meet their business and security needs. As with access control systems, if the end user/data controller chooses to enter personal data into a user's record, it is the responsibility of the end user to ensure that it has a legal ground (such as the end user's legitimate interest, etc.) to do so. In all cases, the end user will also be required to inform the concerned individuals in advance on the processing of their data, including amongst others the type of data being processed and how this data will be used.

5.2/ Response to data subject rights

Honeywell Intruder Detection systems enable the data subject's right to access to be met by means of the end user generating a user database report through the system. This can be printed or provided in electronic form to the concerned data subject. In addition, this electronic form can also be used to meet any request related to the right of data portability.

Finally, the data subject can exercise their right to data correction and submit a change request to the end user to correct any errors. The end user can then edit or delete data fields or delete the entire data subject from the system. As with video or access systems, it is the responsibility of the end user to set up and manage a system to validate and then process data subject requests appropriately.

5.3/ Data Collection

As highlighted under section 5.1 above, personal data does not need to be used in the Honeywell intrusion detection systems. If the end user/data controller chooses to enter personal data into a user's record, they need to ensure that they minimize the collection of data and focus on data which is sufficient and relevant for purpose.

5.4/ Technical and organisational security measures – including data security

In Honeywell intrusion detection systems where it is possible to add additional personal data, such as IQ-SystemControl, these systems have similar safeguards to Honeywell access control systems. Upon entering end user's data in the Intruder Detection system, this end user data is encrypted by the system, as is the related database and communication to user interfaces or web browsers.

5.5/ Data retention

Once the end user has defined their data retention approach, the Honeywell IQ-SystemControl scheduler tool enables the end user to work on their documented plan. Data retention and deletion can be accomplished by the end user using the scheduler configured to purge deleted records and/or History on a schedule definable from 1 to 999 days. The schedule can be run hourly, daily, weekly, once per two weeks, or monthly and multiple schedules can be created to run in a staggered manner.

Similarly, video recorders used in integrated systems can be configured to overwrite after xx amount of days to ensure the right to be forgotten. It is recommended for the end user to purge deleted records and history before 30-days to minimize risks associated with GDPR compliance. IQ-SystemControl automatically meets the right to be forgotten requirement as soon as the user data is deleted, leaving only card history events containing the end user's last name until the history event buffer is overwritten.

IQ-SystemControl users that have not used their badges for a configurable amount of days can be deleted automatically by a scheduler. The IQ-SystemControl log can be configured to automatically store all events in a format which is automatically anonymized.

As with video systems, Honeywell access control solutions provide significant functions and features which can support an end user in the implementation of a GDPR compliant system. However, these need to be part of a wider application of appropriate systems and processes clearly linked back to the GDPR principles.

6/ A GDPR Compliant Cloud Security System

MAXPRO Cloud Security System is a Honeywell hosted cloud solution which provides end users with the potential to run their intrusion, access control or video systems or a combination of all three through the cloud. Since Honeywell is the host of the MAXPRO Cloud solution and stores personal data on behalf of an end user, Honeywell acts as a data processor. Honeywell has taken specific care with the MAXPRO Cloud solution to ensure it can provide a GDPR compliant solution as a data processor.

To assist its customers in their GDPR compliance strategy, the Honeywell MAXPRO Cloud system addresses the following main GDPR requirements and principles:

6.1/ Privacy by design

As already indicated, pseudonymization and anonymization are two of the IT security techniques which are strongly recommended by the GDPR to be implemented in order to reduce any privacy risks.

Honeywell utilizes anonymization, masking, video people blurring and face pixelization capability to support privacy by design. Personal data (as defined by the GDPR) accessed by end users is anonymized and masked and then stored in the Cloud as per the required retention period. After this retention period, the personal data is deleted.

6.2/ Response to personal rights

The GDPR ensures that rights are given to individuals to protect their own personal data and control the digital footprints they leave behind.

As with any other video, access or intrusion system, end users need to address these rights by informing their staff, visitors, customers and other impacted parties through appropriate signage and prior notification in order to ensure that all concerned individuals are aware of how the security system may be impacting them – particularly when video footage is being taken in a particular area.

The end user also needs to set up a procedure to deal with and manage any type of access request. End users gain access to Honeywell cloud after accepting and giving consent to legal terms and conditions and then have the ability to export video clips, reports etc. on individual requests as with a non-cloud solution. This helps ensure easy and appropriate response to the right to access requests.

6.3/ Data Collection

GDPR has a significant effect on how security systems collect, store and secure personal data. Any personal data collected by video surveillance, access control and intrusion systems should be processed in a fair and lawful way, and only for specified, explicit and legitimate purposes and cannot be further processed in a manner that is incompatible with those purposes (purpose limitation).

The Honeywell MAXPRO Cloud solution stores video clips based on alarms and events. Using an appropriate mixture of recording schedules, the data controller can minimize the processing and storage of unnecessary personal data, and stay compliant with the data minimization principle.

As with some Honeywell "on-premise" Access Control and Intrusion Systems, an end user may choose to enter specific data to meet their business and security needs. If the end user or data controller chooses to enter personal data into a cardholder record, it is the responsibility of the end user to ensure that it has a legal ground (such as the end user's legitimate interest), to do so. In all cases, the end user will be required to inform the concerned individuals in advance on the processing of their data, including amongst others, the type of data being processed and how this data will be used. They need to ensure that they minimize the collection of data and focus on data which is sufficient and relevant for purpose.

6.4/ Technical and organizational security measures

Honeywell has implemented both technical and organizational security measures in MAXPRO Cloud, in order to assist the end user to be GDPR compliant. The organizational security measures include log management, account management, verification procedures, and access management.

Log management: With Honeywell MAXPRO Cloud, the customer is able to keep a record of any data processing and safely store data in secured storage to prevent any breach of sensitive information. The access to data storage is controlled by industry standard security policies.

Account management: Honeywell Cloud solutions enable organizations to choose which user or group of users can have access to and manage different profiles. As part of their system, the end user needs to define appropriate levels of access to the system for different users or user groups. Honeywell solutions provide different privilege levels to help the controller to easily grant users the appropriate level of permission to view, access, search, export, delete, or make corrections (as required).

Verification procedures: With Honeywell Cloud Solutions, user account and password information are kept secure using Industry standard practices.

Access management: Data should only be disclosed on a "need-to-know" basis. Honeywell Cloud solutions protect access to data through well-designed privilege control systems. The controller can also enquire and get reports from the cloud system of various activities (e.g. adding credentials) done by users to ensure appropriate management of the data.

In addition to the organizational security measures, Honeywell supports the appropriate technical security measures.

Data encryption is one of the most important technical security measures suggested by GDPR. The Honeywell MAXPRO Cloud system is designed based on robust cyber security practice, authentication and encryption standards. The user data is stored on Industry Leading Public cloud platforms and secured by Industry certified security software and tools. Access to the cloud platform, storage & transmission employ the latest security standards. The security standards and practices are continuously upgraded and updated to meet the latest security challenges.

6.5/ Data Retention

The Honeywell MAXPRO Cloud solution allows the end user to choose the storage duration for video, access and intrusion to be set based on suitable packages they have selected, once they have defined their data retention approach. The data in the Cloud is deleted after the specified retention period.

7/ Biometric data

Biometric data is a special category of personal data requiring a stricter data protection regime. Biometric data is personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (Article 4 GDPR).

Biometric data processing is now often used in automated authentication/verification and identification procedures, in particular for the control of entry to both physical and virtual areas as used in some of our Honeywell security solutions. Biometrics includes physiological characteristics of a person and behavioral-based characteristics.

- Physiological characteristics: fingerprint verification, finger image analysis, iris recognition, retina analysis, face recognition, outline of hand patterns, ear shape recognition, body odor detection, voice recognition, DNA pattern analysis, and sweat pore analysis, etc.
- Behavioral-based characteristics: hand-written signature verification, keystroke analysis, gait analysis, etc.

Fair collection and information:

The collection of biometric data (e.g. image of the fingerprint, picture of the iris or of the retina, recording of the voice) should happen in a fair way. People's faces fall into the category of biometric data. Biometric data is one of the "special categories of personal data" that can only be processed if the data subject has given his or her explicit consent or the envisaged data processing can be based on one of the other legal grounds for processing biometric data.

The new generation of Honeywell MAXPRO Video Management Solutions and equIP cameras will provide face detection, face recognition, and smart search features. These systems will use biometrics to improve privacy compliance via enhanced pixilation solutions, data search, and other analytics. However, data controllers will need to ensure that data subjects are aware of and (where appropriate) have given consent to their use.

Storage of biometric data:

Distributed storage (e.g. on a smart card) of biometric data is preferred. But if identification can only be achieved by storing the reference data in a centralized database, then a careful assessment should be put in place. The other requirements for storage must comply with the general requirements for personal data.

In Honeywell face recognition solutions, the biometric system extracts user-specific features from the individual's face to build face templates. The storage of these faces templates will be in a central database, usually NVR/VMS, to support the analytics and smart search functions.

Sensitive data revealing racial or ethnic origin

Some biometric data could reveal racial or ethnic origin. In Honeywell face recognition solutions, the facial information will not be further processed. No racial or ethnic origin data are collected or processed. The face recognition and smart search functions will only compare the face template which has been abstract from the real face and is anonymous.

Security measures

It is desirable that templates and their digital representations be processed with mathematical manipulations (encryption, algorithms or hash functions), using different parameters for every biometric product in use, to avoid the combination of personal data from several databases through the comparison of templates or digital representations. In addition, the raw data may not be reconstructed from the template.

In Honeywell face recognition solutions, face raw data, face extraction and protection algorithms, and face templates are all simultaneously present in the collection of facial data. All the security measures and protection algorithms make it virtually impossible to reconstruct the original (raw) data from the templates in order to minimize the social risks and prevent the misuse of biometric data.

8/ Conclusion

GDPR was approved by the EU Parliament, and became enforceable as from May 25, 2018. In many ways, it is still an unknown quantity and its final implementation will depend on how it is interpreted and regulated in different countries.

Honeywell has always put tremendous effort into product and system design for effective data collection, data retention and data encryption – ensuring protection of personal data. We are redoubling these efforts to ensure our solutions help end users achieve better data protection compliance and support the compliance of their systems with GDPR. All this results in solutions that offer minimum system downtime, improved business continuity, lower risk of data breaches, and reduced cyber and compliance liability – all leading to enhanced customer satisfaction.

Honeywell solutions are not only deployed for large enterprises and critical infrastructures in the global market, but are also appropriate for small and medium-sized businesses and organisations to protect people, property, and services. Whatever the business requirement, Honeywell can provide appropriate solutions which also help you meet your GDPR compliance requirements.

9/ References

7.1/ The General Data Protection Regulation (GDPR)419/16; Council of the European Union

7.2/ ARTICLE 29 - Data Protection Working Party 12168/02/EN WP 80

7.3/ Preparing for the General Data Protection Regulation GDPR): 12 steps to take now V2.0

7.4/ GDPR in Context: Data Controller Accountability, Matheson

7.5/ Tackling-gdpr-compliance-before-time-runs-out; McKinsey

7.6/ EuroPriSe Criteria for the certification of IT products and IT-based services

7.7/ EU General Data Protection Regulation in 13 Game Changers; Baker & McKenzie LLP

7.8/ IPVM-gdpr-for-video-surveillance-guide-report

10/ Glossary

Access Control, Physical: An electronic physical access control system is typically used to replace mechanical lock and keys and can be extended to control access to parking gates, turnstiles, elevator/lifts, etc. Business benefits over the mechanical lock and key include the ability to easily and quickly replace lost or stolen keys versus rekeying a lock, saving time and money while maintaining physical security. Some or the other benefits include the ability to customize access by time, day, date and door(s) location(s) while recording when an access event occurred

Accountability: The data controller is responsible for demonstrating compliance

Accuracy: Data should be accurate and kept up to date.

Biometric Data: Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Breach Notification: A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. The controller must notify the competent EU supervisory authority about personal data breach without undue delay and no later than 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to the data subjects. The controller must also send a notice about the breach to the data subjects, unless the controller has taken measures to prevent any risk involved in the breach to the data subjects, for example, by encrypting the data. The processor must notify the controller about the breach without undue delay.

Dactyloscopic Data: Identification by comparison of fingerprints.

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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. (Article 4, GDPR).

Data Minimization: The processing of personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which that data is being used.

Data Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (Article 4, GDPR).

Data Processor: A natural or legal person, public authority, agency, or another body which processes personal data on behalf of the controller. (Article 4, GDPR).

Data Protection Officer: In certain circumstances, data controllers and processors must designate a Data Protection Officer (the DPO) as part of their accountability program. The threshold is (i) processing is carried out by a public authority, (ii) the core activities of the controller or processor consist of processing which, by its nature, scope or purposes, requires regular and systematic monitoring of data subjects on a large scale, or (iii) the core activities consist of processing on a large scale of special categories of data. The DPO will need sufficient expert knowledge. This will depend on the processing activities for which the officer will be responsible.

Data Subject: The concerned individual to whom the personal data pertain.

Fairness: The organization processing the data should provide data subjects with sufficient information about the processing and the means to exercise their rights.

GDPR: The General Data Protection Regulation (GDPR) (EU) is a regulation in EU law on data protection and privacy for all individuals within the European Union. It replaces the Data Protection Directive 95/46/EC, and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizen's data privacy and to reshape the way organizations across the region approach data privacy

Genetic Data: Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Health Data: Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Lawfulness: Data should be processed only when there is a lawful basis for such processing (eg, consent, contract, legal obligation, legitimate interest).

Personal Data: Means any information relating to an identified or identifiable natural person; an identifiable 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." (Article 4, GDPR).

Privacy by Design: The principle of data protection (or privacy) by design, is that privacy controls are to be embedded in the design of business operations, processes, products and services. The principle of data protection by default contemplates controllers applying the strictest privacy settings, for example, to a product or service. The aim is that controllers prevent, as far as possible, privacy risks occurring.

Privacy Impact Assessments: Controllers may be required to undertake pre-processing data protection or privacy impact assessments (PIA), which are required if the processing is likely to result in a high risk to an individual's rights, and which may require pre-processing consultation with the relevant supervisory authority. Such high-risk processing includes profiling, large scale processing of sensitive categories of personal data, and may arise where there is innovative use of technological solutions.

Purpose limitation: Personal data may be collected only for a specific, explicit, and legitimate purpose and should not be further processed.

Retention Period: A retention period is the time period which a business or organization identifies as necessary for its purposes to keep personal data. This may be driven by industry regulations or business requirements.

Security: Data should be processed in a manner that ensures security and protection against unlawful processing, accidental loss, damage, and destruction.

Storage limitation: Data should not be held in a format that permits personal identification any longer than necessary.

Transparency: The information provided to data subjects should be in a concise and easy to understand format (eg, the purpose of consent should not be buried in a lengthy document of terms and conditions).

For more information
www.honeywellvideo.com

Honeywell Security
22700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299
1.800.323.4576

Honeywell Security
Aston Fields Road
Whitehouse Industrial Estate
Runcorn, Cheshire, WA7 3DL
United Kingdom
Tel: +44 (0)8448 000 235

Honeywell Security Office
Emaar Business Park, Sheikh Zayed Road
Building No. 2, 2nd floor, 201
Post Office Box 232362
Dubai, United Arab Emirates
Tel: +971 44541704
www.honeywell.com

All information on Honeywell solutions in this document refers to those currently available as at August 2018 and planned solutions due in the next 6 months

Honeywell reserves the right, without notification, to make changes in product design or specifications.

HSV-GDPR-01-EN(0918)WP-Z

Honeywell