CATHEXIS PRIVACY GUIDE

GENERAL DATA PROTECTION REGULATION

11 February 2021

Contents

1. CathexisVision VMS and privacy compliance

This CathexisVision Privacy Guide provides guidelines for understanding personal data protection when using CathexisVision software, particularly in complying with the GDPR. The **General Data Protection Regulation (GDPR)** came into effect on 25 May 2018, passed by the European Union. The GDPR established rules on the protection, processing and movement of people's personal information. It places obligations on any organisations that collect data related to people in the EU, and imposes high penalties against those who do not adhere to its regulations. This document outlines the key features of the GDPR. so that customers understand their data protection responsibilities when using CathexisVision software.

1.1 Who needs to comply with the GDPR?

The GDPR applies to any organisation operating within the European Union, or organisations operating outside of the European Union but which offer products and services to customers and businesses within the EU, or processes personal data within the European Union.

1.2 What parties are involved?

In the case of video surveillance, and use of CathexisVision software in particular, there are three relevant parties in privacy compliance:

- **Data subject**: the person whose personal information is collected and used. In video surveillance, data subjects are the individuals viewed.
- **Data controller:** data controllers collect, process and use the personal information of the data subject. In video surveillance, this is the party that owns and use the video management system (VMS). This Privacy Guide also outlines the role of joint data controllers.
- **Data processor:** the party that processes the data, sometimes outsourced by the data controller.

1.3 Video surveillance system definitions

The European Data Protection Board provides helpful definitions of terms used when discussing privacy and video surveillance. A **video surveillance system** (VSS) consists of analogue and digital devices, as well as software, for the purpose of capturing images of a scene, handling the images and displaying them to an operator.

Components of a video surveillance system

Video environment	The purpose of **image capture** is generation of an image of the real world in such format that it can be used by the rest of the system. **Interconnections** describe all transmission of data within the video environment, i.e., connections and communications. Examples of connections are cables, digital networks, and wireless transmissions. Communications describe all video and control data signals, which could be digital or analogue. **Image handling** includes analysis, storage and presentation of an image or a sequence of images.
System management	**Data management** and **activity management**, which includes handling operator commands and system-generated activities (alarm procedures, alerting operators). **Interfaces to other systems** might include connection to other security (access control, fire alarm) and non-security systems (building management systems, automatic license plate recognition).
Security	**System security** includes physical security of all system components and control of access to the VSS. **Data security** includes prevention of loss or manipulation of data.

The definitions in the table above are from the *European Data Protection Board Guidelines 3/2019 on processing of personal data through video devices*, page 25.

1.4 Privacy compliance while using CathexisVision VMS software

A product, in itself, is not said to be GDPR compliant: a company cannot declare whether or not VMS software is compliant. Compliance depends on the combination of an organisation's access to and use of personal data in its use of products. Your company is legally liable to account for the ways in which it uses, stores and protects personal data.

When a company has data that refers directly to a person, or can be used to identify someone, then its actions fall within the purview of the GDPR. This personal information could, for example, include storing a person's name and surname in a metadatabase, or their identity number, or facial recognition data.

It is essential that companies ensure that their use of CathexisVision software falls within the regulations set out by the GDPR. This Privacy Guide is available to help Cathexis clients understand how they can do this.

2. Understanding GDPR

The GDPR sets out 7 principles which embody the essence and lay the basis for the interpretation of the Act. A breach of any of these conditions can result in significant fines: up to €20 million or 4% of your organisation's total worldwide annual turnover (whichever amount is the highest).

2.1 The 7 GDPR Principles

LAWFULNESS, FAIRNESS AND TRANSPARENCY: compliance with all aspects of this principle is essential. If the processing is lawful yet still hidden from data subjects concerned, that would constitute a breach of this principle. There must be specific grounds for the processing of data (lawfulness). Data must be handled reasonably and in ways that will not have an unjustified adverse effect on the data subject (fairness), and the collection, purpose and handling of the personal data must be done clearly, openly and honestly (transparency). Transparency also relates to "invisible processing": where personal data is collected by a third party from a source which has already gathered it, and there is thus no direct relationship between the final organisation and the data subject. Organisations need to communicate with data subjects using clear language.

PURPOSE LIMITATION: an organisation must be clear about why it is collecting personal data and what it intends to do with it, and supply data subjects with information if requested. Records of this purpose need to be created and maintained as part of the documentation obligations (Article 30). An organisation may only use the data for a new purpose if doing so is compatible with the original purpose, consented to, or as a result of a clear legal function. This principle prevents "function creep" within organisations, and helps to create trust and awareness with data subjects.

DATA MINIMISATION: personal data being processed must be adequate to fulfil the purpose for its collection, relevant or rationally linked to that purpose, and limited to what is necessary. Organisations should aim to hold no more data than needed for the purpose collected. Data minimisation requires regularly reviewing the data held and deleting what is not needed, which links to the storage limitation principle (see below) and data subjects' "right to be forgotten". Applying the principle of data minimisation is much easier when an organisation is clear about the purpose of collecting data. If the data held is not assisting the organisation in achieving the purpose of its collection, then the organisation is most likely in breach of the first element of this principle.

ACCURACY: the organisation must take all reasonable steps to ensure that the data held is accurate and not incorrect or misleading. Processes need to be put in place to check and verify data, correct or erase it when necessary, and consider any challenges to its accuracy. This also applies to data held which is categorised as opinions. In the event of a challenge to the data's accuracy, individuals have the absolute right to have incorrect personal data rectified under the right to rectification.

STORAGE LIMITATION: personal data may not be held for longer than needed, and an organisation will need to be able to justify the time period for which it is holding the data. The storage limitation principle also supports the accuracy and purpose limitation principles, reducing the risk of holding data which could be classified as irrelevant, excessive or inaccurate due to being out-of-date. Organisations need to set retention periods and comply with the documentation requirements of the GDPR. It is necessary to periodically review and delete any inadequate data under this principle. Individuals have the right to erasure, but there is scope for data being held for a longer time when kept for public interest archiving, scientific or historical research, or statistical purposes. Adhering to this principle results in more efficient data management, reduces storage and security costs, and reduces the risk of using unnecessary data in error.

INTEGRITY AND CONFIDENTIALITY: also known as the security principle, this concerns information security. Organisations need to have appropriate security measures to protect the personal and private data which they are holding, testing and making necessary improvements. Information security covers both cybersecurity and physical and organisational security measures. These include risk analysis, organisational policies, and physical and technical measures. Where appropriate, organisations should consider encryption and pseudonymisation. In the event of a technical or physical incident, measures need to ensure that availability and access to personal data can be restored timeously. Data subjects are entitled to be protected from all forms of injury that can result from security breaches, such as identity fraud, fake credit card transactions, witness intimidation, physical harm mortgage fraud, fake applications for tax credits, exposure of physical addresses, targeting by fraudsters, and personal inconvenience.

ACCOUNTABILITY: the organisation is responsible for complying with the GDPR and needs to demonstrate this compliance. Measures which support meeting this principle include adopting and implementing data protection policies, taking a "data by design and default" approach, having written contracts with organisations which process personal data on your behalf, keeping documentation on the processing activities, implementing security measures, dealing with security breaches correctly, carrying out data protection impact assessments, appointing a data protection officer, and adhering to the relevant codes of conduct. The obligations of the accountability principle are ongoing: its measures need to be regularly reviewed and updated.

2.2 What rights do data subjects have?

- The right to be informed (Article 12, 13, 14, ad 34)
- The right to access (Article 15)
- The right of rectification (Article 16)
- The right to erasure (Article 17)
- The right to restrict processing (Article 18)
- The right to data portability (Article 20)
- The right to object (Article 21)
- Rights in relation to automated decision making and profiling (Article 22)

The right to be informed is a key transparency requirement. Individuals must be informed about the collection, use, processing and retention of their personal data, and whether it will be shared with other entities and who those entities are. However, when obtaining personal information from other sources, you do not need to notify individuals with this privacy information if the individual already has the information, if providing it would be impossible or take disproportionate effort, or your entity is required by law to obtain the information.

There are various methods to provide individuals with privacy information, such as: ✓

1. **A layered approach** – a short notice with key privacy information that has additional layers of more detailed information available. (See Right to be informed and Privacy notice.)
2. **Dashboards** – management tools which inform people about their data use and allows them to manage what happens with it
3. **Just-in-time notices** – privacy information delivered at the time the data is collected
4. **Icons** – symbols which indicate the existence of a certain type of data processing
5. **Mobile and smart device functionalities** – these can include pop-ups, voice alerts, and mobile device signals.

The right of access means that individuals have the right to receive a copy of their personal data. Subject access requests can be made verbally, in writing, or even via social media. Generally, an organisation may not charge a fee for such a request and must respond within one month and disclose the information securely.

The right of rectification allows individuals to have their data rectified if inaccurate or incomplete. They can request this verbally or in writing and the organisation has one month to respond.

The right to erasure is also known as the "right to be forgotten". Such a request can be made verbally or in writing and the organisation has one month to respond. This right only applies if the data is no longer necessary for the purpose for which it was collected or processed originally, or when the data can only be held with consent of the data subject and that consent is withdrawn. If the right does apply, the data must be deleted from live as well as backup systems.

The right to restrict processing applies in certain circumstances, in which case the data may be stored but not used or processed. See Access, rectification and restriction of processing.

The right to data portability only applies to information which an individual has provided to a data controller. It allows individuals to view and access and use their own personal data in a way which is portable and safe. It allows them to move, copy or transfer personal data from one IT location to another without affecting its usability. It also allows a data subject to request a data controller to transmit their data to another controller. If the personal data happens to include information

about others in the case of third-party data the organisation must consider whether transmitting the data would negatively affect the rights of those third parties.

The right to object: individuals may object to the processing of their personal data in certain circumstances. In the case of direct marketing, individuals have an absolute right to stop their data being used. In other cases, an organisation may continue processing the data if they can furnish evidence showing a compelling reason for doing so. Individuals must be notified of their right to object *at your first communication with the data subject* a*t the latest* and their objection may be made verbally or in writing and must be responded to within one month. This right effectively allows individuals to stop the processing of their personal data.

Rights in relation to automated decision making and profiling: an organisation may only carry out automated decision-making and profiling where it is necessary for the performance of a contract or authorised by law, or based on the individual's explicit consent. As such decision-making can be high risk, the GDPR requires that a Data Protection Impact Assessment be carried out.

2.3 Further steps to consider

- Have a team run data protection, rather than a single person, and make that team multi-disciplinary (drawing from IT, HR, and administrative functions within the organisation).
- Invest in training staff and making them aware of the legislation and its practical effect on business operations.
- Review the organisation's procedure for withdrawing consent, and make it easy for data subjects to do so.
- Create data risk assessment – for instance, subject access requests will no longer charge a fee for the unlocking of relevant employee data.

Twelve steps to take to ensure GDPR compliance within your organisation:

The UK Information Commissioner's Office has published a 12-step checklist to assist organisations in complying with the GDPR. It advises organisations to:

1. Promote awareness within the organisation by ensuring that decision makers and key personnel know about the new legislation.
2. Carry out an audit by checking what personal data the organisation holds, its source, and how it is stored or shared.
3. Update privacy notes and review data protection policies by updating existing contracts, Terms and Conditions, as well as policies and procedures that involve data protection.
4. Ensure that your procedures respect all the rights that data subjects have.
5. Update your procedures to be ready to handle requests within the new set timescales.
6. Keep records in order to show compliance with the main central concept of the GDPR – that of accountability. Regularly update the organisation's records of what data they are processing and their legal basis for doing so with documents to substantiate that.
7. Review and, if necessary, amend how the organisation searches for and obtains and stores data, as well as consent given to do so by data subjects.
8. Put a system in place to verify ages of data subjects and to obtain parental or guardian consent for use or processing of the data of children, or related to children.
9. Be ready to deal with breaches by having the suitable procedures in place to detect, notify and investigate data protection breaches.
10. Work towards data protection by design. Implement data protection impact assessments.
11. Appoint a Data Protection Officer within the organisation to be responsible for compliance. This is not compulsory for smaller businesses, but it is advisable. A GDPR committee is also prudent for larger organisations.
12. Examine what other international privacy legislation your organisation may need to comply with. Determine the organisation's lead data protection supervisory authority, if it is operating in more than one EU member state.

3. Personal data and using CathexisVision software

3.1 What is personal data?

Personal information is not limited to written addresses and contact numbers – it covers any information which can be used to identify a person. Video surveillance and CCTV footage thus fall within its broad definition and are subject to GDPR requirements.

In video surveillance, personal data is the information which relates to an identified or identifiable person (an object in the footage). When using CathexisVision, personal data could include the processing of video footage and location information, facial recognition, automatic number plate recognition, or access control systems.

According to the GDPR, personal data is "any information relating to an identified or identifiable natural person". An identifiable natural person is one who can be identified, "directly or indirectly" – and thus distinguished from other individuals – particularly by reference to the following (non-exhaustive list of) identifiers set out by the GDPR:

- A name
- Identification number
- Contact details (email address, phone number, residential address)
- Location data
- Online identifier
- User data and images
- One or more "factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Furthermore, the GDPR only applies to the processing of personal data in two ways:

- "wholly or partly by automated means" and
- "to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system" (Article 2(1)).

If a person can be distinguished from other individuals solely by observing the data being processed, then that individual is identifiable.

3.2 What makes data personal?

According to the GDPR, and to quote the Information Commissioner's Office, "even if an individual is identified or identifiable, directly or indirectly, from the data you are processing, it is not personal datal unless it *relates to* the individual". This is of special relevance to the world of VMS. Data may in fact reference an identifiable individual but not be classified as personal data, due to the fact that the information does not *relate* to the individual. For the information to *relate to* the individual it must concern that individual in some way. Three elements may be considered to determine if data relates to the individual:

- **Is the content of the data directly about the individual or their activities?** If so, this data is considered personal data, no matter what the purpose is for gathering and processing it. Specific examples include medical history, work performance review or record, criminal record or record of personal achievements. Data which is also clearly about an individual's activities also is relevant here, such as banking statements or telephone bills. One point to note is that data being held may not in itself be personal data, but if certain circumstances arise where it can be linked to an individual, it can *become* personal data. For instance, when a job advertisement includes salary details, that is not personal data, but once the job has been filled and that data can be linked to the individual occupying that job, the data becomes personal.

- **What is the purpose of the data?** The Information Commissioner's Office explains this point: "if the data is used, or is likely to be used, to learn, evaluate, treat in a certain way, make a decision about, or influence the status or behaviour of an individual, then it is personal data".

- **What are the effects of the processing of the data on that individual?** If something about the individual is learnt through the processing, even if that was not the controller's primary aim, that data is personal, especially if the processing has an impact on the individual as a result.

If information about an individual is inaccurate, it is still deemed personal data if it relates to that identifiable individual. Another consideration relevant to the VMS setting is where data passes between different controllers. With the first or initial controller, the data may potentially not be personal due to the fact that it does not relate to an identifiable individual. However, when passed to the second controller, it may become personal data when used for a different purpose or when combined with other information available only to the second controller. The purpose of the processing needs to be clarified and care taken in analysing and finding a solution for the situation.

When using CathexisVision, personal data does not only apply to the subject viewed in footage. Data controllers must consider whether their interaction with user data – such as activity logs, timestamps, and metadata – constitutes the processing of personal data.

3.3 Online identifiers

Recital 30 provides a non-exhaustive list of possible online identifiers, such as internet protocol (IP) addresses and cookie identifiers. Other examples which may constitute personal data include:

- MAC (Media Access Control) addresses
- Advertising IDs
- Pixel tags
- Account handles, and
- Device fingerprints

Real-world examples falling within the realm of this category of personal data would include:

- An individual's social media 'handle' or username is still considered personal data as it is able to identify the individual and distinguish them from others. Even if the controller is unable to link the online name with the real-world individual, the data is still personal.
- Cookie technologies involve the processing of personal data if used to create a profile of the individual.

Facial recognition technologies for the purpose of identifying an individual would constitute the processing of personal data, in that they record features which distinguish the individual from other individuals.

Thus, holding any identifier or combination of identifiers which can identify an individual, or even simply distinguish an individual from others, makes the individual identifiable and thus raises the possibility of their data being termed personal. This also further links with indirect identification.

3.4 Special categories of personal data

The GDPR sets out 'special categories of personal data' as being more sensitive and requiring a higher level of protection. These categories include personal data relating to an individual's:

- Race
- Ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data and medical history
- Sexual orientation and activities
- Criminal record

In addition, personal data relating to criminal convictions and offences also requires a higher level of protection.

In video surveillance, special categories of personal data can potentially arise when the system is set up near prisons, hospitals or clinics, mines, places of worship, universities and other political, social, labour or legal institutions.

3.5 Pseudonymisation and anonymisation

Pseudonymisation of data is defined by the GDPR as "the processing of data in such a manner"

> *that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*

An example of pseudonymisation is using a reference number for an individual, with the information tying the data to the individual held separately. Held on its own, such information is meaningless. The controller, and typically the entire organisation, can still re-link the information with the data subject, but this method can reduce the risks to the data subject resulting from breaches. Pseudonymisation can also help organisations meet their GDPR obligations.

Pseudonymisation is merely a security measure. Pseudonymised data is still personal data under the GDPR and thus subject to the its requirements. Recital 26 clarifies: "personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person".

Organisations often classify their data as **anonymised** when it is merely **pseudonymised** (and therefore still personal). For data to be anonymised, it must no longer be able to be used to identify or *re-identify* the individual. If the data can be made available again to re-identify the individual, it was only pseudonymised. In addition, under the GDPR this data is still viewed as being processed by the organisation. Until the point of complete anonymisation, the data is it is still being processed as defined by the GDPR and still subject to its regulations. It is recommended that organisations anyonymise data, where possible, as a way to limit risks to both the controller and the data subject.

3.6 What to do when uncertain about the status of data

When there is uncertainty as to whether the data is personal, it is a matter of good practice to treat it as if it is in fact personal. The best approach would be to treat the data with care, hold and dispose of the data securely, and have a clear and lawful original purpose for processing the data. There is always the possibility that another controller would have other data, which when combined with the "indeterminate/uncertain" data would then qualify it as personal data, able to identify an individual.

It is wise to ensure that the information is being kept securely, protect the data from unlawful disclosure, maintain transparency about how the information is being collected, and ensure that you are lawfully justified in the data processing that you are carrying out.

4. The distinction between Data Controllers and Data Processors

The GDPR defines a **data controller** as the party which determines "the purposes and means of the processing of the personal data". It defines the **data processor** as the party "which processes personal data on behalf of the controller". Controllers are termed as **joint controllers** "where two or more controllers jointly determine the purposes and means of processing". The GDPR further defines a **third party** as the body "other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data". In addition to obligations for data controllers, the GDPR sets out statutory obligations for processors in their own right, as well as explicit requirements aimed at joint controllers.

4.1 What is your organisation's role?

It is crucial that the organisation determines whether it falls into the category of data controller or data processor. The GDPR's definition of processing is "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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

The responsibility to exercise control over the processing and to protect the personal data being process falls on the data controller. The role of a data processor relates to the more technical aspects of the handling of the data, such as storage, retrieval or erasure. The data controller carries out more complex activities such as interpreting the data, or significant decision-making in relation

to the data. Providing a processing service to another organisation does not necessarily mean that that organisation is a data processor. In fact, it could be a data controller in its own right. This depends on the extent of its control and responsibility over the processing.

4.2 In video surveillance, what is a data controller?

The organisation which owns and operates the video surveillance system is classified as the data controller. The **data controller** can be defined as the entity whose functions fall within this scope:

- collects the personal data in the first place
- decides the purpose or outcome for such collection
- selects which items of data to collect and thus determines the data content
- ascertains which individuals to collect data about
- decides whether to disclose the data and to who
- will make the final decision on whether subject access rights apply
- makes the final decision on how long to retain the data or whether to update or erase it.
- gains or profits from the processing
- has a contract with the data subjects which allows, or is the cause of, the processing
- has a direct relationship with the data subjects
- makes decisions about the data subjects as a result of the processing
- appoints the processors to deal with the processing of the data on the controller's behalf
- has total autonomy regarding the processing methods.

4.3 In video surveillance, what is a data processor?

The **data processor** is the entity which:

- decides IT systems or methods to use to collect the data
- does not decide what data to collect nor the lawful basis or purpose for such collection
- decides how to store the data
- handles security to do with the data
- deals with transferring data between organisations
- assists in data retrieval
- provides the means for erasure
- checks that the retention plan is maintained
- follows the instructions of another entity (the controller) regarding the processing of the data
- does not make decisions regarding disclosure nor setting of the retention schedule
- makes decisions regarding processing but makes those decisions under contract with the controller.

4.4 What are joint controllers?

Two or more controllers are termed **joint controllers** (as opposed to a controller-processor relationship). They

- have a common objective in terms of the processing
- are both processing the same data (one database) for the same purpose
- have designed this process together
- have a single set of information management rules with each other.

4.5 The importance of the distinction

Data controllers and data processers each have legal responsibilities under the GDPR. It is crucial that all parties know their roles to ensure that no data protection responsibilities are neglected. In the event of breach, even simply due to negligence or accidental error, it will be important to know where liability and responsibility lies. For example, if an organisation mistakenly defines its role as that of a data processor, when in fact its organisational processing activities cause it to fall within the definition of a data controller, a number of vital responsibilities and functions would be overlooked, resulting in breach of the regulations.

With the complexity of modern business relationships, it can be difficult to determine where the data protection responsibility lies. A scale of responsibility evolves according to where the main control over the data lies. The highest level of responsibility lies with the data controller, who is also responsible for the compliance of their respective processor. The type of structure through which an organisation sets specific and detailed processing instructions for its service provider, thus clearly delineating a controller from a processor, is rare in business but more typical of government structures. More commonly, data controllers allow their data processors a fair degree of discretion with handling the processing and leave it to the processor's know-how and expertise.

5. Guidelines for Data Controllers

Data controllers shoulder the ultimate responsibility for ensuring that their processing activities – including processing activities carried out on their behalf by their processors – are GDPR compliant. Controllers are liable for non-compliance and the non-compliance of their processors as well as liable for damage if their processing activities infringe the GDPR. The data controller must know what data it holds, the data source, who the data is shared with, and how it is used. The data controller also must have documentation to record these four activities.

Data controllers must comply with the full set of data protection principles as set out in Article 5 (see The 7 GDPR Principles), and protect data subjects' rights as set out in Chapter 3, Articles 12 to 23 (see What rights do data subjects have?).

- ✓ Assess data flows with information audits.
- ✓ Maintain documentation of personal data processing (Article 30).
- ✓ The "Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for" in Articles 12 to 22 and Article 34, as well as Article 5 as it relates to Articles 12 to 22 (Article 23). These restrictions apply when they are necessary to protect the democratic society's national security, defence, public security, or judicial proceedings, among others.

📎 A helpful checklist for Data Controllers is available on the GDPR website.

5.1 Relationship with the Data Processor

If the Data Controller hires a Data Processor to manage its VMS systems, then the parties need to draw up a binding contract which includes the compulsory provisions as specified in Article 28(3).

- ✓ Select a processor that guarantees its adherence to GDPR regulations.
- ✓ Create a Data Processing Agreement with your Data Processor.

For a sample *Data Processing Agreement*, see Appendix 1: Document Templates.

5.2 Organisational procedures

The organisation needs to demonstrate a culture of data protection compliance. Controllers and processors must implement organisational and technical measures proportionate to the "risks to rights and freedoms of natural persons resulting from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to video surveillance data" (*EDPB Guidelines*, 240).

Article 24 sets out that controllers need to implement the "appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed" in accordance with the GDPR, including implementing the "appropriate data protection policies". Controllers need an **internal framework** and set of **policies** which implement this. Safeguards to data and privacy should be built into not only the design specifications of the technology, but also the organisation's practices and culture.

✓ The data controller must protect the system and its data "during storage (data at rest), transmission (data in transit) and processing (data in use)" (See *EDPB Guidelines*).

✓ Organisations should aim for technical solutions which enhance data and privacy security and are thus "privacy-friendly": for example, allowing masking or scrambling irrelevant areas or editing out third-person images.

Controllers should implement the technical and organisational measures needed for data protection *before* they begin processing footage (Article 25). As the EDPB Guidelines advise, organisations can use "built-in privacy enhancing technologies, default settings that minimise the data processing, and [...] tools that enable the highest possible protection of personal data".

5.2.1 Staff

All staff members within the organisation must be aware of and obligated to adhere to the principles of data privacy and protection.

✓ Train the organisation's staff in data protection policy.

5.2.2 Data Protection Officer

Controllers and/or processors must appoint a **data protection officer** (DPO) if the "core activities of the controller or processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale" (Article 37(1) b).

✓ Appoint a data protection officer within your organisation (Article 37) if it meets the requirements for one or, at the very least, appoint an individual or individuals to manage personal data protection and GDPR compliance within the organisation.

When must a DPO be appointed?

Article 37(1) sets out three instances in which a DPO must be appointed:

a) where the processing is carried out by a public authority or body;

b) where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or

c) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

A DPO would be **mandatory** in the case of a private security company which carries out security surveillance of public places. This surveillance is the core activity of the company and is linked to the processing of personal data. A company which processes its employees' personal data for payment records would **not** need to appoint a DPO for this process, as it is one of its many secondary functions.

What is large-scale processing?

The definition of processing "on a large scale" as set out in Article 37(1) still needs further clarification. However, the Article 29 Data Protection Working Party's Guidelines on Data Protection Officers set out some criteria which might constitute processing "on a large scale":

- the number of data subjects concerned – either as a specific number or as a proportion of the relevant population
- the volume of data and/or the range of different data items being processed
- the duration, or permanence, of the data processing activity
- the geographical extent of the processing activity.

Examples of large-scale processing include:

- processing of patient data in the regular course of business by a hospital
- processing of travel data of individuals using a city's public transport system (for example, tracking via travel cards)
- processing of real time geo-location data of customers of an international fast-food chain for statistical purposes by a processor specialised in providing these service
- processing of customer data in the regular course of business by an insurance company or a bank
- processing of personal data for behavioural advertising by a search engine
- processing of data (content, traffic, location) by telephone or internet service providers.

The following examples **do not** constitute large-scale processing:

- processing of patient data by an individual physician
- processing of personal data relating to criminal convictions and offences by an individual lawyer

The Article 29 Data Protection Working Party interprets "systematic" as meaning one or more of the following:

- Occurring according to a system
- Pre-arranged, organised or methodical
- Taking place as part of a general plan for data collection
- Carried out as part of a strategy

CCTV falls within the definition of "systematic" processing.

Who should be the DPO?

The DPO "shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39" (Article 37(5)). The level of "expert knowledge" can be determined based on the data processing operations being carried out (Recital 97).

A single DPO (typically with a supporting team) can be designated to serve a number of organisations, provided the DPO is "easily accessible from each establishment" – in terms of the DPO's role in advising the controller, processor and employees regarding their GDPR obligations – as well as to data subjects (Article 37, (2) and (3)).

It is advisable that the DPO be located in the EU. However, this is not essential, especially if the controller and/or processor have no establishment within the EU.

Appointing a volunteer DPO

The DPO is often the cornerstone of the organisation's accountability. Therefore, even if it is not mandatory, an organization can still appoint a DPO on a voluntary basis. By appointing a DPO, an organisation can gain a competitive advantage regarding GDPR compliance. The DPO facilitates Data Protection Impact Assessments, as well as acting as an intermediary between relevant stakeholders.

Whether mandatorily or voluntarily appointed, the DPO is subject to Articles 37 to 39. In line with the accountability principle, the organisation must document its reasons for not appointing a DPO, and keep these records in the event that a relevant supervisory authority investigates the decision.

The DPO's responsibilities

DPOs are not personally responsible for the controller or organisation's GDPR compliance but they are tasked with carrying out measures that support the organisation's compliance (Article 39). The controller or processor is responsible for compliance. The controller needs to support the DPO in carrying out their tasks by providing them with the resources and autonomy to do so. The DPO shall "directly report to the highest management level of the controller or the processor" (Article 38(3)). The DPO's autonomy needs to be respected and DPOs should "not be dismissed or penalised by the controller or the processor for performing [their] tasks".

In performing their tasks and responsibilities, the DPO shall consider the risks associated with data processing, "taking into account the nature, scope, context and purposes of processing".

When the organisation installs a video surveillance system or updates its video surveillance system, the DPO should advise this process so that any updates comply with the GDPR.

The Article 29 Data Protection Working Party recommends that the DPO is involved in the organisation's decision-making in the following ways:

- The DPO is invited to participate regularly in meetings of senior and middle management.
- The DPO's presence is recommended where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice.
- The opinion of the DPO must be given due weight. In case of disagreement, the WP29 recommends to document the reasons for not following the DPO's advice.
- The DPO must be promptly consulted once a data breach or another incident has occurred.

The DPO's responsibilities include:

- Train employees in GDPR requirements and other data protection obligations.
- Monitor the organisation's compliance with the GDPR, carry out regular assessments and audits and acquire third-party certification when necessary, and create compliance reports.
- Advise the controller regarding the data protection impact assessment and monitor its performance (see Data Protection Impact Assessment), or hire an independent party to carry out the data protection impact assessment.
- Co-operate with the Supervisory Authority and serve as the contact point for the Supervisory Authority regarding data processing, including the prior consultation referred to in Article 36.
- Keep records of all of the organisation's personal data processing activities.
- Make sure that the organisation responds to data subjects' requests.
- Advise on the organisation's Video Surveillance Policy.
- Manage the Data Processor Agreement.
- Manage the Record of Processing Activities (Article 30). According to the GDPR, maintaining a record of the processing is not necessarily a task of the DPO, but the controller may assign them this task. This could assist the DPO in their tasks, such as monitoring compliance and advising the controller or processor on related matters.
- Post the Data Breach Notification when necessary.

The controller and processor must involve the DPO in all issues that relate to the protection of personal data, and support the DPO in performing these tasks (Article 38).

Keeping a running overview and maintain records of data processing activities.

For a *Record of Processing Activities* template, see Appendix 1: Document Templates.

5.3 Setting up a video surveillance system

5.3.1 Technical measures

There are measures to support system and data security (which, as the EDPB explains, protect "against intentional and unintentional interference with its normal operations") and access control.

System and data security measures:

- Protection of the entire VSS physical set-up (including cameras, cabling, and power supply) against physical interference and theft.
- "Protection of footage transmission with communication channels secure against interception".
- Data encryption.
- Use of both hardware and software solutions such as firewalls and antivirus.
- "Detection of failures of components, software and interconnections".
- "Means to restore availability and access to the system in the event of a physical or technical incident".

Access control measures:

- Keeping secure from unauthorised third parties the premises where the monitoring of the surveillance footage is carried out and the footage is stored.
- Positioning monitors which are in open areas so that only authorised staff may view them.
- "Procedures for granting, changing and revoking physical and logical access are defined and enforced".
- Keeping user authentication methods, such as passwords, updated and implemented.
- "User performed actions (both to the system and data) are recorded and regularly reviewed".
- Weaknesses in the system are identified and addressed timeously by monitoring and detecting access failures regularly.

CathexisVision supports encryption for all external site connections and offers four selectable encryption levels. It also has secure IP camera connection and data encryption.

Cathexis has increased the level of video "signing" to explicitly associate the signatures with the source, providing more detail in the archive player of the video verification results.

5.3.2 Video Surveillance Policy

Before processing, the organisation, in consultation with its DPO, needs to outline the purpose of its video surveillance and ensure that it complies with the GDPR. Article 5(1)b, the purpose limitation clause, states that personal data will be "collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".

The European Data Protection Board clarifies that "cameras that are used for the same purpose by a single controller can be documented together, as long as every camera in use has a documented purpose". Generally, Article 6(1)f will apply to video surveillance: it states that processing is only lawful if it "is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." This can be referred to as the "**legitimate interest clause**".

It is not sufficiently specific to merely classify the purpose of the video surveillance as "safety". It is recommended that controllers document any past security-related incidents which could be used to support the legitimate interest claim. To provide a legitimate interest claim, it is not enough to simply present general or national crime statistics. It is also not necessary for such security breaches to occur in order to justify such a legitimate interest. Ideally, the controller would provide documentation about nearby business experiences with security issues, combined with area-specific statistics and relevant cases, to prove a legitimate interest.

These purposes for monitoring must also be documented in writing (Article 5(2)) and must be specified for every camera in use.

Create a Video Surveillance Policy.

In terms of data minimisation (Article 5(1)c), before installing the system it is important for the controller to determine the means to achieve the purpose of the system that are least intrusive to the rights of the data subject.

5.3.3 Data Protection Impact Assessment

Before your organisation installs and operates a video surveillance system, you need to assess whether the system will comply with the GDPR and data protection laws. Where high-risk data processing is planned, a formal **data protection impact assessment** (DPIA) is crucial. The DPIA can be viewed as a "useful and positive activity that aids legal compliance".

It is important to view the DPIA as an ongoing process, not a once-off assessment. Where necessary, the "controller shall carry out a review to assess if processing is performed in accordance with the DPIA at least when there is a change of the risk represented by processing operation" (Article 35(11)). Controllers need to continually assess the risks created by their processing activities, to identify whether they require a DPIA at a later stage.

For a video surveillance system, the DPIA would set out the planned surveillance system, evaluate its necessity and proportionality, its impact on data subjects' rights, the measures the organisation is taking to prevent privacy violations, and other data protection policies.

Depending on the outcome of the assessment, the organisation might discontinue its plans, or carry out further data security and privacy compliance measures. If the controller's processing activities are subject to a DPIA, failure to correctly carry out the assessment or consult the relevant supervisory authority if required can lead to significant fines.

Is a DPIA necessary?

A **formal data protection impact assessment is required** for "systematic monitoring of a publicly accessible area on a large scale" and when the data processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35).

✓ If the exceptions do not apply and processing is likely to result in a "high risk" to individuals' rights, conduct a data protection impact assessment (in consultation with the DPO).

Article 35(3) provides categories of operations presenting a high risk to data subject's rights. The Article 29 Data Protection Working Party gives 9 examples of operations that require a DPIA:

1. Evaluation or scoring, including profiling and predicting
2. Automated decision-making with legal or similar significant effect
3. Systematic monitoring
4. Sensitive data or data of a highly personal nature
5. Data processed on a large scale
6. Matching of combining datasets
7. Data concerning vulnerable data subjects
8. Innovative use or applying new technological or organisational solutions
9. When the processing itself "prevents data subjects from exercising a right or using a service or a contract".

Where the processing meets at least two of these criteria, a DPIA would be required. However, if the processing meets only one of these criteria, it might still be necessary to carry out a DPIA.

A single DPIA may be used to assess multiple processing operations which are similar in scope, nature, context, purpose and risks. For example, a group of municipal authorities or controllers, each setting up a similar CCTV system, could carry out a single DPIA covering the processing by separate controllers. Another example would be for a single operator to cover the video surveillance in all of its locations or stations with a single DPIA. Justification must be given for performing a single DPIA, and a reference DPIA should be made publicly accessible.

A DPIA is *not* required in these instances:

1. Where the processing is not likely to result in a high risk to the rights and freedoms of natural persons.
2. Where the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out (in such cases, results of DPIA for similar processing can be used (Article 35 (1)).
3. Where the processing operations have been checked by a supervisory authority before May 2018 in specific conditions that have not changed.
4. Where a processing operation has a legal basis in EU or Member State law and where a DPIA has already been carried out.
5. Where the processing is included on the optional list of processing operations for which no DPIA is required.

Even when a controller does not do a DPIA, the accountability principle means that every controller must maintain a record of its processing activities. The record should include the purposes of the processing, a description of the categories and recipients of data, a description of the technical and organisation security measures (Article 32(1)) and an assessment of the likelihood of high risks to the data subjects.

If there is uncertainty whether or not to do a DPIA, the European Commission recommends that the organisation nonetheless performs an assessment as a tool to help the controller in complying with the GDPR. This is especially advised when dealing with new data processing technologies.

Before installing a video surveillance system, assess of the impact of the organisation's data processing activities according to their lawfulness, fairness, and other GDPR regulations.

Examples of processing	Possible relevant criteria	DPIA likely to be required?
A hospital processing its patients' genetic and health data (hospital information system).	○ Sensitive data or data of a highly personal nature. ○ Data concerning vulnerable data subjects. ○ Data processed on a large scale.	Yes
The use of a camera system to monitor driving behaviour on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognise license plates.	○ Systematic monitoring. ○ Innovative use or applying technological or organisational solutions.	
A company systematically monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc.	○ Systematic monitoring. ○ Data concerning vulnerable data subjects.	
The gathering of public social media data for generating profiles.	○ Evaluation or scoring. ○ Data processed on a large scale. ○ Matching or combining of datasets. ○ Sensitive data or data of a highly personal nature.	
An institution creating a national level credit rating or fraud database.	○ Evaluation or scoring. ○ Automated decision making with legal or similar significant effect. ○ Prevents data subject from exercising a right or using a service or a contract. ○ Sensitive data or data of a highly personal nature.	
Storage for archiving purpose of pseudonymised personal sensitive data concerning vulnerable data subjects of research projects or clinical trials.	○ Sensitive data. ○ Data concerning vulnerable data subjects. ○ Prevents data subjects from exercising a right or using a service or a contract.	
Examples of processing	**Possible relevant criteria**	
A processing of "personal data from patients or clients by an individual physician, other health care professional or lawyer" (Recital 91).	○ Sensitive data or data of a highly personal nature. ○ Data concerning vulnerable data subjects.	No
An online magazine using a mailing list to send a generic daily digest to its subscribers.	○ Data processed on a large scale.	
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website.	○ Evaluation or scoring.	

The above table is from *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.*

Balancing interests

The controller's assessment must balance the interests of the data subject's rights with that of the controller's need for video surveillance. The **balancing of interests** is compulsory (Article 6(1)f) and decisions must be made on a case-by-case basis. A crucial factor in this regard is the "intensity of intervention" of the data subject's rights. This intensity factor is determined by the "type of information that is gathered (information content), the scope (information density, spatial and geographical extent), the number of data subjects concerned [...] the situation in question, the actual interests of the data subjects, alternative means, as well as the nature and scope of the data assessment".

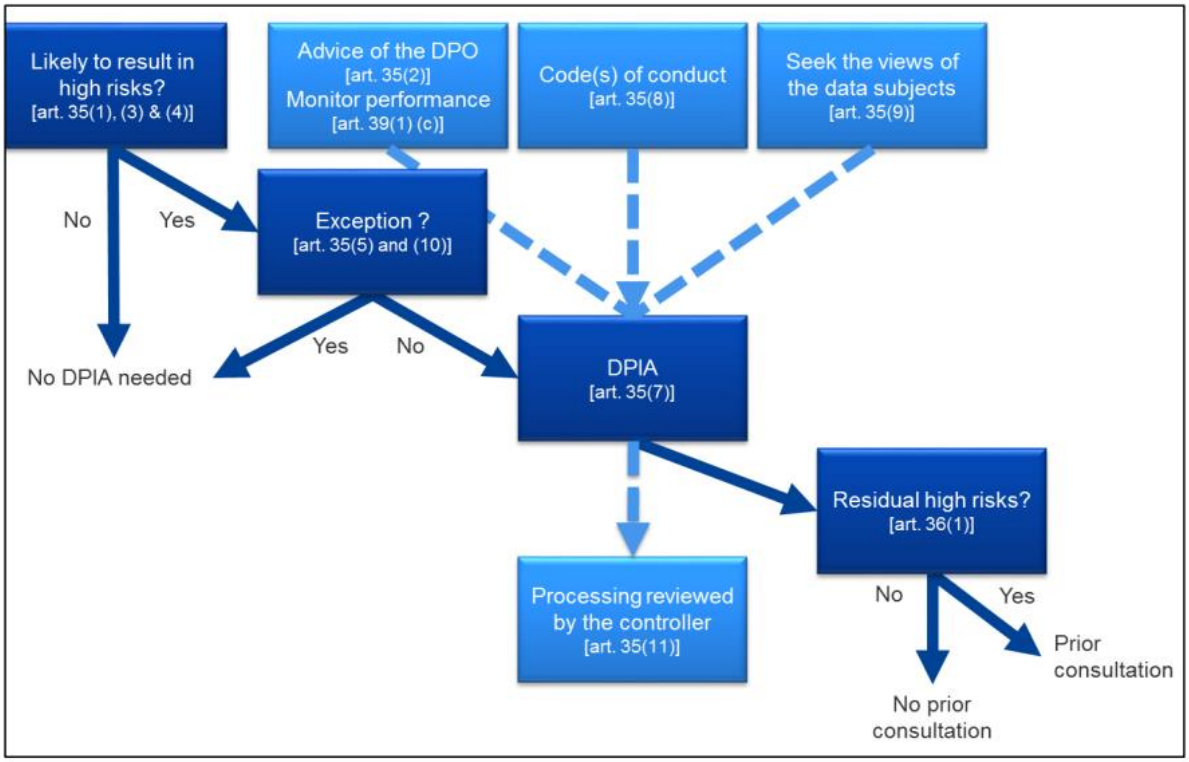
In addition to complying with national laws on data protection, for data processing to be **lawful** according to the GDPR, at least one of the following provisions must be met (Article 6(1)):

1. *the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
2. *processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
3. *processing is necessary for compliance with a legal obligation to which the controller is subject;*
4. *processing is necessary in order to protect the vital interests of the data subject or of another natural person;*
5. *processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
6. *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

The data subject's reasonable expectations must be considered in balancing interests (Recital 47).

Does the video surveillance system affect the data subject's rights? If so, does it violate their rights? This has to be balanced against the controller's needs and legitimate interest. Consider, for example, a video surveillance system which was installed to prevent theft from within a parking lot, and the filming of the parking lot is also protecting the data subjects' interest by protecting their cars while parked in the lot. If the filmed area is not being used by the data subject for recreational purposes, the legitimate interest of the controller to secure the parking lot with video surveillance overrides the data subject's right to not be monitored.

The resources and level of detail involved in a data protection impact assessment are proportional to the risks and extent of the proposed video surveillance system. Whether or not the assessment is a **formal** data protection impact assessment, it should be recorded in writing.



The above diagram illustrating the process of assessing whether to conduct a formal DPIA is from *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.*

The potential abuse of video surveillance can violate data subjects' rights, such as:

- Sharing footage with users without access rights
- Recording data subjects' activities without consent
- Using footage to intimidate or coerce data subjects
- Monitoring the behaviour and actions of employees

If the data protection impact assessment "indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk", the controller must consult the supervisory authority before data processing (Article 36).

For further information on the *Data Protection Impact Assessment,* see Appendix 1: Document Templates.

5.3.4 Cameras

Additional functions – such as zoom capability, unlimited movement of cameras, analysis and audio recording functions – must be deactivated if not necessary for the initial processing purpose.

5.3.5 Boundaries of surveillance

✓ Ensure that the areas of surveillance comply with the GDPR.

Generally, the surveillance must end at the property's boundaries in the event of it being used for the security surveillance of that premises. However, if filming goes beyond the boundaries of the premises, the controller should block out areas not needed for security surveillance, using means such as pixelating non-relevant areas.

Physical areas where data subjects' rights and legitimate interests will often override the controller's legitimate interests to film are those used for recreational activities, and public areas typically used for "recovery, regeneration, and leisure activities", as well as sitting areas, restaurants, parks, and fitness facilities.

When creating video surveillance policies and procedures, consider the following:

1. Carrying out a DPIA.
2. The role and person responsible within the organisation for the management and operation of the VSS.
3. The purpose of the video surveillance.
4. Where and when the video surveillance is allowed and not allowed – for example, in the case of hidden cameras.
5. Transparency and information obligations.
6. How video is recorded and for what duration (this would include procedures regarding archiving stored footage relating to security incidents).
7. Which staff need to be trained in relation to these changes, and when.
8. Who within the organisation has access to the footage, and for what purposes?
9. Operational procedures, such as what response is followed in the event of a data breach.
10. Procedures for data access requests.
11. Procedures for VSS "procurement, installation and maintenance" (*EDPB Guidelines*).

5.4 Profiling and automated decision-making

✓ When the data controller's processing operations constitute automated decision-making, the controller needs to meet the GDPR requirements in this regard (Rights in relation to automated individual decision-making, including profiling - Article 22).

5.5 Right to be informed

Article 12 of the GDPR states that the data controller "shall take appropriate measures"

> *to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language…*

If a data subject requests information under Articles 15 to 22, the data controller must provide the subject with this information "without undue delay and in any event within one month of receipt of the request".

✓ Data controllers should know the purpose for which they collect personal data. This purpose needs to be lawful and documented.

✓ Data controllers must ask for the consent of data subjects, record that consent, and carry out a review of the way in which it requests, records and manages consent.

✓ As a Data Controller, it is your company's responsibility to provide information about its data protection activity to data subjects. This includes the following actions:

- Provide information on-site where data will be collected from data subjects (Article 13).
- When the data subject is a child, privacy information should be communicated in a way that children would understand (Recital 58).
- Provide information where personal data will be collected from someone who is not the data subject (Article 14).
- Publish your privacy policy information online and in company reports.
- Provide data subjects with information about the processes to follow if they wish to lodge complaints or queries about their personal data.
- Respond to data subject requests timeously (Article 12).

The data controller should adopt a layered approach of methods to ensure transparency. The first layer is the **notice** to the data subject that they are being filmed or observed "using automated data capturing devices or data capturing software such as cameras" (EDPB guidelines, page 21). The second layer should be accessible to data subjects without entering the monitored area.

For more information on the on-site *Privacy Notice* see Appendix 1: Document Templates.

5.5.1 Data breach

A data breach, as the GDPR defines, is 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".

- "Destruction" would mean that the data no longer exists.
- "Damage" would mean that the data has been altered, corrupted or is no longer complete.
- "Loss" would mean that the data may still exist, but the controller has lost access to it.
- "Unauthorised or unlawful processing" would mean disclosure of the personal data to unauthorised recipients.

A breach is a security incident, but only one which involves personal data. It is a breach when the incident means that the controller is unable to adhere to the Article 5 principles of the GDPR. Thus, as the Article 29 Data Protection Working Party points out, while "all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches".

In the event of a data breach, data controllers must have systems in place to notify the competent national supervisory authority, and in some cases notify the relevant data subjects and parties involved, "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" (Article 33). When controllers notify the relevant authority, they can also obtain advice on whether or not to notify the individuals affected.

The DPO can assess whether notification is necessary based on these terms. There must also be procedures to prevent a breach from reoccurring. Processors play a role here, as they must notify controllers of personal data breaches. The focus of the breach response plan should always be to protect individuals and their personal data. Failing to report a breach can result in a sanction to the controller under Article 83.

Two elements are key in a breach scenario:

- Having a data security policy which aims to prevent a breach.
- Reacting timeously to a breach if it occurs, mainly as a result of having procedures and policies already in place to facilitate a rapid response.

Types of breaches

The Article 29 Data Protection Working Party groups breaches into three categories:

- Confidentiality breach: unauthorised or accidental disclosure of personal data
- Integrity breach: unauthorised or accidental alteration of personal data
- Availability breach: unauthorised or accidental loss of access to personal data (or destruction of personal data)

When implementing technical and organisation measures to ensure a level of security appropriate to the risk, controllers need to consider:

- "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services", and
- "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".

A security incident in which data is unavailable for a period of time (not a planned maintenance shutdown) is classified as a breach, because the lack of access impacts the rights and freedoms of natural persons. As with any breach, this should be documented in accordance with Article 33(5).

✓ Whether the notification obligation is triggered would depend on the degree or likelihood of risk to the rights and freedoms of natural persons and would be decided on a case-by-case basis.

Failure to notify

Recital 87 emphasises the importance of identifying a breach using "all appropriate technological protection and organisational measures", assessing its risk and notifying the relevant stakeholders "without undue delay". The notification "may result in an intervention of the supervisory authority".

Where a breach notification is required but not carried out, the relevant supervisory authority can impose an administrative fine of up to 10M€ or 2% of the total worldwide annual turnover of the undertaking concerned, as stipulated under Article 83(4)(a), on its own, or as an accompanying corrective measure as set out under Article 58(2).

If the breach notification failure occurred due to the absence of adequate security measures, the supervisory authority would need to issue sanctions for *that* security measure failure (Article 32) as well as sanctions for the failure to notify (Article 33 and 34), as these are separate infringements.

The personal consequences of breaches

Consequences to natural persons due to a data breach could include:

- Loss of control over their personal data
- Limitation of their rights
- Discrimination
- Identity theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy

When to notify

It is crucial to know when to notify. Article 33(1) states that in the case of a personal data breach,

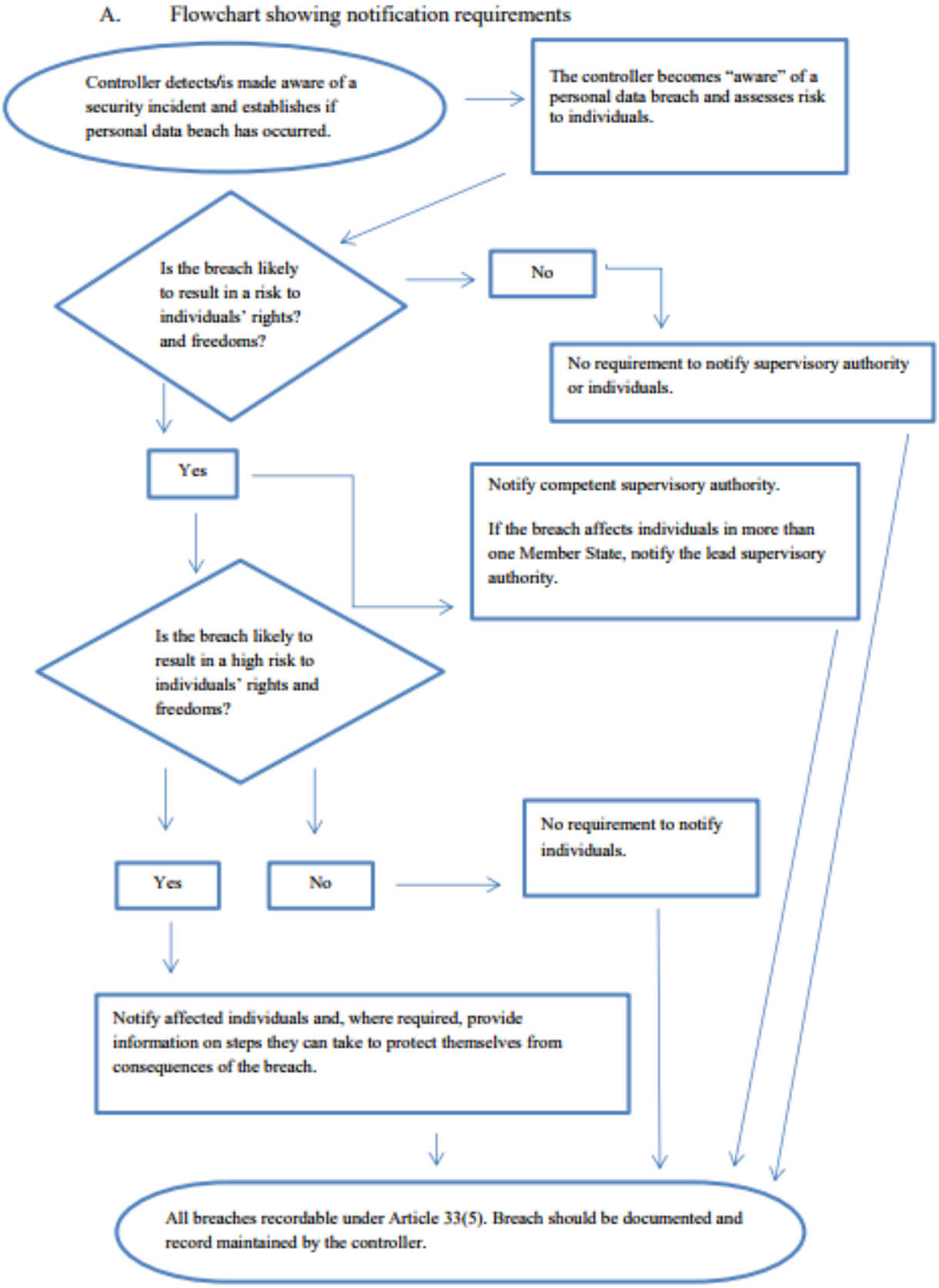
> the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The Article 29 Data Protection Working Party considers that a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

When communication is *not* required

There are three instances where communication is not required as set out in Article 34(3):

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.



The flow chart of the notification requirements regarding a data breach is from *Guidelines on Personal data breach notification under Regulation 2016/679*, as is the table below.

Example	Notify supervisory authority?	Notify the data subject?	Notes
A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state-of-the-art algorithm, backups of the data exist, the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However, if it is later compromised, notification is required.
A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or confidentiality. However, if the supervisory authority became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.

An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.	Yes.	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes that additional step of notifying other individuals if there is high risk to them.
A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross-border processing.	Yes, as could lead to high risk.	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. The controller should also consider any other notification obligations, e.g. under the NIS Directive as a digital service provider.
A website hosting company acting as a data processor identifies an error in the code which controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay. Assuming that the website hosting company has conducted its own investigation, the affected controllers should be reasonably confident as to whether each has suffered a breach and there is likely to be considered as having "become aware" once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority.	If there is likely no high risk to the individuals they do not need to be notified.	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS Directive as a digital service provider). If there is no evidence of this vulnerability being exploited with any of its controllers a notifiable breach may not have occurred but it is likely to be recordable or be a matter of non-compliance under Article 32.

Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
A direct marketing email is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequence.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

✓ Data controllers must have an information security policy which has procedures to identify, report, manage and resolve personal data breaches.

✓ Notify data subjects of personal data breaches "without undue delay" when the "personal data breach is likely to result in a high risk to the rights and freedoms of natural persons" (Article 34).

✓ Data controllers must notify the Supervisory Authority (Article 55) of personal data breaches within 72 hours "without undue delay" (Article 33).

For more on *Data Breach Notification*, see Appendix 1: Templates for CathexisVision clients.

5.6 Data Subject Requests

The right of individuals to access and receive a copy of their personal data and related information is commonly referred to as a **subject access request** (SAR). This right enables individuals to know the controller's purpose in using their personal data and allows them to check that the controller is carrying out this purpose lawfully. Such a request may be made verbally or in writing, including via social media. The individual is entitled to:

- Confirmation that their data is being processed by the controller
- A copy of their personal data
- Other supplementary information
- Information explaining the controller's purposes for processing the personal data
- Information regarding the categories of personal data being processed
- Notice of the retention period for storing the data or the controller's policies in this regard
- Information about the individual's rights, such as their right to rectification, erasure or restriction or to object
- Information regarding the source of the data
- Clarification on whether the controller makes use of automated decision-making (including profiling), as well as the impact of the processing on the individual
- Elaboration on the security precautions taken by the controller where the personal data may be transferred to a third-party or international organisation.

Generally, most of this information will be in the initial privacy notice or warning signs given before gathering the data.

The data subject or individual making the request does not need to refer to a specific contact within the controller's organisation or refer to relevant legislation. In addition, a third party (for instance, a friend, family member or attorney) may make a SAR on behalf of someone else, but that third party must produce evidence of their authorisation to act on behalf of the data subject.

✓ Data controllers need to have a procedure for responding to requests by data subjects.

✓ Notably, only controllers, not processors, are responsible for answering SARs.

✓ It is advisable that clauses in the Data Processing Agreement set out how the processor can assist the controller in meeting their SAR obligations. For example, if processor holds copies of the data, they would need to give the controller that copy in order to fulfil the SAR, or the processor might need to search for the relevant data on the controller's behalf.

✓ In the case of joint controllers, this needs to be addressed in their contractual provisions, but it is advisable to make each controller aware of each SAR.

5.6.1 Access, rectification and restriction of processing

Along with the right to be informed if their data is being stored or processed, data subjects have the right to access a copy of their data and information about it (Article 15).

If data is not stored, but only filmed in real-time and not held beyond the moment of filming, the controller would not be able to give any access to the data – only the information that no data is being held.

✓ Controllers must respond to SARs timeously and no later than one month after the request has been received. However, in the case of a more complex request or a series of requests, the time limit may be extended to two months.

✓ There are some limitations which might apply to the right to access.

✓ The information a data controller provides to a data subject (see Right to be informed and Articles 15 to 22) "shall be provided **free** of charge" (Article 12(5)).

However, if the requests are "manifestly unfounded or excessive, in particular because of their repetitive character", the controller may:

a. *Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or*
b. *Refuse to act on the request.*

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 15(4) states that the data subject has the right to a copy of the personal data being processed only if it shall "not adversely affect the rights and freedoms of others". The controller may also refuse the request if an exemption or restriction applies or if the request is unjustified or excessive. If the request involves information about another individual, the controller does not necessarily need to fulfil the request, unless they can obtain the other individual's consent, or it is reasonable to fulfil the request without the other individual's consent.

According to the Information Commissioner's Office, the controller is not required to conduct searches that would be "unreasonable or disproportionate to the importance of providing access to the information". In that situation, the controller would need to explain the reasons why the individual's request cannot be fulfilled. The controller also needs to provide information about the individual's right to complain to a supervisory authority in their member state, as well as their entitlement to seek to enforce their right via the court system.

In all other cases, the controller must carry out a reasonable search for requested data.

When a data subject wishes to see footage containing persons in addition to the data subject, viewing such footage would constitute additional processing of the personal of the other data subjects, which would adversely their rights and freedoms. The controller needs to address this issue on a case-by-case basis. However, this hurdle may not be used by the controller as a means of preventing data subjects' legitimate claims to their data from being fulfilled. Technical measures – such as image editing via masking or scrambling – should be utilised to fulfil such access requests.

Article 11 states that if the "purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this regulation". In such cases, when "the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification".

The data controller needs to ensure that the personal data held is accurate and current (Right to rectification - Article 16).

When data is transferred to a data subject, security measures need to be in place. (See Exporting data below.)

If the data controller would have to search through a significantly large amount of stored footage to find the data subject that has requested the data, the controller may not always be able to find the footage of the data subject.

- It is advisable for the data subject to give the controller a specific time frame within which to find the footage of the data subject within the monitored area.
- The controller needs to notify the data subject first regarding the qualifiers it would need to assist in the search through the stored data.
- If the search is still futile, the controller must notify the data subject of this fact.

Data controllers should have procedures to respond to data subjects' requests to restrict the processing of their personal data (Article 18). Individuals have this right when they are contesting the accuracy of their personal data and the organisation holding it is busy with verifying the data accuracy, or when the organisation no longer needs the data but it needs to be stored for a legal claim. The main methods used to restrict processing are to temporarily move the data to another processing system, to make the data unavailable to users, or to temporarily remove data from a website.

For more information on *Data Subject Requests*, see Appendix 1: Document Templates.

Useful links on the right of access:

- The European Commission's response to "What personal data and information can an individual access on request?"
- The Information Commissioner's Office summary of the right of access.
- The Handbook on European data protection law – the right of access to an individual's own data (p. 216).

5.6.2 The right to be forgotten (the right to erasure)

Article 17 of the GDPR outlines the data subject's right to "obtain from the controller the erasure of personal data concerning him or her without undue delay" under certain conditions, one of which being if the personal data is no longer necessary for the original purpose it was gathered.

The right to be forgotten applies when data is being processed beyond real-time filming or monitoring.

The conditions (Article 17(1)) under which a data subject can request data erasure, or in which a data controller is obligated to erase personal data are:

- The personal information is no longer necessary for the purpose for which it was gathered
- The data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) or point (a) of Article 9(2), and where there is no other legal ground for the processing
- The data subject objects to the processing (see Right to object) according to Article 21(1), or the data subject objects to the processing and there are no overriding legitimate grounds for the processing
- The processing of the data has been unlawful
- The data controller is subject to European Union or Member State law and the personal data needs to be erased to comply with these legal obligations
- The personal data has been collected in relation to the offer of information society services referred to in Article 8(1).

Data controllers must retain video footage for as long as it meets the stated purpose of the surveillance system, and dispose of personal data securely once it is no longer needed.

The controller should, to a reasonable extent, attempt to "communicate any rectification or erasure of personal data or restriction of processing carried out [...] to each recipient to whom the personal data have been disclosed" (Article 19). See Exporting data.

✓ If the data subject requests this information, the data controller must inform the data subject about the recipients with whom that the data controller has shared the personal data (Article 19).

✓ If the right to erasure does apply, the information must be deleted from both live and backup systems. If backup systems take longer than one month to update, the organisation must tell the data subject about this. That backup data must be put "beyond use" until such time as it is erased, if it cannot be immediately overwritten.

If the data controller has made the personal data public and is obliged to erase the data, "the controller, taking account of **available technology** and the **cost of implementation**, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data" (Article 17(2)).

Article 17(1) and (2) shall *not* apply "to the extent that processing is necessary":

- *For exercising the **right of freedom of expression and information***
- *For **compliance with a legal obligation** which requires processing by Union of Member State law to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*
- *For reasons of **public interest in the area of public health** in accordance with points (h) and (i) of Article 9(2) and Article 9(3)*
- *For **archiving purposes in the public interest**, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing, or*
- *For the **establishment, exercise or defence of legal claims**.*

In a video surveillance system, it is not reasonable to erase an individual from video footage, but it is possible to controller how long recordings are kept.

If the controller can blur the footage without it being able to be recovered, such personal data is considered erased under the GDPR.

5.6.3 Right to object

The data subject has the right to object, "on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions" (Article 21). In the context of surveillance for direct marketing, the data subject's right to object is absolute: the data subject may object to the processing on a discretionary basis.

If a data subject objects to the surveillance, the controller will need to show that it has a ***compelling*** legitimate interest (see Video Surveillance Policy) that is sufficient to override the rights of the data subject, or that the surveillance is needed for a legal claim. The legitimate interest must be genuine, real-world, and not "fictional of speculative". In the case of surveillance for security purposes, there needs to be a "real-life situation of distress" at hand which would mean a past event proves a need for security surveillance. The European Data Protection Board advises that "given a real and hazardous situation, the purpose to protect property against burglary, theft or vandalism can constitute a legitimate interest for video surveillance".

Data controllers should have procedures for handling data subjects' objections to the processing of their personal data.

A data subject may object to the filming at any point from before entering until after leaving the monitored area. Without both compelling and legitimate grounds, the data controller's monitoring of the area is only lawful if the controller can immediately stop the processing of personal data if requested. Alternatively, it is only lawful if the area is restricted so that a controller can be assured that the data subject has given approval before entering. Thus the restricted area cannot be an area that a data subject has a right to access by way of their citizenship.

5.7 Security and storage

5.7.1 Storing data

Personal data may not be stored longer than necessary for the purpose for which it is being processed (Article 5). The decision to store data should be "controlled within a narrow timeline" (EDPB Guidelines). For example, filming to detect damage to property from vandalism would only need to be stored for a few days, as such an incident would have been detected by that stage. Due to the principles of data minimisation and storage limitation, such footage would then be deleted.

The longer footage is stored, the greater the argument needed to justify the necessity of storage and the legitimacy of its purpose.

If the controller intends to store the data, doing so must be necessary for the purpose of the processing. The storage period needs to be set and defined for the particular purpose. It is the controller's responsibility to do this in accordance with the GDPR provisions as well as its principles of necessity and proportionality.

Storage of footage can be approached in various ways to avoid risk for data subjects, and for the organisation to prevent accidental breaches of GDPR provisions. The "Black Box" approach allows for footage to be automatically deleted (after a set storage period) but still available to be accessed in the event of an incident. Another solution might be to opt not to record and use "real-time monitoring" of the footage.

Implement security measures to protect the personal data being held.

Dispose of data securely.

CathexisVision 2020 offers optional database shredding, which enables permanently destroying video older than the user-defined recording limit.

5.7.2 Exporting data

The general regulations of the GDPR apply in the case of disclosure of video footage to **third parties** because such disclosure is a type of processing of the personal data. The controller therefore needs to meet the requirements of Article 6, such as obtaining consent from the data subject.

Third parties are defined in Article 4 (10) as a "natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct

authority of the controller or processor, are authorised to process personal data". Both the third party and the controller have to assess the legality of the processing (which, in the case of the third party, would be the reception of the material) under Article 6. In the case of disclosure of video footage to a **law enforcement** agency, Article 6 (1) (c) states that such processing is legal if it is to comply with a legal obligation which applies to the controller.

- ✓ Data controllers need to allow for personal data to be moved, copied, or transferred by the data subject in a safe and secure manner (Right to data portability – Article 20).

- ✓ If the controller transfers personal data outside of the EU, security needs to be in place to protect this data. Data controllers need to comply with international restrictions on the transfer of personal data outside of the EU.

- ✓ If the data controller has rectified, erased or restricted the processing of personal data (in accordance with Articles 16, 17 or 18), then the controller needs to communicate this to "each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportional effort" (Article 19).

- ✓ When transferring data to a data subject (in response to a Subject Access Request), the data controller needs to ensure that this transfer is done securely, and in an accessible, concise, intelligible format.

✓ **Security measures when transferring data:**

- Have proper systems in place to record Subject Access Requests.
- Train staff who will handle SARs.
- Before responding to a request, check addresses.
- When sending information electronically, it is advisable to provide it in an encrypted form.
- Send a passphrase separately to the individual.
- If sharing a hard copy of information, using a courier or special delivery is good practice.
- Providing remote access to a secure system, so that the data subject can download a copy, can support the secure transfer of information.
- It is practical, and good practice, for the data controller to find out the format in which the data subject would prefer to receive the information before fulfilling the access request.

5.7.3 Processing biometric data

In accordance with the data minimisation principle, and when assessing data subjects' interests and rights, it is advisable to design a system which either does not capture, or minimises the capturing of footage revealing sensitive personal data.

If the purpose of the use of the video footage is to ascertain special categories of data, Article 9 applies. When the surveillance system does capture and process special categories of personal data, the controller needs to fulfil these two requirements:

1. Identify an exemption to the general rule in Article 9 prohibiting such processing, and
2. Identify a legal basis for the processing under Article 6.

Processing special categories of personal data means that the controller needs a far higher level of caution and security, and possibly a formal Data Protection Impact Assessment.

It is rare for exemptions to apply to video surveillance. For example, controllers cannot rely on the exemption in Article 9(2), which allows processing of special categories of data related to "data which are manifestly made public by the data subject". If data subjects allow themselves to be filmed, this does not imply that they have made their special categories of data public simply by being within the camera range.

5.7.4 Biometric data

According to the GDPR, biometric data "means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic [fingerprint] data". Mere video footage of an individual does not qualify as biometric data unless it is processed in a way which meets the definition provided in Article 4 – this would mean that the data would be processed to contribute to the unique identification of the individual.

Biometric data use, and particularly facial recognition "entail heightened risks for data subjects' rights" and the controller must carefully assess the impact on the rights of the data subjects, and even consider other means of surveillance.

The controller must not make consent to biometric processing a condition to making use of and accessing its services. There must always be an alternative authentication solution available for the data subject, which does not involve biometric processing and does not involve additional costs or restraints for the data subject.

The EDPB advises that biometric data can be classified with three criteria:

1. **Nature of data**: the data must relate to physical, psychological or behavioural characteristics of a natural person.
2. **Means of processing**: the data must result from a "specific technical processing".
3. **Purpose of processing**: the purpose must be to uniquely identify a natural person.

When the processing is to distinguish a category of people, as opposed to uniquely identifying an individual, then Article 9 does not apply. For example, if a shop uses video surveillance to capture gender and age characteristics of its customers for advertising purposes, the processing does not fall under Article 9 because it is used to classify people, not to uniquely identify a person or people.

However, if the shop/data controller did install a **facial recognition** video system, it would first need the "explicit and informed consent" of all the individuals being filmed. If the system captured the footage of any individual or passer-by who had not consented filming for such a biometric template, this behaviour would be considered unlawful, even if the biometric template were deleted after the shortest period possible. Consent must be obtained first.

Another approach would be to set up two entrances – one to capture biometric data and one which does not. Crucially, the entrances would need to be arranged to ensure that no non-consenting individuals might accidentally pass through the entrance capturing biometric templates.

✓ **The EDPB suggests the following to minimise risks while processing biometric data:**

1. DATA MINIMISATION: only extract data from the digital image which is required for the purpose and nothing beyond that.
2. DATA PROTECTION: ensure that templates cannot be "transferred across biometric systems".
3. DATA STORAGE SECURITY: such a setup may need to include "encrypting the template using a cryptographic algorithm" but either way, measures must be taken to avoid unauthorised access to the template's storage location.
4. ACCOUNTABILITY: steps must be taken to preserve the "availability, integrity and confidentiality" of the data being processed.
    a. "Compartmentalise data during transmission and storage,
    b. store biometric templates and raw data or identity data on distinct databases,
    c. encrypt biometric data notably biometric templates,
    d. define a policy for encryption and key management,
    e. integrate an organisational and technical measure for fraud detection,
    f. associate an integrity code with the data (for example signature or hash), and
    g. prohibit any external access to the biometric data".
5. DELETION OR ERASURE OF DATA: ensure that the raw data is effectively deleted. The concern is that a biometric data base can be derived from the raw data and must then also be deleted obviously. In the case where the raw data needs to be retained though it must be kept in such a way that a biometric template cannot be created again – for instance by using a "noise-additive method" such as watermarking. If there is a security breach and unauthorised access to stored biometric data takes place, then such data must be deleted. The controller must also delete any data not needed for processing "at the end of the biometric device's life".

5.7.5 CathexisVision cybersecurity

By strengthening their organisation's cybersecurity measures, data controllers strengthen their compliance with the GDPR, especially the following articles:

- Article 5(1)f, which specifies that data should be processed "in a manner that ensures appropriate security the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".
- The data controller needs to "implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation" (Article 24).
- Article 32, regarding Security of processing, stipulates that data controllers need to take into account "the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed". Moreover, controllers or processors need to make sure that an individual "acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law".
- In the event of a data breach, the supervisory authority might need to be notified (Article 33).

The National Cyber Security Centre is a UK government organisation that advises the public and private sector on how to prevent threats to computer security.

To ensure that video footage does not get into the public domain, CathexisVision has the ability to:

- Archive video that can only be played back under password control.
- Overlay a watermark on the video to depict the source of the information (for example, user info).

Communication between CathexisVision components

CathexisVision ensures secure communications between its components, including Recording servers to clients, other recording servers, video walls, and alarm management gateways. The security of communication between thesecomponents is achieved by the following measures:

1. All external site connections support encryption of varying levels:
   - Disabled
   - Minimal (only critical connections encrypted)
   - Secure (the default option, which encrypts all connections except those with high-volume video)
   - All (all connections encrypted, including high-volume video links)
2. Passwords are never stored as plain text and instead are hashed using SHA512 (from CathexisVision 2017).
3. Login credentials are negotiated using Diffie-Hellmann key exchange and signed with an RSA private key (supports 1024 and 2048 RSA keys).
4. Encryption on network channels is performed using AES128/GCM with unique cipher keys negotiated per connection.
5. HMAC is used for integrity verification.
6. Public Key Infrastructure (PKI) is managed internally by Cathexis for added security.

Archiving

1. The integrity of the videos is secured using dual RSA1024 keys (for signing).
2. Optional encryption is performed using AES128 block encryption with a randomised IV per block and a user-generated pass-phrase.
3. Video can be watermarked to indicate the source of the information (i.e. user info)
4. The video footage and metadata can only be played via a proprietary Cathexis Archive Video Player.
5. Exported/archived video may be restricted to password-controlled playback.

Further information on CathexisVision archive security can be found in Appendix 2: Cathexis Security.

5.7.6 System and third-party security

Peripheral equipment

Cathexis works with technology partners and other industry players to increase the security of the products and protocols to which CathexisVision connects. In general, connection with IP cameras includes the following:

Camera configuration	• HTTP: hypertext protocol • Encryped ssl/tls • Supported by CURL (client-side URL transfer library).
Camera control	• RTSP – real time streaming protocol. • HTTPS encrypted camera connection control (where supported by the manufacturer).
Video streaming	• RTP – real time transport protocol. • Encrypted video streaming (where supported by the manufacturer).

IT considerations

Network access: the first step in any system is to ensure that access to the network is properly controlled. There are various techniques for this, which should be adopted by any networking company. These include firewalls, Intelligent Network Switches, Managed networks, and controlling "physical" access to the network.

Operating System lockdown: in order to attack software, access must be gained through the operating system on the system on which the software is running. It is important to ensure that the OS is "locked down" to prevent unauthorised access. This can be done in several ways, including:

- Preventing the opening of unauthorised ports enabling use of items such as ftp, telnet, email. If any communication needs to occur via these means, then one needs to ensure that security protocols like SSH/SFTP are utilised
- Disabling "root" access to the OS
- Ensuring strong password levels
- Adding anti-virus and anti-malware software, which is continuously updated
- Restricted internet access.

6. Guidelines for Joint Data Controllers

Regardless of the arrangement between the joint data controllers, each controller is responsible to comply with the GDPR in its entirety. Due to the relationship between the joint controllers regarding the data being processed, there are also additional responsibilities for joint controllers.

- Joint controllers must put a transparent arrangement or contract in place, which sets out their respective roles and responsibilities.
- The arrangement or contract must be made available to data subjects.
- Joint controllers must agree and be transparent about how both controllers will comply with the GDPR. They need to be clear about their compliance with the accountability and transparency principles, and the ways they will protect individuals' rights.
- The Data Protection Impact Assessment should set out which joint controller is responsible for which specific measures to deal with the inherent risks and to protect the rights and freedoms of data subjects.

7. Guidelines for Data Processors

If an organisation employs a data processor to carry out some of its video surveillance, it must ensure that the data processor complies with the GDPR. Although data processors have less decision-making power over the data they process and fewer responsibilities under the GDPR than data controllers, they must still comply with various obligations.

- ✓ Sign and adhere to a Data Processor Agreement.
- ✓ If the organisation is based outside the EU but offers services to individuals within the EU, it should appoint a representative within the EU.
- ✓ Processors are directly obligated to adhere to the GDPR's prohibition on transferring personal data outside the European Economic Area.

7.1 Keep a record

- ✓ To ensure compliance with the GDPR accountability principle for instance by maintaining records and appointing a data protection officer.

7.2 Keep personal data secure

- ✓ To implement security measures to protect the data from threats such as accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.

7.3 Assist the data controller

- ✓ Enter into and comply with a contract with the data controller, which is binding and contains the compulsory provisions.
- ✓ Only process personal data as (lawfully) instructed to do by a controller. Processing the data for any other purposes outside of those instructions, such as for the processor itself, will cause the processor to essentially become a controller and in breach.

- ✓ Do not employ a sub-processor without authorisation from the data controller. Where that authorisation is permitted, have a similarly binding contract with the sub-processor, which protects personal data.

- ✓ Notify the controller without delay in the instance of a data breach, or if any of their instructions would result in a breach of the GDPR.

- ✓ Ensure that any transfer of data outside of the EU is authorised by the controller and complies with the relevant provisions within the GDPR.

8. Conclusion

If an organisation installs a CCTV system, it needs to carry out a **Data Protection Impact Assessment**, which would identify and document the impact the installation would have on the privacy rights of data subjects or individuals affected. The organisation also needs to review whether CCTV is the **best security solution** in the context of those rights.

The organisation needs to **nominate** someone within it to be responsible for the operation of the CCTV system, and to draw up a **policy** covering the use of the system, including the relevant GDPR-required procedures. **Staff training** needs to be carried out to educate staff on how to operate the CCTV system and deal with requests for footage.

Procedures need to be in place to respond timeously to **data subject access requests** to view the CCTV footage. The footage must only be **retained** for the necessary amount of time. What constitutes a "**necessary**" period of time needs to be set out and pre-defined within the policy concerning the use of the footage. The footage needs to be clear and of a high quality, and stored **securely**. Only **authorised** individuals should have access to the footage. To comply with the terms of fair processing and transparency, the organisation must **inform** individuals of its use of CCTV.

8.1 Useful links

- The full text of the GDPR.
- A complete guide to GDPR compliance.
- The Information Commissioner's Office Guide to the GDPR.
- The European Data Protection Board's set of guidelines, recommendations and best practices on the GDPR.
  - The European Data Protection Board's guidelines on processing personal data through video devices.
  - Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.
  - Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.
- The Information Commissioner's Office Data Protection Code of Practice for Surveillance Cameras and Personal Information.

Appendix 1: Document templates

Data Processing Agreement

A Data Processing Agreement template is available on the GDPR website.

It is advisable for the Data Processing Agreement to cover how the processor will assist the controller in responding to subject access requests.

Data Protection Impact Assessment

The GDPR gives controllers flexibility to determine the structure and form of their DPIA. The DPIA implementation is scalable, so that even a small data controller can implement a DPIA suitable for their processing operations. The data protection impact assessment shall contain, at least:

a. *a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
b. *an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
c. *an assessment of the risks to the rights and freedoms of data subjects [...]*
d. *the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*

- To align with the principles of data protection by design and default, the DPIA should be done prior to the processing (even if some details are unknown at that stage).

- The controller is responsible to ensure that the DPIA is done and must consult the Data Protection Officer (Article 35(2)). If a data processor is doing all or part of the processing, the processor should assist the controller in performing the DPIA (Article 28(3)(f).

- The controller must "seek the views of data subjects or their representatives [...] where appropriate" (Article 35(9)). This can be done through questionnaires, surveys, or studies, for example. This is not the same as gaining consent from a data subject. If the controller does not seek the views of data subjects (for example, for reasons of business confidentiality), the reasons for this must be documented.

- ✓ The DPO should "monitor the performance" of the DPIA (Article 35(1)(c)).
- ✓ These is no legal obligation to publish the DPIA, but publishing it (or a summary) can foster trust. In certain situations, the relevant supervisory authority might require the full DPIA.

Annex 2 – Criteria for an acceptable DPIA

The WP29 proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

- ☐ a systematic description of the processing is provided (Article 35(7)(a)):
  - ☐ nature, scope, context and purposes of the processing are taken into account (recital 90);
  - ☐ personal data, recipients and period for which the personal data will be stored are recorded;
  - ☐ a functional description of the processing operation is provided;
  - ☐ the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
  - ☐ compliance with approved codes of conduct is taken into account (Article 35(8));
- ☐ necessity and proportionality are assessed (Article 35(7)(b)):
  - ☐ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
    - ☐ measures contributing to the proportionality and the necessity of the processing on the basis of:
      - ☐ specified, explicit and legitimate purpose(s) (Article 5(1)(b));
      - ☐ lawfulness of processing (Article 6);
      - ☐ adequate, relevant and limited to what is necessary data (Article 5(1)(c));
      - ☐ limited storage duration (Article 5(1)(e));
    - ☐ measures contributing to the rights of the data subjects:
      - ☐ information provided to the data subject (Articles 12, 13 and 14);
      - ☐ right of access and to data portability (Articles 15 and 20);
      - ☐ right to rectification and to erasure (Articles 16, 17 and 19);
      - ☐ right to object and to restriction of processing (Article 18, 19 and 21);
      - ☐ relationships with processors (Article 28);
      - ☐ safeguards surrounding international transfer(s) (Chapter V);
      - ☐ prior consultation (Article 36).
- ☐ risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):
  - ☐ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
    - ☐ risks sources are taken into account (recital 90);
    - ☐ potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
    - ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
    - ☐ likelihood and severity are estimated (recital 90);
  - ☐ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);
- ☐ interested parties are involved:
  - ☐ the advice of the DPO is sought (Article 35(2));
  - ☐ the views of data subjects or their representatives are sought, where appropriate (Article 35(9)).

The above Annex outlines the criteria to assess whether a DPIA complies with GDPR is from *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.*

Record of Processing Activities

The Information Commissioner's Office website has templates for controllers and processors.

Data Subject Access Request

Article 15 stipulates that when a data subject accesses their personal data, they should be provided with the following information:

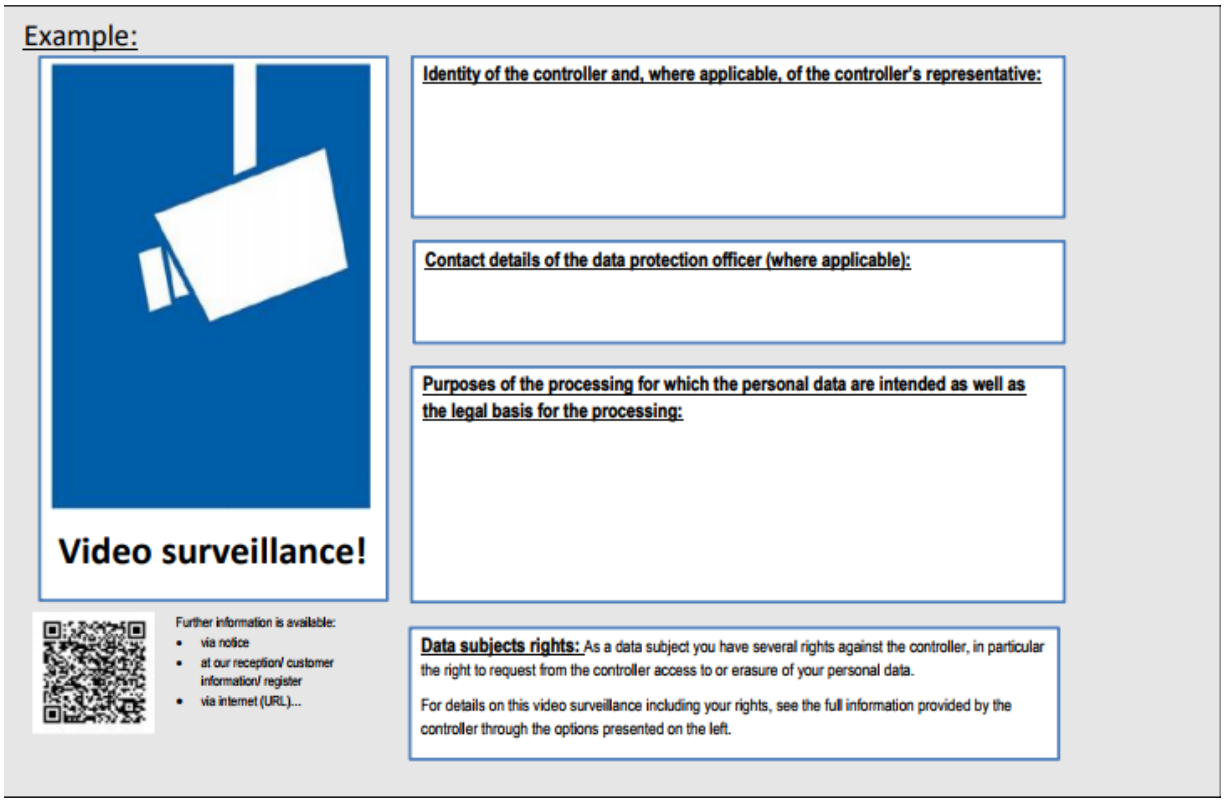
a. *The purposes of the processing;*
b. *The categories of personal data concerned;*
c. *The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;*
d. *Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;*
e. *The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;*
f. *The right to lodge a complaint with a supervisory authority;*
g. *Where the personal data are not collected from the data subject, any available information as to their source;*
h. *The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*

✓ The information requested must be disclosed to the data subject securely and in an accessible, concise, intelligible format.

For example, if the SAR was made electronically, the controller should provide the requested data in a commonly used electronic format. It is practical and good practice to establish which format the data subject would prefer before fulfilling the subject access request. It is possible to provide other options, such as the data subject accessing their information remotely and downloading the copy themselves.

In the case of a verbal request, a verbal response may be given if the identity of the individual can be assured. It is essential to keep a record of this interaction – the date of the request, the date of the response, and the details of the individual and information given to them.

Privacy Notice



This example is taken from the *EDPB Guidelines 3/2019 on processing of personal data through video devices* (page 23).

FIRST LAYER OF INFORMATION

The Privacy Notice is the primary way that a controller will communicate to the data subject that they are being filmed.

- It is advisable to use a **symbol or icon** as part of the warning sign, which conveys the fact of the filming to all potential data subjects.
- The warning sign information should be **positioned** while data subjects are still merely *potential* data subjects in that they can recognise where the filming is about to commence and as such make the decision as to whether to enter the monitored areas before they have entered it. Eye-level positioning of the sign is advisable.
- In order for a data subject to be able to avoid surveillance if they wish, there must be absolute clarity on the extent of the demarcated **area** being surveilled. However, it is not crucial for the data subject to know the actual positions of specific cameras or surveillance equipment.
- As the first layer of communication with the data subject, the warning sign must contain all of the most relevant **content** regarding the data collection, such as the purposes of filming or processing, the controller's identity, the data subject's rights, and the largest impacts of the processing.

- For example, the warning sign could include the legitimate interests of the controller or a third party as well as the DPO's contact details, and, crucially, should refer to where the second layer of information can be found.
- In addition, if there is something **unusual** or which could be reasonably surprising to a data subject, this should also be included in the warning sign, such as information regarding the storage period or the transmission of the data to third parties outside of the EU. Without such information, the data subject should be able to assume that the filming is merely a live monitoring, with no recording or transmission occurring.
- It is advisable for the first layer information to refer to a **digital** source for the second layer information, such as a website or QR-code. However, such information must also be available in a non-digital format.

SECOND LAYER OF INFORMATION

- This information must be made easily **accessible** to the data subject – for example, as a "complete information sheet available at a central location (e.g. information desk, reception or cashier)".
- The data subject must be able to access the second layer of information **without entering** the monitored or surveyed area, possibly by way of a phone number or link.

There is a sample Company Privacy Policy on the GDPR website, as well as guidelines on writing a GDPR-compliant privacy notice and policy.

Data Breach Notification

All data breaches must be documented (linked to the accountability principle in Article 5(2) and the controller's obligations under Article 24).

If the breach is not communicated with data subjects, this fact and the reasons for it must be documented.

If the breach *is* communicated, this must also be documented to retain evidence of the fact that the controller has complied with the accountability principle and other relevant GDPR provisions.

Failure to properly document a breach can trigger Article 58 (concerning the investigate powers of the supervisory authority), and result in fines being imposed on the controller under Article 83.

According to Article 33(5), the documentation of personal data breaches "shall enable the supervisory authority to verify compliance" and needs to comprise:

- The facts relating to the personal data breach
- Its effects
- The remedial action taken.

If such records contain personal data, the storage minimisation or limitation principle applies to the storage retention period, and it would be incumbent on the controller to determine this.

Communication with the supervisory authority

According to Article 33(3), the notification to the supervisory authority should:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The controller may wish to seek the advice of the supervisory authority first to ask for direction as to how or whether to communicate the breach to the data subjects. Recital 86 states that: "such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority",

respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

Communication with the data subject

When a notification is required, the main objective must be to provide specific information about how the data subjects can protect themselves post-breach. Article 34(2) states that the "communication to the data subject [...] shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)".

Communication to the data subjects must be done directly, unless this would involve disproportionate effort and, in this situation, a public communication done effectively would suffice (Article 34(3)(c)). The communication must be made clear and transparent. One way to do this is to not include the communication in the form of newsletters or regular updates, standard messages or ordinary corporate blogs, but through a combination of direct messages. Examples of direct or public messages would be SMS, email, direct message, prominent website announcements, postal communication, and prominent adverts in print media.

The controller should provide the following information, as outlined in the *Guidelines on Personal Data Breach Notification under Regulation 2016/679:*

- A description of the nature of the breach
- The name and contact details of the data protection officer or other contact point
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

The controller should advise the data subject on security protection tasks, such as changing passwords. The fundamental principle is to make sure the data subjects are notified and can understand the nature of the breach, and the announcement informs them about what they need to do to protect themselves.

Appendix 2: Cathexis Security

Archive Security

In addition to the existing login configuration options for up to 30 user types, Lightweight Directory Access Protocol (LDAP) and Windows Active Directory for enterprise level are supported. This allows for the standardisation and control of access within a customer's existing network management framework. For increased security and accountability, users can be assigned to archive profiles for which default watermarks and password protection may be set according to the user levels. Archives can be watermarked to determine the archiving user, and password protected to restrict access to archive review to desired user levels only.

Watermarks: Site users are assigned to archive profiles according to their access levels. Administrators can assign watermarks to archive profiles. When a site user performs an archive and their archive profile has had a watermark configured, the archive is watermarked by default. On review, the archive watermark will be displayed from top left to bottom right.

Password protection: Archives with password protection require the correct password to be entered in order to review. The addition of password protection to an archive can be forced in the creation of a profile. On the creation of an archive, the user has the ability, from within the selected profile, to add password protection. There are 3 password options available to the user – Custom, Fixed and Random. Multiple password options can be assigned to archive profiles. Password requirements will have to be met by all users wishing to review the archive in the CathexisVision Archive Viewer. Lost passwords are not recoverable and the archive will need to be recreated.

Signing: Archives retain an overall archive signature linking them to the source NVR. Additionally, critical portions of audio/video are independently signed and can be explicitly linked to the archiving NVR. Sub-archives (archive of already archived footage) do not contain any signatures generated by the original NVR that sourced the video data. The authenticity of these archives cannot be determined.

Verification: The verification feature produces a report on the authenticity of an archive. An archive verification report will determine whether or not the archive signature is valid and indicate whether the archive is or is not verified according to this information. Because sub-archives (archive of already archived footage) do not contain any signatures generated by the original NVR that sourced the video data, sub-archives will *fail* the verification as their authenticity cannot be determined.

Auditing: Audit logging of the archive client on each NVR sourcing data for an archive is included.

Encrypted Archive Files: CathexisVision uses AES 128 encryption and RSA 256 signing for all archives. Only the CathexisVision Archive Player can review CathexisVision Archive files.

Privacy Policy – website

Cathexis is committed to protecting your privacy. By accessing the website, users accept and agree to the terms of this Privacy Policy. “Cathexis” refers to Cathexis Technologies (Pty Ltd), Cathexis Africa (Pty Ltd), and all of their direct and indirect subsidiaries.

When Visiting the Cathexis website: you may be required to provide personally identifiable information. Alternatively, you may elect to not provide Cathexis with personal data. The personal information you provide may include your name, company, job title, address, e-mail address, your business, profession, and product preferences. Cathexis’s web servers may automatically collect website usage information from you. Website usage information informs Cathexis about how visitors and subscribers use and navigate the websites. This includes the number and frequency of users to each page, their IP addresses, and the length of their stays.

Personal data: Cathexis will not collect any personal information about you through our website, or any other means, unless you have given your consent or provided it to us of your own volition. You have the option to give your consent when registering on our website. User data is captured on registration and users have access to their information.

Use of information collected: The personal information collected on the website will be used to operate the website and to provide the services, or carry out the transactions, you have requested. Cathexis may combine the information you have provided with other accessible information about you, including website usage information and information from other sources. Cathexis may use this information to process, validate, and verify requests for products and services. Your personal data may also be used for the purposes for which you specifically provided the information; to enhance your experience of the website; to improve and develop new products, features and services; to alert you to new products, services, and special offers; to provide marketing with aggregate information about the user base and usage patterns; and to allow Cathexis to personalise advertising for users based on their personal characteristics or preferences.

Information for our newsletters and sales force: Users have the option to agree to this upon registering on our website, and have the option to opt out.

Do we share your personal data with our partners? No.

Information required for legitimate purposes: Cathexis may disclose any information about you to law enforcement agencies, government officials, or other authorities, as Cathexis, in its sole discretion, believes necessary or appropriate in the circumstances.

Retention policy: There is no expiration to the retention of your personal data. Cathexis reserves the right to retain your data for the purposes outlined in this Privacy Policy as permitted by law.

Cookies: Cathexis automatically collects information and data through the use of cookies. A cookie is a small text file that is placed on your hard disk by a web page server, which enables a website to recognise repeat users, facilitate the user's ongoing access to, and use, of the website, and allows a website to track usage behaviour and compile aggregate data that will allow content improvements and targeted advertising. A cookie will not provide Cathexis with personal information. If you have not supplied Cathexis with any personal information, you can still browse the website anonymously. You have the ability to accept or decline cookies, and you can modify your browser settings to decline them. If you choose to decline cookies, you may not be able to fully experience the interactive features of the Cathexis website or other websites you visit.

How we ensure the security of your data: The personal data we collect about you is stored in limited access servers. Cathexis maintains safeguards to protect the security, integrity, and privacy of these servers and your data. In particular, SSL and Cloudflare protect you against information theft.

IP address: the IP address will be automatically collected and logged as part of the connection of your computer to Cathexis's web server and may be used to determine the total number of visits to each part of the website. If there is a security breach, the relevant IP Address will be identified by the Internet Service Provider and the user may be contacted.

Using our mobile application: Cathexis does not collect any personally identifiable information from clients who use our mobile application. We do send anonymous crash reports that include, among other data, the type of mobile device you are using and your operating system. These crash reports are only sent with your consent.

Video management system (VMS): The CathexisVision VMS does not collect any personally-identifiable data. In keeping with the Cathexis ethos, our VMS prioritises your privacy, safe-guarding the sensitive data and information of our clients.

Links to other websites: external links are not subject to this Privacy Policy. Cathexis recommends that you review the privacy policy of each website to determine how it impacts you.

Policy updates: Cathexis may amend this Privacy Policy from time to time, and will post any changes. Notwithstanding the right to amend the Privacy Policy, Cathexis will not use your personal information in a manner materially different from this Privacy Policy without your prior consent.

Comments and questions: If you have any questions regarding our privacy policy or data collection process, want to withdraw consent, or edit your details, please fill in the Contact Us form. Cathexis reserves the right to contact you at any time regarding problems or questions. Cathexis may also notify you of changes to the Privacy Policy, or to other policies or terms that affect you, but it is not obliged to do so.

This Privacy Policy is subject to the **terms and conditions** of use of the Cathexis website.