6S Global

CCTV obligations Under the General Data Protection Regulations and the Data Protection Act -2018

WP-DP-CCTV-01

INDEX

CCTV obligations Under the General Data Protection Regulations and the Data Protection Act 2018.

Abstract

Surveillance cameras are no longer a passive technology that only records and retains images but is now a proactive one that can be used to identify people of interest and keep detailed records of people's activities, such as with ANPR cameras. The use of surveillance cameras in this way has aroused public concern due to the technology no longer being used solely to keep people and their property safe, but increasingly being used to collect evidence to inform other decisions, such as the eligibility of a child to attend a school in a particular area.

In London the Metropolitan Police, Highways England and TfL control rooms share CCTV images using the Television Network Protocol (TVNP), which was developed by TfL over 20 years ago. This technology is analogue based and is now outdated and becoming obsolete as digital CCTV equipment becomes the standard – meaning that camera sharing opportunities will reduce.

The unwarranted use of CCTV and other forms of surveillance cameras has led to a strengthening of the regulatory landscape through the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA18) the Protection of Freedoms Act (POFA), the Human Rights Act 1998 (HRA) and the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act (POFA code).

Digital Video Network Protocol (DVNP), is now being introduced within Metropolitan Police, Highways England and TfL control rooms, this paper will look at the issues around compliance to privacy legislation as well as practical installations of a digital CCTV network.

Introduction

The GDPR is a set of EU-wide data protection rules that have been brought into UK law as the DPA18. All CCTV operators must be proactive in assessing, and continually improving their compliance efforts – tick box compliance is no longer sufficient. Users need to assess their CCTV systems alongside the rest of their IT and remember that the DPA 18 applies to everything from a single camera monitoring the entrance to their office or home to a larger system used in a business, housing or public spaces.

In the case of Woolley v Akbar– the default position is that any professional (individual or organisation) setting up a surveillance system will be aware of the potential impact of their activities on data subjects and be familiar with the application of relevant law and guidance." CCTV systems use technology which has a high potential to intrude on the right to respect for private and family life. Any surveillance camera technology must, therefore, be consistent with a legitimate aim and a pressing need. Such a legitimate aim and pressing need must be articulated clearly and documented, as the stated purpose for any deployment.

CCTV systems can also be jointly owned or jointly operated, therefore the governance and accountability arrangements should be agreed between the partners and clearly documented so that each of the partner organisations has clear responsibilities, with clarity over obligations and expectations and procedures for the resolution of any differences between the parties or changes of circumstance.

CCTV systems should be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value. Measures are in place to ensure that data shall be as accurate, complete, and up to date as is necessary [South Lanarkshire Council v. Scottish Information Commissioner [2013] UK SC55] for the purposes for which personal data are best used.

CCTV and the GDPR/DPA 18

One of the most important features of the GDPR and perhaps one of the most challenging for the CCTV Data Controller is compliance with Art.25, GDPR - the principle of Data Protection by Design and Default.

Any company, council, government agency, etc, proceeding with the idea of installing CCTV around their building could expect complaints from the public. The proposition is particularly high risk given the new era we have entered with the General Data Protection Regulation. The GDPR gives people greater rights in relation to their data, greater remedies when those rights are infringed and provides for vicious sanctions. It also contains a provision for litigation for data protection breaches.

As such CCTV installations would be highly intrusive, and the public interest justification just isn't there (although stronger in the case of detecting crime than spotting funny incidents).

A person who walks down a street must expect that he will be visible to any member of the public who happens also to be present. So too if they cross a pavement and get in to a car. They can also expect to be the subject of monitoring on CCTV in public areas wherever he may go, as it is a familiar feature in places that the public frequent. (Kinloch v. HM Advocate [2012] UKSC 62).

Any increase in the capability of CCTV surveillance technology has the potential to increase the likelihood of intrusion into an individual's privacy. The Human Rights Act 1998 (HRA) gives effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, whilst others are qualified, amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR.

CCTV Information engages Article 8 by being within the scope of a person's private or family life, home or correspondence. The 'touchstone' of when information concerns private life to engage Article 8 is whether the person concerned has a reasonable expectation of privacy in respect of the information. This will be made out where it is shown that 'the person publishing the information knows or ought to know that there is a reasonable expectation that the information in question will be kept private' (Campbell – Baroness Hale), i.e. it is an objective test which involves consideration of all the circumstances – a broad and open textured approach. GDPR is set to test may of the previous case laws.

Seeing the bigger picture and filling in the gaps

At first glance, Data by Design and Default (Art.25, of the GDPR is deceptively simple. Although it's relatively short in length compared with other parts of the EU Regulation, its impact is very far reaching in terms of compliance. It's notable that the GDPR isn't prescriptive in the way the CCTV CCTV Data Controller needs to demonstrate how it meets these new requirements. This isn't a tick-box exercise but brings to life a risk-based approach to data protection that's outcome focused. In this new compliance landscape, personal data protection must be front of mind rather than after-thought.

Principle of Least Privilege (POLP)

A useful first step in complying with the Data Protection by Design and Default is the application of the Principle of Least Privilege (POLP). In the context of employees and contractors working for the CCTV Data Controller, the POLP only grants workers with the lowest level of access[1] to personal data that's sufficient for them to do their jobs.

The POLP also applies to things other than people, including software programs and processes. For example, an employee may be permitted to view CCTV footage but not print it, download it or modify it.[2]

Granular permissions can be granted by the CCTV Data Controller where certain employees and contractors can have access to all CCTV data, whilst others have access to specific CCTV activities. This can be from within the CCTV Controller or at other points of the value chain such as CCTV Data Processor(s) and sub-Data Processors.

The POLP isn't referenced in the GDPR but adherence to it will assist the CCTV Data Controller to comply with the principles of data protection including purpose limitation,[3] data minimisation[4] and ensuring the security of personal data.[5] A CCTV Data Controller can ensure consistency across the entire value chain by automating privileges and permissions through technical measures.

Data Privacy Impact Assessment

Under Art.35, GDPR, the Data Protection Impact Assessment (DPIA) is a tool that can help the CCTV Data Controller and the Data Processor identify the most effective way to comply with data protection obligations and meet the expectations of Data Subjects under the GDPR.

The DPIA is required to be performed where processing of personal data and when using new technologies is likely to result in a high risk to the rights and freedoms of individuals. It will be required in cases of an evaluation of personal aspects based on automated data processing including profiling; processing on a large scale of special categories of personal data or systematic monitoring of a publicly accessible area.

[1] In other words, access to a minimum amount of personal data of the Data Subject
[2] These rights can be set by the CCTV Data Processor and the CCTV Data Processor so this helps to mitigate the risks involved in processing personal data.
[3] Art.5(1)(b), GDPR
[4] Art.5(1)(c), GDPR
[5] Art.5(1)(f), GDPR

Under the GDPR, the DPIA is a mandatory 'hygiene factor' for a CCTV Data Controller prior to the commencement of certain personal data processing activities as specified under Art. 35(3), GDPR.

The DPIA entails describing all personal data classes processed along with associated data protection risks, whether personal data processing is lawful; an assessment of the impact of data processing on the rights and freedoms of Data Subjects and managing the risks to processing personal data by using appropriate safeguards.

Importance of the DPIA

Companies and organisations can use the DPIA to systematically assess and identify the privacy and data protection impacts of any products and services they offer and provide. It enables the CCTV Data Controller to identify the impact and take the appropriate actions to prevent or mitigate the risk of those impacts on Data Subjects. From an internal perspective, consistently using DPIAs helps to raise awareness of compliance with the GDPR and also helps to identify problems with processing of personal data early on.

This could avoid costly mistakes being made and may trigger a fresh assessment of the actual personal data that needs to be processed in order to fulfil the purposes for processing in the first place and observance of the Principle of Data Minimisation (Art.5(1)(c), GDPR).

Staff working for the CCTV Data Controller will need to be provided with appropriate training and support to assist in conducting DPIAs, overseen by the Data Protection Officer (DPO).

Under Art.35(3), GDPR, the DPIA is a mandatory 'data cleanse' prior to the commencement of certain personal data processing activities and unlike a Privacy Impact Assessment (PIA) that's been standard practice for many years and tended to be carried out on a project-by-project basis, the DPIA applies across the whole organisation.

The DPIA entails describing all personal data types processed along with associated data protection risks:

- Whether personal data processing is lawful
- An assessment of the impact of data processing on the rights and freedoms of Data Subjects
- Managing the risks of processing personal data by using appropriate safeguards.

When is it appropriate to conduct a DPIA?

The DPIA should be carried out "prior to the processing" of personal data (Art.35(1) and 35(10), GDPR) and this is consistent with the principle of Data Protection by Design and by Default (Art. 25, GDPR).

In some cases, the DPIA will be an on-going process, for example where a processing operation is dynamic and subject to on-going change. Carrying out a DPIA is a continual process, not a one-off exercise.[6] Where the CCTV Data Controller identifies very high-risk processing that it can't mitigate with existing organisational and technical measures, then under Art.36(1), GDPR it's under a duty to consultant with the relevant Supervisory Authority (Figure 6.2).

According to the GDPR,[7] there are circumstances under which it may be reasonable and economical for the issue of the DPIA to be broader than a single project, e.g. where the CCTV Data Controller may intend to establish a common CCTV application or processing platform.

This may mean where similar technology is used to collect the same sort of personal data for the same purposes, e.g. the CCTV Data Controller could conduct a DPIA to cover all video surveillance across all locations with one DPIA.

[6] In accordance with guidance published by Art.29 Data Protection Working Party 17/EN WP 248, adopted on 4 April 2017, there are some basic principles when conducting a DPIA.
[7] Recital 92, GDPR

Under the GDPR, the appropriate time for an organisation to carry out the DPIA would be prior to anyof the following circumstances:

- When introducing new technology and/or new applications
- When processing special personal data
- When processing new data classes to which the level of risk is unknown
- When carrying out automated personal data processing and/or profiling where the result of such personal data processing creates legal effects on the Data Subjects or significantly affects the rights of the Data Subject
- When systematically monitoring of a public area on a large scale (e.g. CCTV cameras)
- When making significant changes to the existing data processing operations
- And highly recommended when using cloud-based services for processing personal data.

Art.35, GDPR sets out a broad requirement that the DPIA must be carried out when personal data processing is 'likely to result in a high risk for freedoms of individuals'. The DPIA must consider the entire lifecycle of personal data processing from the point of collection to the point of deletion. At all stages, the rights and freedoms of Data Subjects must be protected.

The CCTV Data Controller will need to periodically check that the "residual risk" remains acceptable and if it increases with no ability to mitigate this increase in risk, then it will need to consider prior consultation with the Supervisory Authority in accordance with Art.36, GDPR.

In accordance with best practice, the CCTV Data Controller, Joint CCTV Data Controller and CCTV Data Processor will need to review all personal data processing operations NO LATER THAN May 2021 to ensure that such personal data processing risk have been mitigated and reduced to a residual risk that doesn't cause harm or damage to the rights and freedoms of Data Subjects.

Who should carry out the DPIA?

The CCTV Data Controller and the Data Processor is responsible for ensuring the DPIA is carried out.[8] Carrying out the DPIA may be done by someone else, inside or outside the company and organisation but the CCTV Data Controller and the Data Processor remain ultimately accountable for that task under the GDPR. The CCTV company must seek the guidance and advice of a DPO[9] and this advice, and the decisions taken, should be documented within the DPIA.

Consulting the Supervisory Authority

Under Art.36(1), GDPR, the CCTV Data Controller must consult the relevant Supervisory Authority prior to the processing of personal data where the DPIA indicates that the processing would result in a high risk in the absence of measures taken by the CCTV Data Controller to mitigate that risk and reduce it to a residual risk that doesn't cause harm or damage to Data Subjects.

In accordance with guidance published by Article 29 Data Protection Working Party an unacceptable high residual risk includes where the Data Subjects may encounter significant or even irreversible consequences that they may not overcome, and/or when it seems obvious that the risk will occur.

In addition, the company and organisation must also comply with individual Member State laws where prior consultation is also required with the Supervisory Authority to obtain prior authorisation [10]

[8] Art.35(2), GDPR
[9] Ibid
[10] 17/EN WP 248, adopted on 4 April 2017
[11] Art.36(5), GDPR

in relation to processing for the performance of a task carried out in the public interest, including processing in relation to social protection and public health.[11]

Publishing the DPIA on the CCTV Data Controller's website

Although publishing the DPIA isn't a legal requirement under the GDPR, the CCTV Data Controller should seek to publish it or a version of it on its website, seeking guidance and advice from the DPO.

Conducting a Legitimate Interest Assessment (Recital 50)

In the absence of a Data Privacy Impact Assessment (DPIA), the CCTV Data Controller may want to conduct a LIA that's a gap analysis of what it's doing that complies with the GDPR, what it's doing that doesn't comply with the GDPR and what it needs to start doing in order to comply with the GDPR.

Generally, authorities and CCTV companies may rely on legitimate interests as an appropriate legal basis for processing personal data – it entails organisational accountability and enables the responsible uses of personal data, while protecting employees' data privacy rights. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller."

Note: when CCTV footage is disclosed to the police(or other competent authority as defined by Schedule 7 of the DPA 2018), it will be processed for under law enforcement process as defined by Part 3 of the DPA 2018, and not processed under the GDPR. How the police (or other competent authority) process it is no longer your concern. In both cases, you must weigh your lawful basis against the data subjects' privacy rights.

CCTV and Implementing Data Protection by Design and by Default

The following considerations apply when implementing the data protection principles of the GDPR.

Lawfulness, fairness and transparency (Art.5(1)(a), GDPR)

The interaction between the CCTV Data Controller and the Data Subject needs to be reviewed to ensure Data Subjects grasp what's being done with their personal data. These communications include the website, a pre-recorded telephone message and a customer service call.

Any activity of the CCTV Data Controller that attempts to get consent on a sneaky basis, that buries the Data Privacy Notice in terms and conditions and uses legal gobbledygook rather than clear language will fail to satisfy the test of lawfulness, transparency and fairness and will be an infringement of Art.5(1), GDPR.

If front-line staff can't direct a person to the right place or if the Data Subject needs to scrutinise the fine print of a CCTV Data Controller's terms and conditions to find out how to exercise Data Subject rights, a CCTV Data Controller will not only fail to meet transparency and fairness requirements,[12] it may also open itself to greater scrutiny by the Supervisory Authority in the face of complaints by frustrated Data Subjects.

Purpose limitation (Art.5(1)(b), GDPR)

A CCTV Data Controller must ensure it knows what's actually happening with personal data it processes and whether this goes beyond the purposes stated in the Data Privacy Notice and the Record of Processing Activities.[13]

Rogue or well-meaning employees that re-purpose personal data or third parties that surreptitiously collect personal data, for example by 'scraping' data from a website or by profiling, will put a CCTV Data Controller in breach of Art.5(1)(b), GDPR.

Data minimization (Art.5(1)(c), GDPR)

A CCTV Data Controller may only process personal data that's necessary for a specific processing activity. For example, if the occupation of a gym member is irrelevant for registration purposes to use the gym, this shouldn't be recorded, and it would be better to remove this field from the registration process to eliminate unnecessary collection of personal data.

To do this, a CCTV Data Controller should confirm which processes exist in practice:

- are there unknown, informal practices that haven't been captured in the Record of Processing Activities ?[14]
- have the business owner or database administrator walked through it to explain what's happening at a technical and organizational level?
- have automated scanning tools been used?
- has the CCTV Data Controller spoken with front-line staff who access and use the CCTV databases to see what's happening in the ordinary course of business? Do they understand the broad definition of personal data under the GDPR in order to answer questions accurately?

[12] Art.5(1), GDPR
[13] Art.30(1)(b), GDPR
[14] Art.30, GDPR

Data Minimisation by Architecture

The CCTV Data Controller should apply the POLP when designing the information system so individuals who process personal data only receive what they need.

Accuracy (Art.5(1)(d), GDPR)

A CCTV Data Controller must take every reasonable step to ensure inaccurate data is rectified or erased "without delay".[15] This is technically challenging where personal data hasn't been directly obtained from the Data Subject, for example through a merger or acquisition or from a data broker.

Storage Limitation (Art.5(1)(e), GDPR)

The CCTV Data Controller may only store personal data for as long as it can be justified by the processing activity, subject to another legal or regulatory obligation(s).[16] In that case, it's important to confirm which data elements must be retained, as it may not be necessary to retain a complete profile.

The GDPR codifies a data loss management (DLM) best practice and the CCTV Data Controller should have processes in place to either automatically destroy or aggregate personal data once the storage time limit has expired or to trigger a review process.

For example, CCTV footage recorded for security purposes should only be retained long enough to resolve a security incident. If no security incident requires a review of the footage, it should be automatically over-written by programming an automatic override of CCTV recordings every X number of days, where X reflects the amount of time usually necessary to discover there's an incident requiring longer retention of the specific footage required. The remainder would then be overwritten in the regular cycle.

Integrity and Confidentiality (Art.5(1)(f), GDPR)

Technology helps protect the integrity and confidentiality of personal data, but people are the 'weakest link' in the value chain. The CCTV Data Controller should have a process for regularly testing, assessing and evaluating effectiveness of these measures,[17] including testing policy compliance, gathering metrics and closing gaps.

[15]Art. 5(1)(d) and Art.16, GDPR
[16]Art.25(2), GDPR

Accountability (Art.5(2), GDPR)

A CCTV Data Controller must demonstrate compliance with the data protection principles and GDPR processing requirements.[18] The Records of Processing Activities, the DPIA/LIA, Certification and Codes of Conduct can collectively be used to demonstrate compliance with the GDPR. They must also ensure all suppliers are correctly trained together with the correct level of administration rights.

At the same time, it's important to integrate necessary safeguards to meet GDPR requirements, such as those regarding security[19] and international data transfers.[20] Such measures include encryption, pseudonymisation as well as other technical and organizational safeguards in light of international data transfers.

Protecting the Data Subject's Right of Access

This is an important right[21] under the GDPR and the CCTV Data Controller must design processes and technologies to ensure:

- the Data Subject can readily access all personal data held on them or derived or inferred from that data
- the Data Subject can receive a copy of that personal data
- the Data Subject can obtain confirmation of and information about the processing activities.

A CCTV Data Controller must be prepared to respond to an individual Subject Access Request (SAR) in a timely manner and from a technical perspective customer database will need to be searchable by Data Subject.

Protecting the Data Subject's Right to Rectification

A CCTV Data Controller must have the technology and processes to ensure a Data Subject can have inaccurate personal data rectified or completed without undue delay. The way to make such a request needs to be spelt out in the Data Privacy Notice.[22]

[17] Art.32(3), GDPR
[18] Art.5(2) and Art.24(1), GDPR
[19] Art.32-Art.34, GDPR
[20] Art.46, GDPR
[21] Art.15, GDPR
[22] Art. 13(2)(b) and Art.14(2)(c), GDPR

Protecting the Data Subject's Right to Erasure

The erasure of personal data without undue delay and the notification to other CCTV Data Controllers that process this personal data only applies where certain conditions have been met.[23] There needs to be technical measures available to be able to do this, although it should be remembered that deleted personal data can be re-constructed even if it doesn't appear in a file directory.

It will be important to verify with the IT Department and other Infosec professionals that the personal data has been erased and isn't recoverable by having a certificate to that affect.

The Right to Erasure exercised by the Data Subject will terminate the relationship with the CCTV Data Controller often when there's been a complete failure to fulfil its obligations or deliver the rights and freedoms of the Data Subject.

In each of these infringements of the GDPR, there's an increased risk of harm or damage to the Data Subject. In addition, the Data Subject has the right to withdraw consent or object to a processing activity that's based on a CCTV Data Controller's legitimate interest.[24]

Restriction of Processing

This is a new right[25] of the Data Subject compared with the previous Data Protection Directive 95/46/EC. The CCTV Data Controller must ensure it's possible to isolate a Data Subject's personal data temporarily or permanently to prevent it from being processed alongside other personal data across the value chain.

Data Portability

The Right to Data Portability[26] enables a Data Subject to obtain and reuse her/his personal data across a range of services and other CCTV Data Controllers. For example, it can assist the Data Subject to shop around for the lowest electricity tariff or move from one insurance provider to another. The personal data must be in a structured, commonly-used and machine-readable format so it can be easily used by another CCTV Data Controller to provide those services.

Right to Object to Processing

The first time a CCTV Data Controller communicates with a Data Subject it must inform the individual about the right to object to processing of their personal data. [27]

Where a DPO is appointed, s(he) should ensure this right to object to personal data processing is built into workflows and communication strategies. Standard language or templates used by the CCTV Data Controller may well assist in this regard. A CCTV Data Controller should also establish a decision-making process for handling objections to the processing of personal data.

The CCTV Data Controller should as a matter of urgency confirm whether there are technical and organizational measures in place to comply with the right to object to personal data processing. This will require a high degree of co-ordination across the value chain and data tags as well as the identification of different personal data types processed within the organization will be helpful.

[23] Art.17, GDPR
[24] Art.6(1)(f), GDPR
[25] Art.18, GDPR
[26] Art.20, GDPR

The right not to be subject to a decision based solely on automated processing including profiling

The right not to be subject to a decision based solely on automated processing including profiling[28] needs to be read in light of Right to Object to Processing[29] and the Right to Withdraw Consent.[30] A CCTV Data Controller seeking to process personal data for profiling and automated decision-making purposes must ensure it can cease profiling a Data Subject that exercises this right.[31] Under Art.12(3), GDPR the CCTV Data Controller must respond without undue delay and in any event within one month of receipt of the request.

Access Rights

Best practice for information society service providers is to allow a Data Subject to download their personal data that includes not only what they see when logged-in but also information on the ads they've clicked on and IP addresses they've used.

Social media sites and online services may lend themselves more readily to this type of service but that doesn't prevent CCTV organisations adopting a similar process in their Data Protection by Design efforts. Business who consider the need to develop a surveillance camera system should give due consideration to the establishment of proper governance arrangements. There must be clear responsibility and accountability for such a system. As the CCTV system covers public space a company would be considered as an operator and must be aware of the statutory licensing requirements of the Private Security Industry Act 2001.

[27] Art.21, GDPR
[28] Art.22, GDPR
[29] Art.21, GDPR
[30] Art.7(3), GDPR
[31] Art. 12(2) and Art.15-22, GDPR

Hybrid CCTV locations

These are both public and private (for instance, a care home is both a residence and a workplace). Given that the Court has emphasised the household exception arises only when the processing can be tied 'purely' to private and family life hybrid locations are unlikely to be considered within the household exception. By creating links between business, CCTV systems and members of the public who can sign up to be 'CCTV Spies' and uploading to the company website will have a consequence of a breach not just for the ECHR, but for the Data Protection Act 2018, as well as other guidance and standards.

The hybrid CCTV systems should only be used in a public place for the specific purpose or purposes it was established to address. It should not be used for other purposes that would not have justified its establishment in the first place. Any proposed extension to the purposes for which a system was established and images and information is collected should be subject to consultation before any decision is taken. By creating links to various businesses will bring in to question the image quality of the CCTV being provided, system security and administrative control.

The Balancing exercise

Where it has been established that there is a reasonable expectation of privacy in respect of information, such that a claimant's Article 8 rights are engaged, the court must undertake the 'ultimate balancing test', weighing the claimants Article 8 rights, the rights of the defendant, and the rights of other individuals concerned, to ascertain which should yield.

Technical and organisational measures

The GDPR requires CCTV Data Controllers and processors to implement "appropriate technical and organisational measures" to protect personal data. This entails an approach based on regular assessments to ensure that all risks are appropriately addressed.

1. *Access to CCTV systems must be limited to authorised personnel*

   a. This is especially important where systems are connected to the Internet or footage is stored in the Cloud, and there is a greater risk of unauthorised access.
   b. Administrative controls must be implemented this must be identified in the POLP, fully documented and audited.

2. *Pink box exploratory scan*

   Prior to completing any system penetration tests to a Digital Video Network Protocol (DVNP), it would be considered prudent for network owners to implement a 'pink box exploratory scan'. The process is used to discover and visualize physical and virtual network connectivity via a group of interrelated tasks that facilitate the creation of a network map, including flow charts, network diagrams, topology detection and device inventories. It is geared toward the creation of visual aids and materials that can be used for a broad array of purposes, especially network maintenance. The pink box exploratory scan is evolving therefore, network mapping continues to increase in importance with the rise of complex, dynamic networks, globalization and cloud computing.

   The Pink Box exploratory scan allows the CCTV owners to visualize and break down complex networks into smaller portions, allowing analyses as well as views of the network, checking for connection errors as well as identifying details which facilitate any issue's thus providing a root cause analysis. By using a mapping system's active monitoring module, the exploratory scan can identify network changes in real time. This is useful for network providers and Internet service providers (ISP), as well as anyone that operates a large, complex CCTV networks.

3. CCTV Sharing

a. Recently it has been widely reported about websites which have been openly streaming video from surveillance systems across the globe, the largest being a website called Insecam which featured over 73,000 live streams from networked CCTV systems whose owners had failed to change their default DVR & NVR passwords. There have been reports criticizing this website message claiming to only exist to make the public aware of this security flaw. But whether it is right or wrong for these video feeds to be online the message is the same.

b. An issue which must be considered is where will the shared data be stored? If the data is stored within a company's own data room then suitable safeguards must be in place e.g. technical controls, Cyber essentials certification as well as ISO 27001. Alternative if the CCTV Data Controller uses cloud based or servers from a third party, the Data Controller / Processor must ensure adequate safeguards are in place. Such safeguards include the provision of an LIA which will identify any further controls which should be in place.
By using a third-party cloud provider the Data Controller / Processor may well be transferring data out of the European Union to a third country with does not fall under the adequacy requirements of both the GDPR or the DPA 18. Companies must consult with a DPO to ascertain which measures must be taken to ensure compliance to legal requirements.

4. Penetration testing

Like any other Information Technology Network, CCTV networks are often vulnerable to unwanted attackers who can find out about, access, and interrupt service. When attempting to make a CCTV network secure against unauthorized access, it is common to hire a company to perform penetration tests. These persons, execute a variety of strategies to gain control of systems within the CCTV network, to access CCTV images and data, whilst determining which parts of the CCTV network are vulnerable to attack. They generally begin Pink box exploratory scan to access to the network, so they must discover vulnerabilities in much the same way as the unwanted computer hacker.

A penetration test, or "pen test," is an attempt to evaluate the security of IT infrastructures using a controlled environment to safely attack, identify, and exploit vulnerabilities. These vulnerabilities may exist in operating systems, services, networks, and application. They may also exist due to improper configurations or risky end-user behavior.

Penetration testing assessments are also useful in validating the efficacy of defensive mechanisms and determining how well end-users adhere to CCTV security policies. Network professionals also take note of all dialogs associated with user alerts and error messages. This information can be communicated via a software application to an external user. If the external user has malicious intent, it is important for network professionals to identify how and what information is being revealed to external users. During the planning phase, network professionals also identify various disaster scenarios to get a better idea of what a network attack would entail. The information gathered originates from specific network threat models and any previously known exploits.

The information gathered during the planning phase helps to guide network professionals through the actual penetration testing process. The testing process is all about variation and locates different aspects in software applications and the environment that are varied. The test then involves varying these aspects to determine the response. This helps to ensure software applications can perform under both reasonable and unreasonable circumstances. When it comes to overall security, the primary locations where variations can expose security issues are within user input, the network environment that consists of system resources, files and applications, and internal logic and data in the system. When information is varied during a pen test, this identifies and confirms security issues, so the appropriate measures can be taken to fix the problem.

Penetration testing is never a one-time event, instead it must be a continual process to accurately measure how well your security model is performing. It also helps your business to gain awareness of any gaps in the security model that may exist at any given point in time.

CCTV Installers must complete a system penetration test to comply with the requirements of both the GDPR and the DPA18, they must document the results of the test and provide advice to the CCTV Data Controller / Processor on any Data Privacy issues identified.

5. *Network Configuration*

a. Surveillance systems should also incorporate privacy-by-design features, including the ability to be switched on or off, and the option to switch off image or sound recordings independently where it would be excessive to capture both. CCTV equipment must also be of a sufficient quality and standard to achieve its stated purpose.

b. When installing additional hard / software in to an existing CCTV system the CCTV Data Controller or Processor must ensure that all administrative Controls are reset from the initial manufactures settings, they must all ensure all cloud activation ports are either locked or removed to prevent unauthorised access e.g. from the manufacturer.

c. Anti-virus for the network must be up to date, whilst being regular checked and monitored, as failure to complete this will result in authorised access to your network.

6. *Test access and access to the NVR*

a. All networks must be check for any possible assess issues on a regular scheduled basis, such testing access must also include the NVR, ideally such testing should be completed via a third part to ensure impartiality to any issues identified within the CCTV network.

7. *Audit*

Any CCTV system witch access Data Subjects must be audit for compliance to the GDPR. The DPA 18, PECR and relevant codes of practice as well as guidance. If a CCTV Data Controller/Processor, sub-processor or installer fails to complete documented audits of their respective CCTV system(s) then they run the risk for the full wright of any enforcement authority. I any company is in doubt they should discuss their issue with a DPO, who will provide advice on Data Privacy Issues. The international standard for information security management, ISO 27001, is an excellent starting point for implementing the technical and organisational measures necessary under the GDPR.

8. *Staff training in Data Protection*

Table 1.1 identifies staff who must be trained in Data Privacy prior to handling, installing equipment or administrating any data relating to CCTV and data subjects.

TABLE 1.1: Training of employees under the GDPR

Who	Type	Frequency	Description
All staff handling personal data / installation engineers	General GDPR	Annual	Basic course on the GDPR that includes the personal data breach (PDB) reporting process. Mandatory attendance required.
All staff handling personal data / installation engineers	General GDPR	Bi-annual	A bi-annual 'refresher' for the basic course on the GDPR. Mandatory attendance required.
Human Resources	Specialist HR	Annual	Covers the implications of the GDPR for Human Resources professionals. Mandatory attendance required.
Customer facing (CF) staff and front desk reception staff	Specialist HR	Every quarter	Covers the implications of the GDPR when collecting personal data, and responding to customer/client requests. Mandatory attendance required.
Finance	Specialist Finance	Annual	Covers the implications of GDPR as it applies to third party suppliers including Data Processors such as cloud service providers. Mandatory attendance required.
IT	Specialist IT	Bi-annual	Specialist GDPR and data protection training for IT helpdesk/support staff; database administrators (DBA), IT architects and staff who specify storage media, extract and transfer personal data; cyber-security specialists; and IT testing staff. Mandatory attendance required.
IT Architects and Developers	Specialist Finance	Annual	GDPR technical training on encryption and encrypted links, pseudonymisation, tokenisation, anonymisation, data minimisation, and data protection by design.

Marketing	Specialist Marketing	Quarterly	How the GDPR impacts direct marketing and personal data collection as well as other laws and regulations such as the e-Privacy Regulation. Mandatory attendance required.
DPO, Compliance/ Legal Staff and IT Cybersecurity Officer	Specialist GDPR Audit Training	Bi-annual	Data Protection Impact Assessment (DPIA) training, compilation of records of processing training and forensic PDB training. Mandatory attendance required.
Purchasing or Contracts	Specialist regulatory training	Bi-annual	Training to comply with the requirements of the GDPR as it applies to all appropriate supplier contracts and the assurance of them.
All staff	Data protection awareness campaign	Annual	Internal communication within the organisation that includes noticeboard communications, screens savers, and in-house competitions with prizes to promote awareness.

Audit

This sits outside the Risk Management and Data Governance Framework but supports it by testing the overall effectiveness and 'fit-for-purpose' of the processes and controls as described by the data governance framework.

The audit must be independent of the other functions to avoid a conflict of interest and to be effective.

The Data Controller and Data Processor must audit those parts of their value chain for which they are directly responsible to assure the effectiveness and 'fit-for-purpose' of the technical and organisational measures deployed by those parties (Art 28, GDPR).

CCTV Establish a Security Baseline

Your security policies are your foundation. Without established policies and standards, there's no guideline to determine the level of risk. But technology changes much more rapidly than business policies and must be reviewed more often. Software vulnerabilities are discovered daily. A yearly security assessment by an objective third party is necessary to ensure that security guidelines are followed.

Security audits aren't a one-off event. Don't wait until a successful attack forces your company to hire an auditor. Annual audits establish a security baseline against which you can measure progress and evaluate the auditor's professional advice. An established security posture will also help measure the effectiveness of the audit team.

Conclusion

Both the GDPR and the DPA18 have ignited the passion for tighter technical controls along with relevant safeguards. The obvious catalyst behind this improvement is the financial fines, reputation damage and litigation which will occur from a data breach. CCTV companies have to understand their obligations behind the legislation landscape and commence auditing their networks and suppliers to ensure all safeguards are achieved.