

Legal Compliance of CCTV Systems for Data Protection

It is becoming increasingly common for members of the public to completely discredit public safety and law enforcement CCTV systems, because authorities have not complied with their own data protection legislation. Failure to comply with even the most relaxed laws of compliance, has proven to cause irreparable harm to those who breach such guidelines, which undermines their crime fighting capabilities and also exposes them to significant financial penalties.

Viseum Product Solutions uniquely minimise such risks of negative exposure, by optimally controlling what live and recorded video that operator staff look at, during live emergencies and investigations. The cameras' built-in software means the recordings of people's activity can be based on behaviour and location rather than how people look. If required, the camera protocols can only allow the viewing of live images when a crime is actually underway, and recordings relevant only to a particular incident.

This document describes some aspects to be reviewed regarding CCTV compliance with Data Protection laws. This is not a full and exhaustive list. Audits should be carried out by independent experts in CCTV data protection compliance. Should any of the answers to these questions below result in a "no" this indicates a current issue with very basic requirements for compliance with Data Protection legislation.

Transforming Pan, Tilt & Zoom (PTZ) cameras from being reactive infrastructure-dependent CCTV installations, to proactive independent security assets.



The only PTZ Camera installations in the world to automatically watch everything in all directions at the same time.



The only PTZ Camera installations in the world to make remote CCTV monitoring a highly efficient option, rather than just a necessary cost.





The following are aspects of a CCTV system that are typically audited to comply with Data Protection Guidelines and in accordance with the UK Information Commissioner's CCTV Code of Practice

Purposes:

- Has the system been assessed in the previous 12 months?
- Is the system registered with the governing bodies for the purposes that the system is being used for?
- Are those specific purposes reflected on the statutory signage?
- Are the reasons for the CCTV fully documented?

Siting of Cameras:

- Do the cameras only monitor the identified locations for the specified purpose, or do some of the cameras also monitor outside the perimeter into unspecified areas?
- Are people monitored without specified purposes?
- Are people monitored without their knowledge?
- Is there a regular review (at least annually) of camera positions and requirement of cameras?

Signage:

- Are signs clearly visible and readable for the public?
- Are the locations of the signs correctly sited and regularly reviewed?
- Are signs correctly worded: purposes, Data Controller, contact details?
- Is there the correct number of signs and correct locations in accordance with the law?





Images:

- Are all parts of the system performing correctly with no issues – fit for purpose?
- Are Date / time stamps checked regularly and fully documented?
- Is recording set up to ensure no inadvertent corruption – recording and storage device fully protected and secure within a secure area?

Access to Images:

- Are all monitors that display images in correct location(s) in order that only persons trained and authorized are exposed to images?
- Is access to images restricted to correct staff?
- Are all operators with access to images aware of procedures about the use of images?
- Is all access to the recording medium formally documented?
- Is disclosure of images to a third party restricted and fully documented?
- Is the correct information requested from a member of the public for Subject Access Request (requests for images recorded of themselves)?

Security of Data:

- Is the recording equipment in a restricted area and secure with suitable lock and key within that area?
- Are the recorded images retained in a further restricted part of this area e.g. a safe?

Training:

- Are all persons involved with the system aware of the registered purposes of the system?
- Are all persons involved with the system trained in privacy issues of using cameras?
- Are all persons involved with the system trained in Data Protection for CCTV?
- Is all staff aware that it could be a criminal offence to misuse images?



Procedures:

- Are there regular reviews of documented procedures?
- Are there clearly documented procedures including the on-site CCTV Code of Practice?
- Are there procedures in place for Subject Access Requests?
- Are there procedures in place for reviewing evidential images? and are these procedures retained on site for onsite viewing?

Documentation:

- Does Control Room access include reference to complying with the Data Protection?
- Is Recorded Material Handover Documentation regularly reviewed?
- Are there Subject Access Request forms available?
- Third party viewing of images – is documentation available for data processors?
- Is there Public Awareness information on the CCTV system?
- Is there documentation for Date & Time checks?
- Is there documentation on the regular checks of quality / correct recording?



> [Viseum Technology and Support Strengths](#) < This is a brochure presentation of our technical support and capabilities. It is very successful for Viseum sales training and provides our customers with confidence in our project support and delivery.



Legal Statement

We have invested heavily in the protection and policing of our intellectual property rights (IPR). Central to our business is the commercial protection we provide our partners in sharing these secured markets. We commit to the policing of this IPR in the following way: As with any infringement, its trade reseller is the primary target for legal action, which is, in turn, followed up by making the potential user aware of the infringing product's recall due to its illegal use. This is then followed up with full and complete legal action with the suppliers of such goods. This policy of proactive policing our markets in this way since 2002 has proven so successful that we have only ever identified one infringing party. A PLC entity was found to be trading with infringing goods and they can now no longer sell such goods into our international territories, nor can they secure investment due to this breach.

Viseum technology and software is protected by a number of intellectual property rights. Purchase of a Viseum-driven product from an authorized Viseum[®] supplier guarantees that it contains authentic Viseum[®] software, and carries with it a licence giving the purchaser permission to use the Viseum technology. Attempted use of Viseum[®] software without a valid license is in breach of international law.

Patents Granted European Patent > [EP 1 579 399](#) <, United States of America > [US 7,952,608 B2](#) <.

Registered Trade Marks Viseum[®] SafetyWatch[®]

Copyright Except where noted otherwise, all material in this document is Copyright © 2018 Viseum. No part of the materials in this document including but not limited to the text, graphics, designs and devices, may be reproduced or transmitted to third parties in any form or by any means without written permission from Viseum[®].

This document is for information only and does not constitute an agreement between Viseum and any 3rd party.



For further information on how to set up Sales Agent, Regional Reseller and Distribution agreements to become a Viseum Certified Corporate Partner please contact your Viseum representative or write to us via the Viseum website.