Observation Report:

CCTV MONITORING & RECORDING

of

OFFSHORE DIVING OPERATIONS

By
Chris Hodge
[Updated June 2024]

TABLE OF CONTENTS

Report History

Revision 1 2009	Original report capturing the 'new' Data Protection Act
Revision 2 2010	Peer review and change to layout and grammar corrections
11th January 2010	Discussed with Chris Shearman of the HSE
Revision 3 2011	Further changes to legislation
11th February 2012	Tabled at IMCA Meeting by Chris Sherman of the HSE. IMCA Members agreed this could be an issue and would take the matter into consideration.
12th February 2012	Report forwarded to IMCA and discussed with IMCA
Revision 4 2013	Review. Updated legislation, grammar and formatting
Revision 5 2015	Annual Review
Revision 6 2024	Post BREXIT changes Reformatted with different layout and font. 6.3 Added communication schematic from IMCA D46 showing use of CCTV 6.4 Added IMO & NORSOK requirement for video recording 6.4 Sent to UK HSE for consideration (Again)
Revision 6 2025	6.5 Corrections to grammar using Grammarly and changed header layout
Revision 6 2026	6.6 Annual review. Minor changes to grammar and formatting

Abbreviations and Initialisms

ACOP	Approved Code of Practice
BS	British Standard
CCTV	Closed Circuit Television
CoP	Code of Practice
DSAR	Data Subject Access Request
DNV	Det Norske Veritas
DPA	Data Protection Act
GDPR	General Data Protection Regulations
HDD	Hard Disk Drive
HRA	Human Rights Act
IMCA	International Marine Contractors Association
IMO	International Maritime Organisation
ICO	Information Commissioners Office
MUO	Manned Underwater Operation
NoK	Next of Kin
NORSOK	Norsk Sokkels Konkurranseposisjon (Norwegian shelf competitive position)
OCM	Offshore Construction Manager
ROV	Remote Operated Vehicle
UKCS	UK Continental Shelf
UK	United Kingdom
VDR	Voyage Data Recorder

1.0 INTRODUCTION

1.1 Summary

Closed-circuit television surveillance has become a common feature of daily life on and offshore. Onshore surveillance is primarily used for monitoring, detection, recognition and identification. At offshore worksites, it is usually used for security and safety.

During offshore diving operations, CCTV monitors personnel in the chambers, the bell, and the water, using helmet-mounted and ROV cameras.

Any CCTV footage captured during diving is stored in various formats, usually on a digital hard drive and a backup 'black box' HDD.

All recordings contain images of identifiable individuals and should be treated as 'personal data' under the Data Protection Act (DPA). Personal data is at the heart of the DPA; if a living individual can be identified from CCTV images, those images constitute personal data and must be treated as such.

The Data Protection Act is the UK law that governs what may or may not be done with personal data. It was set up to protect individual rights rather than to assist organisations in running their business. It covers data held in both manual and electronic records.

Using CCTV to monitor employees' actions may have implications under the Data Protection Act, the Human Rights Act, and the Freedom of Information Act. Employers must ensure that personal data or information is 'processed' fairly and lawfully.

Diving contractors take great care with personal data in the onshore office; however, the same care is needed for CCTV at diving and offshore worksites. CCTV recordings from diving (and deck) operations must be subject to greater control. The employer must inform the employee what is being recorded, why, and who will have access to it.

Although this report primarily covers company-operated CCTV, the same safeguards and data control should apply to personal handheld recording devices such as camera phones and tablets.

1.2 Limitation

This report, originally issued in 2009, primarily addresses the use of CCTV in offshore diving projects. Since then, UK regulations concerning CCTV monitoring, recording, storage, and the handling of personal data have undergone significant changes. While this report aims to reflect those updates, understanding data protection law remains a specialised field beyond the author's expertise.

This report is limited to protecting the data of an 'identified or identifiable natural person' captured on an image or moving image.

This report doesn't consider Flag State or maritime laws on seagoing vessels.

1.3 Objective

This report provides an overview of CCTV use during offshore diving projects. It provides guidance to ensure the company adopts the correct standard operating procedures for closed-circuit television cameras, monitors, and recordings.

The report provides an overview of the legal responsibilities regarding recordings and images. It clarifies who controls them, to whom they may be disclosed, and who is permitted access. Finally, it helps managers collect, maintain, and store personal recorded data on board a ship (or at other dive locations) in accordance with legislation.

1.4 Aims

The aims of this report are:

- Highlight the methods used offshore to capture images/recordings, and provide guidance on good practice for those responsible for operating CCTV systems that record images/recordings of individuals.
- Ensure diving contractors/vessel owners comply with the law and best practices.
- Protect the diving contractor/client from potential court cases and fines
- Protect divers from appearing on social media without their consent.
- Protect NoK from seeing a diving incident on social media

1.5 Scope

The report is limited to diving support vessels operating under the scope of the Health and Safety at Work Act (Application outside Great Britain) (Amended) Order 2009—generally any vessel recording and storing moving images of identifiable personnel while operating within the UKCS.
The same data protection requirements will apply to inshore diving and other offshore sites where a different type of diving platform is used.

2.0 CCTV LEGISLATION

The UK has extensive legislation governing the collection and use of CCTV footage in the workplace. This legislation aims to uphold a business's right to protect its interests and employees' fundamental human rights to privacy and dignity.

2.1 Data Protection Legislation, Guidance and Best Practice

Data protection law does not prevent employers from using closed-circuit television surveillance to monitor workers in private workplaces in the UK. Still, when monitoring involves collecting or storing data, it must be done in compliance with the law.
There are several pieces of legislation/guidance/best practice that cover images and audio recordings gained from CCTV use, such as:

- The Data Protection Act (and the General Data Protection Regulations (GDPR))
- The Information Commissioner's CoP, Monitoring at work
- The Human Rights Act
- The Freedom of Information Act
- BS7958 CCTV-Management and Operation-Code of Practice

2.2 The Data Protection Act & The General Data Protection Regulations

The Data Protection Act 2018 (DPA) was enacted on 1st March 2000. It has since been updated. The Data Protection Act expands upon the surveillance implications of Article 8 of the Human Rights Act and the General Data Protection Regulations.

The introduction of the Act and related legislation has far-reaching consequences for those who own, manage, or operate CCTV systems in the United Kingdom.

The Act covers the use of CCTV to monitor employees if it involves the "processing of information by automated means from which a living individual can be identified."

The DPA sets out duties for organisations and grants individuals rights, such as access to their personal data and the right to claim compensation if they suffer damage.

The GDPR clarifies that CCTV footage is personal information and sets out several specific requirements for its storage and processing. It also requires those who hold this data (i.e., employers) to disclose it in response to data subject access requests (DSARs) from employees.

In practical terms, it is personal information if individuals can be identified from CCTV images or from audio recordings.

Individuals whose images are recorded have the right to view them and receive a copy.

2.2.1 DPA and GDPR Obligations

The DPA and GDPR outline several obligations regarding the use of CCTV in the workplace, including:

- Informing anyone who might come under surveillance about the CCTV cameras, their purpose and any likely recipients of the footage
- Maintaining and making available a clear policy about the purpose and extent of the monitoring
- Supplying anyone who asks with all the footage in which they appear
- Ensuring that footage is secured from theft and accessible only by designated personnel
- Ensuring that footage is securely deleted after it is no longer needed
- Ensuring that any data transfer is done in compliance with the data transfer law.

2.2.2 Data Controllers and Data Processors

Personal data is crucial under GDPR because the law covers individuals, organisations, and companies that are either 'controllers' or 'processors'. Contractors with CCTV installed around or in their buildings will likely already have identified controllers and processors within their organisation.

- Controllers are the primary decision-makers (such as the diving contractor)—they exercise overall control over the purposes and means of processing personal data.
- Processors act solely on behalf of, and strictly in accordance with, the instructions of the relevant controller (such as the offshore management).

2.3 Information Commissioner's Code of Practice

When the Data Protection Act was enacted, the Information Commissioner issued a Code of Practice for CCTV systems. The Code of Practice "Monitoring at Work" guides how to avoid breaching the GDPR.

The Code of Practice contains 62 legally enforceable 'Standards' that must be met to ensure compliance with the data protection legislation. The Commissioner includes 30 points of good practice, which, together with the standards, are designed to build and maintain confidence in CCTV systems and ensure that they operate within the law.

The code is primarily aimed at organisations that routinely capture images of individuals on their CCTV systems and provides guidance on meeting the legal requirements of the legislation. Organisations may use alternative methods to meet these requirements, but risk breaking the law if they do nothing.

2.4 Human Rights Act

The Human Rights Act (HRA) is the most comprehensive and fundamental legislation governing the use of CCTV cameras. Article 8 of the HRA recognises the right to privacy, which applies to both public spaces and the workplace.

Overly intrusive CCTV surveillance without legitimate security or business purposes can breach this right. Employers who decide to monitor their employees must clearly specify the limits of the monitoring.

2.5 Freedom of Information Act

Individuals whose images are recorded have the right to view their images and to receive a copy of the photos.

3.0 MONITORING, RECORDING AND STORAGE REQUIREMENTS

3.1 Monitoring with CCTV Cameras

UK legislation clearly permits employers to use CCTV cameras in the workplace. Cameras may be installed wherever there is a legitimate business or security reason, provided their use is proportionate, necessary, and addresses a specific need that cannot be met by other means. Nevertheless, the use of CCTV in the workplace is subject to comprehensive privacy and data protection laws, which are designed to protect everyone's fundamental rights to privacy and dignity, regardless of their occupation or status.

Employers are not allowed to monitor workers everywhere (for example, not in the toilet). They could breach the Data Protection Act if they don't respect this.

3.1.1 Registered to Monitor

If a business uses CCTV, it must register with the Information Commissioner's Office and pay a data protection fee.

3.2 Impact Assessment

Before any monitoring or recording is introduced, an impact assessment must be carried out to determine what (if any) monitoring or recording is justified by its benefits.

The assessment should focus on targeting monitoring only at areas of particular risk, limiting it to places where people's expectations of privacy are low, employing video and audio monitoring separately, using it only when necessary rather than continuously, and evaluating whether less intrusive methods can achieve similar benefits and what adverse effects it may have on workers.

3.3 Informing Those Being Monitored

Employees should be informed about the monitoring, including where it is taking place and why. Recording anyone without their knowledge is illegal. You may record workplace conversations only if all individuals on-site are aware of the recording when it is active and understand why it is being done.

If monitoring is introduced to enforce specific rules and standards, the employer must ensure that workers are aware of and understand them.

Other individuals who might be captured by the monitoring, such as third-party contractors, visitors, and members of the public on the quayside, should also be informed that monitoring is in place and the reason for it.

A prominent sign can meet the notification requirements. This sign must state the organisation responsible for monitoring, when, where, and why the monitoring is being carried out, and who to contact about it (simply informing workers occasionally that they may be subject to monitoring is insufficient).

3.3.1 Policy Statement

The CCTV monitoring and recording scheme should have a written policy statement that clearly and comprehensively outlines the following:

- The identity of the owners and details of how they can be contacted
- What privacy the employees have
- The extent and purpose of any surveillance being conducted, either permanently or occasionally
- The rights and obligations that the company and employees have regarding CCTV use in the workplace

It is essential to use the appropriate camera equipment and locations that serve the purposes for which CCTV is employed and outlined in the policy.

3.4 Access to Stored Recording

Data protection laws do not specify in exhaustive detail who may view CCTV footage. It is for the CCTV operator to determine who is authorised to access the recordings. The DPA requires that access to the images be restricted to those who need them to fulfil the system's purpose.

When it comes to who can view CCTV footage at work, keeping this list as short as possible is not only a legal requirement but also, more often than not, good operational practice.

Anyone can request access to CCTV footage in which they appear. Employees may request to view footage of themselves but cannot access footage of others. In addition to granting access when necessary, the DPA requires employers to record all access to CCTV footage and to document all access requests, including the reasons for any denials.

The disclosure of images from the CCTV system must be managed in line with its purpose. For instance, if the system is set up to prevent accidents, it would be inappropriate to share images of identifiable individuals with the media or post them online.

If images or recordings are shared with a third party and include identifiable individuals who have not consented, the company should be aware of the potential scope of any claim.

The method for sharing images should be secure to ensure they are viewed only by the intended recipient.

Identify who the data controller and data processor are: diving contractors, vessel operators, or employers of personnel.

4.0 MONITORING AND RECORDING ON A DIVING SUPPORT VESSEL

Several areas on board diving support vessels are subject to voice recording, visual monitoring, or both. International and national legislation, best practices, or local requirements determine the reasons for monitoring these areas.

Areas that are routinely monitored and recorded are:

- Bridge – Audio recorded continuously
- Gangway – Monitored when alongside
- Deck –Constantly monitored and sometimes recorded moving images
- Diving-During diving operations:
    - Diving Bell – Continuously monitored and recorded audio and moving images
    - Dive Control – Audibly recorded during diving operations
    - Saturation System – Continuously monitored and sometimes recorded audio and moving images
    - Divers – Monitored and recorded continuously moving images and continuously recorded audio

4.1 The Bridge

The vessel's bridge records various vessel data in accordance with the International Maritime Organisation's resolution. Data such as:

- Radio traffic
- Radar
- Echo sounders
- Vessel speed and direction
- Wind speed and direction
- Bridge audio (up to 12 microphones)
- CCTV of engine rooms, etc

Typical VDR

The data is stored on the Voyage Data Recorder (VDR). The ship's length indicates its capacity and the type of monitoring. The VDR is very similar to an aircraft's 'black box'. It typically stores data for 30 days and either detaches from the vessel or can be retrieved by an ROV.

Although personnel are recorded on the bridge 24 hours a day, which inevitably includes 'private' conversations, this is not a concern. The recordings are made to investigate an accident.
The Maritime Accident Investigation Board is the only organisation permitted to access the data. Under maritime guidance, the Maritime Coast Guard Agency audits and tests the VDR annually.

4.2 Gangway Area

When a vessel is alongside, the gangway area is monitored by CCTV in accordance with the International Ship and Port Security (ISPS) requirements. A ship is audited and certified to meet this requirement.

4.3 Working Deck Area

The ship's working deck areas are remotely monitored, allowing the bridge crew and dive supervisors to observe deck operations, cranes, lifeboats, and upper workstations. They are usually not recorded unless connected to a 'black box.'

4.4 Diving Operations

4.4.1 Recording of Diving Operation Communications

UK regulations, international guidance, codes of practice, and company policies require that communication be recorded during diving operations. All these standards require the recording of voice or audio communication between the diver and the supervisor; however, NORSOK and IMO also require **video** recording.

1. Commercial Diving Projects Offshore-Diving at Work ACoP L103, *All divers in the water require a communication system that allows direct voice contact with the supervisor….. All such communications should be recorded.*

2. IMCA
   - IMCA D014 International Code of Practice for Offshore Diving. *All divers in the water will need a communication system…….All such communications will need to be recorded…..*
   - IMCA D22: *Record all voice communications starting with the pre-dive checks.*
   - IMCA D22: *All voice communications with the diver need to be recorded*

3. NORSOK U100 Manned Underwater Operations
   - *Recordings during operations. Communication with divers should be recorded.*
   - *Recordings of video and communication with the diver in water/bell/basket/wet bell/habitat shall be made.*

4. IMO International Code Of Safety for Diving Operations
   - *Communications between the dive control, the diving bell or wet bell, the standby diver and the divers in the water should be recorded (audio and video) and retained for a minimum of 24 hours after the dive is completed*

4.4.2 Retention of Diving Operation Communication Recordings

The same regulations, international guidance, codes of practice, and company policies that require recording communications during diving operations also specify a minimum retention period for voice recordings. None of these standards specify a maximum retention period or the security requirements for recorded material.

1. Commercial Diving Projects Offshore-Diving at Work ACoP L103. *……the recording is kept until 48 hours after the diver has returned to the surface or saturation living system*

2. IMCA
   - IMCA D014 International Code of Practice for Offshore Diving*…recommended that recordings be kept for 24 hours*
   - IMCA D22. *The recording needs to be kept until it is clear that there were no problems during or following the dive. It is recommended that recordings be kept for at least 24 hours.*

3. NORSOK U100 Manned Underwater Operations
   - *… Recording from the last 48 hours shall be available*
   - *Any recorded dive data and communication shall be stored in a safe and easily retrievable manner*
   - *A diver in the water shall be monitored by an ROV or a second diver's camera. Video recordings shall be kept for at least 24 h*

4. IMO International Code Of Safety for Diving Operations
   - *Communications between dive control, the diving bell or wet bell, the standby diver and the divers in the water should be recorded (audio and video) and retained for a minimum of 24 hours after the dive is completed*

4.4.2 Monitoring of Diving Operations

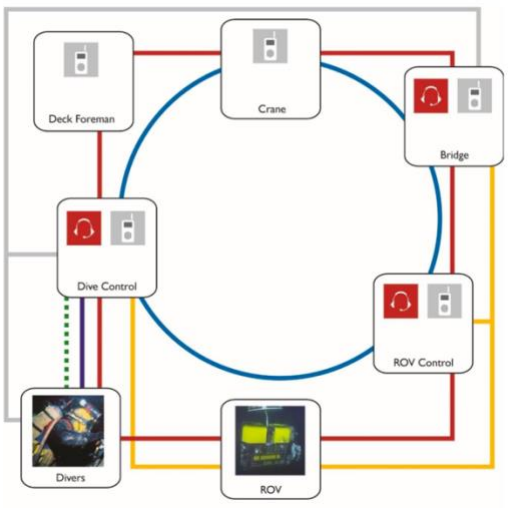
The same regulations, international guidance, codes of practice, and company policies that require communications during diving operations to be recorded also require visual monitoring of divers in chambers and diving bells.

1. Commercial Diving Projects Offshore-Diving at Work ACoP L103 ….. *able to see divers in the bell or the compression chamber during saturation operations*

1. NORSOK U100 Manned Underwater Operations.
   - *Visual monitoring. All chamber compartments, bells and habitats shall be equipped with a video monitoring system, enabling the surface crew to monitor the occupants and operation visually.*
   - *Diver monitoring system shall be provided for each Diver*
   - *All chamber compartments, bells and habitats shall be equipped with video monitoring system, enabling the surface support crew to visually monitor the occupants and operations*
   - *A diver in the water shall be monitored by an ROV or a second diver's camera. Video recordings shall be kept for at least 24 h*

2. DNV OS-E402202 *For saturation diving systems, suitable means (e.g. TV) shall be arranged for visual observation of the divers in the bell from the control stand for bells, and the divers in the chamber compartments for the control stand for the chambers.*

3. IMCA
   - IMCA D014 International Code of Practice for Offshore Diving. *During saturation or bell diving operations, supervisors must see the divers inside the bell or compression chamber. This will usually be achieved on the surface by direct viewing……., but a camera will be needed when the bell is underwater.*
   - IMCA CPD *Closed-circuit video is typically fitted to the helmets of divers to provide visual information to the surface of the progress of work done by the diver…. this is always used in conjunction with voice communication*
   - IMCA D46 Guidance on Operational Communications



Typical communication diagram

Note Divers CCTV

5.0 RECOMMENDATIONS

Contractors/Vessel Operators should comply with legislative obligations. The simplest way is to check the DPA and GDPR outlined obligations regarding the use of CCTV in the workplace, such as:

1. Check with the ICO guidance to establish if a fee is payable for data gathering
2. Carry out an Impact Assessment
3. Maintaining and making available a clear policy about the purpose and extent of the monitoring
4. Informing anyone who might come under surveillance about the CCTV cameras, their purpose and any likely recipients of the footage
5. Supplying anyone who asks with all the footage in which they appear
6. Ensuring that footage is secured from theft and accessible only by designated personnel
7. Ensuring that footage is securely deleted after it is no longer needed
8. Ensuring that any data transfer is done in compliance with the data transfer law.

6.0 CONSIDERATIONS FOR COMPLIANCE

This section, following on from 'Recommendations,' suggests ways that diving contractors and/or vessel operators might comply with legislative obligations.
For the data protection legislation, the employer is the 'data controller' and must adhere to the principles set out in the data protection legislation

6.1 Register with the ICO

The first step is to register with the Information Commissioner's Office and pay a data protection fee.

6.1.1 Data Protection Impact Assessment

Carry out an Impact Assessment (DPIA).

6.2 Policy

Diving contractors who use CCTV to monitor employees should have a corporate policy on recording, monitoring, and storing recordings, and should conduct their activities in a manner that respects employees' privacy.

Establish a CCTV and audio recordings policy, to include;

- Named personnel to safeguard recordings/images on board vessels
- Stated maximum retention time of all recordings
- State why recordings are being made and what outcome is expected
- The permanent deletion of images through secure methods
- State who's responsible for controlling recordings/pictures and making decisions on how they can be used.
    - Named personnel to safeguard recordings/images when transferred
    - Procedures for passing on images/recordings to a third party

6.3 Inform Personnel

6.3.1 Contract of Service

Diving contractors should consider the following:

- Including agreement of CCTV monitoring in personnel's contract
- Include posting/displaying the CCTV policy alongside other company policies
- Include CCTV in the vessel and dive site familiarisation
- Add a photo/moving image waiver in the contract of service

6.3.2 Signage

Companies that monitor and record in the workplace must inform people that they are in an area where CCTV surveillance is taking place.

The most effective way to do this is to use prominently placed signs at the entrance to the CCTV zone and to reinforce them with additional signs inside the area.

Clear and conspicuous signs are essential, especially when cameras are discreet or located where people might not expect surveillance. Signs should be larger and more frequent in areas where it is less obvious that CCTV monitoring is taking place. All monitored or recorded areas should display clear signs indicating this, including the bridge, deck chambers, dive control, gangway, quayside areas, and the diving bell.

In circumstances where audio recording is being carried out, such as the diving bell, dive control and bridge, any signs should state this explicitly and prominently. Signs should:

- Be clearly visible and readable
- Contain details of the operating organisation
- Be an appropriate size
- State the purpose for using CCTV

6.2.2 Explain Why CCTV Monitoring (and Recording) is Required

Divers and deck crew who are recorded should be given explicit notification of the monitoring being carried out, where it is being carried out, and the reasons for it; the scope of the monitoring must be limited to what is strictly necessary to deliver those benefits. The purpose of the CCTV system will be stated in the CCTV Policy, noting that very few regulations, international guidance, codes of practice, or standards require the recording and storage of moving images (IMO and NORSOK for diving).

Considerations Before Stating Justification

1. 'Diver safety' is usually cited as the reason for recording the diving bell internally and from divers' helmet-mounted cameras. If this is the justification, how does a diving contractor justify monitoring and recording only divers? Any recording is reactive, not preventative. All departments and personnel could potentially experience an accident or an undesired event. Why isn't everyone wearing a camera and being monitored, or is it only divers who have accidents?
2. Within the saturation system, cameras are positioned to monitor the occupants. Is it vital to continuously monitor the occupants? If so, the cameras should be fitted with night vision so that viewing can be conducted when occupants sleep or in blackout conditions.
3. In areas where people have heightened expectations of privacy, such as chambers, chamber wet pots during showering, and toilet areas, cameras should be used only in the most exceptional circumstances, when they are necessary to address serious concerns. A camera sited in a shower/toilet area is forbidden under the legislation.

6.4 Securing Recorded Data

DSVs have no dedicated 'data processor' for collected data. 'Anyone' could remove a black box recording or copy data from the digital hard drive using a memory stick or a recordable disk. Personnel wouldn't need access to the hard drive; anyone could use a mobile phone to record the monitor screen.

Any recorded data featuring an identifiable person (visual and/or audio) must be stored securely. Recorded images featuring identifiable people should be viewed in a restricted area, such as dive or sat control. The monitoring or viewing of images from areas where an individual expects privacy should be restricted to authorised persons.

Many websites display CCTV footage of identifiable divers at work, captured by deck cameras, ROVs, diver-mounted cameras, chamber cameras, and bell internal cameras. These CCTV images are owned by the 'data controller', the diving contractor. Footage containing identifiable individuals is 'personal data' and should be treated accordingly. However, employers can be held 'vicariously' liable for their employees' use of company data, such as CCTV recordings, when these appear on websites like "YouTube".

Example of dive control HDD and video distribution. There is no security to prevent unauthorised access

Image from black box with two identifiable individuals within the bell.

ROV recording of identifiable individual.

Considerations

1. All images must be protected with sufficient security to ensure they do not fall into the wrong hands. This should include technical, organisational and physical security. For example:
    - Is the ability to make copies of images restricted to appropriate staff?
    - Where copies of images are disclosed, how are they delivered to the recipient?
    - Are control rooms where images are stored and viewed securely?
    - Are employees trained in security procedures, and are there sanctions against staff who misuse CCTV images?
    - Are employees aware that they could commit a criminal offence if they misuse CCTV images?
2. Identify a 'data processor' on board the vessel and a 'data controller' onshore. For ships operated by the diving contractor, the data controller could be the senior dive technician or the OCM. The data controller should be the sole person authorised to access the HDD playback download function.
3. Diving contractors and vessel operators should review existing presentations featuring identifiable personnel and ensure that images or recordings do not cause damage or loss to those individuals.
4. Appropriate technical and organisational measures should be implemented to prevent unauthorised or unlawful processing of personal data (e.g., images or recordings posted on websites) and to guard against accidental loss or damage.
5. Appropriate technical and organisational measures should be taken to protect images and recordings when vessels leave the European Economic Area, unless the country or territory provides adequate safeguards for the rights and freedoms of data subjects in relation to the processing of personal data. For instance, when vessels plan to operate overseas, all images and recordings should be deleted.
6. All procedures and policies should be subject to internal and external audits.

6.5 Allowing Data Subject Access Requests

Respect should also be shown to the fact that anyone captured and recognisable on CCTV has the right to access that footage. People captured are entitled to make a Data Subject Access Request, which an employer must respond to within a month. The request can be made verbally or in writing. The process by which employees can request access to CCTV footage of themselves should be transparent and accessible to all, without unnecessary obstacles.

Considerations

1. Do the diving contractor and the vessel operator have an internal procedure for a data subject access request?
2. Do the diving contractor and the vessel operator have the capacity to supply moving images to individuals (without providing those individuals with images of others)?

6.6 Deleting Data

Data laws do not set fixed minimum or maximum retention periods for all systems or footage. Instead, retention must align with the organisation's reasons for recording images. The maximum retention period should be set out in the CCTV policy. The vessel's data controller must delete or erase material at the specified time and maintain a log of what was removed.

Considerations

1. Diving contractors and vessel operators should only retain images for a limited time to serve their recording purposes. Therefore, images should not be kept longer than the duration specified by the diving industry or regional requirements, usually 24 or 48 hours.

2. When operations are carried out on third parties or vessels of opportunity, the diving contractor should ensure that all recorded data is removed from the ship or deleted.

6.7 Accessing Digitally Stored Material

Establishing a clear basis for handling personal information is essential, and managing moving images of individuals is no exception. It is crucial to demonstrate who controls the images, including decisions on what to record, how the images should be used, and to whom they may be disclosed. The entity responsible for these decisions is the data controller and is legally accountable for compliance with the Data Protection Act. Diving contractors are therefore considered 'data controllers'.

Considerations

1. Diving contractors should develop (if not already in place) a restriction on the use of private still and moving-image devices, such as mobile phones and GoPro cameras. Images and recordings are uncontrolled and can be uploaded to social media within minutes.
2. Disclosure of images from the CCTV system must be controlled and aligned with the purpose for which the system was established. The CCTV Policy should state the reason for using images, and images should be used only for that purpose.
3. During certain diving operations, clients require a live video broadcast link to their onshore offices. However, they have no control over that data while it is being transmitted or once it reaches land.
4. If images or recordings are shared with a third party and include identifiable individuals who have not consented, the company should be aware of the potential scope of any claim.

7.0 CONCLUSION

Diving contractors record essential voice communications and moving images in accordance with established procedures. The diver wears a camera so the diving supervisor can give instructions. It is common sense to record both moving images and voice simultaneously. This practice has been in use long before data protection and human rights regulations were introduced.
IMO and NORSOK both require video recording.
CCTV surveillance at work is a relatively new area with potential risks for employers. They must balance the risk of liability for misuse of company facilities with respect for their employees' privacy and human rights.
It is now possible for an offshore accident, injury, or fatality to be posted on an internet site before the next of kin are informed.