



**How we help organisations  
with GDPR compliance  
of their visual data**

2021

## GDPR AND VISUAL DATA

Anyone running a CCTV platform, from large international corporate entity to small local business or private householder, needs to be mindful of data protection and privacy legislation.

The new General Data Protection Regulation (GDPR), enshrined in law in the UK from the end of May 2018, provides the ideal opportunity for all users of CCTV to take a look at what they do and how they do it, to overhaul clunky, out of date systems, add a host of modern, cloud based features that will make better use of the visual data they collect, and ensure legal compliance all at the same time.

The GDPR was born out of an ambition to make legislation around data protection fit for the many ways in which personal data is collected and managed today, and into the future. Its principle goals are to protect the rights, privacy and freedoms of people in the EU, and to facilitate the free movement of data throughout the EU, thereby helping to reduce barriers to business. Importantly, any organisation that works with data which passes through an EU country will need to be compliant.

Six key principles enshrined within the GDPR are fundamental to meeting its requirements. As a

company providing visual data management services for customers, Cloudview is a 'Data Processor' (in running Cloudview's business operations we are also a Data Controller). As a Data Processor, we can remove the myriad of responsibilities related to Processing visual data under GDPR from our clients, so they can focus on being Data Controllers of visual data.

So, here are the six key principles of the GDPR with a brief description of how Cloudview can help regulate visual data for its clients.



# 1

## PRINCIPLE

### LAWFULNESS, FAIRNESS AND TRANSPARENCY

The data subject must be told what processing will occur, the processing must match its description and the processing must be lawful.

#### Issue:

While signage can inform people that they are being recorded, when it comes to regular CCTV, viewing and use of visual data before and after it has been recorded is difficult to regulate and almost impossible to accurately audit.



#### How Cloudview helps:

Cloudview securely consolidates data from multiple cameras across many sites and is designed to be accessed securely by multiple users.

Visual data is securely stored and can't be accessed by unauthorised users. A 'reason code' is provided to authorised individuals to ensure they only see appropriate data for their level of approval. For security staff this might be 24/7 access to all footage, but not everyone needs this level of access and the reason code would be different for different roles. Auditing protocols ensure that data access is 'fair' and 'transparent' in terms of the consent of the data subject (the person that's been recorded).

# 2

## PRINCIPLE

### PURPOSE LIMITATION

Personal data can only be collected for specified, explicit and legitimate purposes.

#### Issue:

Signage near a camera tells people why it is being used. But it is not easy to control a camera that is unsupervised against recording whatever it happens to 'see'.



#### How Cloudview helps:

Secure, authorised access to visual data, protected through 'reason codes' helps ensure data is only used for stated reasons. The ability to audit access at any time deters abuse, and instances of abuse are easily identified through an audit.



# 3

## PRINCIPLE

### DATA MINIMISATION

Personal data collected should be adequate, relevant and limited to what is necessary in relation to the purpose.

#### **Issue:**

Legacy CCTV systems often record continuously, capturing everything they 'see'.



#### **How Cloudview helps:**

Cloudview captures triggered recordings of smart objects like people and vehicles only. These smart triggers and ability to set specific zones of interest mean that unnecessary footage is not recorded. Personal privacy can also be protected by obscuring features and redacting/masking individuals or areas that are not required or permitted to be recorded in.





# 4

## PRINCIPLE

### ACCURACY

Data must be accurate and where necessary, kept up to date.

#### Issue:

To comply with the GDPR, systems must be checked regularly to ensure they are keeping the correct time. Where CCTV systems are in multiple locations weekly or monthly checks may be completely impractical.



#### How Cloudview helps:

Cloudview regularly checks the time and date numerous times through out the day, ensuring that all footage recorded by cameras connected, is accurately timestamped.



# 5

## PRINCIPLE

### STORAGE LIMITATION

The regulation requires personal data that is kept in a form which permits identification of data subjects to be kept for no longer than necessary.

#### Issue:

It is difficult to reliably manage retention times on CCTV DVRs, and usually impossible to specify different retention periods for different cameras.

#### How Cloudview helps:

Data retention times can be set per business requirements, and when a time limit is reached data is automatically deleted – or securely archived if that's lawful. The addition of further cameras does not impact overall storage capacity. So, scaling up and down is quick and easy. In addition, deleting privileges can be provided to certain users who have permission to delete to ensure a greater control of data, as well as audit trails and logs of any material deleted.



# 6

## PRINCIPLE

### INTEGRITY AND CONFIDENTIALITY

Organisations are required to process personal data in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, damage or destruction.

#### Issue:

All personal data has to be treated as confidential within the collecting organisation, but this is difficult with traditional CCTV systems that often have permission free accessibility and even an openness to breaches due to poor system security.



#### How Cloudview helps:

Password protection, 'reason codes' to control levels of access, unique data encryption from capture to storage and regular firmware testing against intrusion all combine to make Cloudview the most secure platform on the market.





The GDPR is predicated around the strongest protection of data to prevent its misuse and safeguard the privacy of individuals. Placing the burden of meeting these requirements on traditional CCTV systems which save visual data to digital video recorders with insecure firmware, poor access controls, often non-existent control of deletion and archiving, and insufficient audit trailing of access is unworkable. Cloudview is built from the ground up with data security and the protection of individual privacy at its core. It is a far better way to manage visual data in the context of the GDPR.

## **LOGAN BELL**

### **HEAD OF PRODUCT**

#### **CONTACT:**

**E: [lbell@cloudview.co](mailto:lbell@cloudview.co)**

**T: +44 7917 050 336**

