In The Picture: Is Your Multimedia Evidence Breaching Data Protection?

Photo, video and audio evidence is as easily shared as it is captured. At work, the camera on a smartphone can be a handy shortcut, replacing notes, scans and even whole reports.

Take the insurance industry: In recent years, many insurance companies have been inundated with household claims from flood and storm damage. Collating the lengthy and detailed data needed to process these claims can be a complex and extremely time consuming task.

New technology is rightly taking over here, to prevent the nightmare of missed details and repeat visits - and make the whole process more efficient.

But while there is no doubt that technology has speeded up many tasks, one serious implication is very often overlooked, or indeed never even brought to mind. That implication is data protection.

Data breach – within easy reach

Consider the following scenarios – again taking insurance as an example.

While capturing a video interview of a couple detailing how flood damage has impacted on their lives, a loss adjuster fails to realise that clearly showing on the video are photographs of two young children.

While using the zoom and focus facility on his phone to capture all the detail of the damaged room, he inadvertently films a copy of a bank statement lying on a table showing all the recipient’s account details.

And finally, he fails to realise that the whole video showcases a wealth of valuable silverware, china and antiques, which would be very useful indeed were it to fall in the hands of, say, a burglar.

These are all data protection breaches in the making, a fact that needs to be considered by anyone using audio visual technology.

Data protection regulation just got scarier

If the issue of managing data protection in a new medium is not enough, there is an even bigger potential nightmare in store, in the form of the General Data Protection Regulation (GDPR) that comes into force in May 2018.

The GDPR is one of the most controversial and anticipated pieces of legislation conceived in the EU in recent years – and a game changer for businesses:

- It represents a fundamental shift in the risks associated with data protection - and, more importantly, with a data breach.
- It places new challenges on an organisation’s security operations and its technology estate.
- It forces organisations to change the way they think about data processing, including subcontracting to third parties such as cloud service providers.

While the scope of the GDPR is wide-ranging, it’s the consequences of non-compliance that organisations should be most concerned about:

The maximum penalty for non-compliance is 4% of annual revenue or £20 million, whichever is the higher.
This means that data protection will have a similar status, in terms of the level of fines, to anti-corruption and bribery legislation.

**How prepare for GDPR?**

Sensitive data has never been easier to obtain or disseminate electronically, while the risks have never been greater. A responsible organisation will need to recognise the risks and prevent, or mitigate, any potential problems.

Data can be stored on a wide variety and number of different devices in a modern organisation from servers and PCs to tablets, smartphones, USB sticks, and portable hard drives.

A well-designed IT lifecycle will look at all the potential problem areas and ensure policy and protection is in place throughout, from installation through to safe destruction.

While most organisations already have robust processes in place to safeguard written data, images, photographs and audio require special consideration. This is particularly true in light of the ease with which multi-media data is captured today.

**Staying in control**

The best way of reducing the data protection risk of audio-visual media is to bring the capturing of these into the fold of the enterprise IT system. In short: provide employees with the means to use video or audio safely, without compromising on efficiency or ease of use.

We developed eviid to do just that. Rather than banning the use of personal smartphones or asking employees to carry a separate camera, eviid creates a secure, self-contained system that can be accessed from a standard smartphone device.

This means organizations can fully exploit the potential of smartphone technology and audio-visual documentation, while staying in full control of the data.

For example, video/audio footage captured through the eviid app cannot be accessed through the device's photo gallery or other apps. As soon as the phone has sufficient signal to transmit data, the footage is automatically removed from the device and uploaded to the central system.

Access to the footage is tracked, sharing is controlled tightly (it is possible, for example, to control the number or duration of views of a clip after sharing).

These are just a few examples of features that ensure the possibility of data breaches is designed out as much as possible.

The conclusion: Data protection doesn’t have to stand in the way of using new technology, and convenience doesn’t have to come with a £20m price tag.

For more information about eviid, please visit [www.eviid.com](http://www.eviid.com).

ENDS