

# Observation Report:

## CCTV MONITORING & RECORDING

of

## OFFSHORE DIVING OPERATIONS



By  
Chris Hodge  
[Updated June 2024]

### Disclaimer

The author is not aware of any inaccuracy or omission from this document. No responsibility is accepted by the author or any person or company concerned with furnishing information or data used herein, for the accuracy of any information or advice given in or any omission from this document, nor for any consequences whatsoever resulting directly or indirectly from reliance on or adoption of this document, even if there was a failure to exercise reasonable care on the part of the author or any person or company as aforesaid.

The recommendations and conclusions of this report are the author's personal view. They do not necessarily reflect any specific company policy. In this complex area of health and safety, the issues raised are indicative rather than exhaustive. Readers will judge the relevance of recommendations to their particular situation.

---

**TABLE OF CONTENTS**

<b>1.0 INTRODUCTION .....</b>	<b>4</b>
1.1 Summary.....	4
1.2 Limitation.....	4
1.3 Objective.....	5
1.4 Aims.....	5
1.5 Scope.....	5
<b>2.0 CCTV LEGISLATION .....</b>	<b>5</b>
2.1 Data Protection Legislation, Guidance and Best Practice .....	5
2.2 The Data Protection Act & The General Data Protection Regulations .....	6
2.2.1 DPA and GDPR Obligations .....	6
2.2.2 Data Controllers and Data Processors.....	6
2.3 Information Commissioner’s Code of Practice .....	7
2.4 Human Rights Act.....	7
2.5 Freedom of Information Act.....	7
<b>3.0 MONITORING, RECORDING AND STORAGE REQUIREMENTS .....</b>	<b>8</b>
3.1 Monitoring with CCTV Cameras .....	8
3.1.1 Registered to Monitor.....	8
3.2 Impact Assessment.....	8
3.3 Informing Those Being Monitored .....	8
3.3.1 Policy Statement.....	9
3.4 Access to Stored Recording.....	9
<b>4.0 MONITORING AND RECORDING ON A DIVING SUPPORT VESSEL.....</b>	<b>10</b>
4.1 The Bridge .....	10
4.2 Gangway Area.....	11
4.3 Working Deck Area.....	11
4.4 Diving Operations.....	11
4.4.1 Recording of Diving Operation Communications.....	11
4.4.2 Monitoring of Diving Operations.....	12
4.4.3 Retention of Diving Operation Communication Recordings .....	12
<b>5.0 RECOMMENDATIONS .....</b>	<b>14</b>
<b>6.0 CONSIDERATIONS FOR COMPLIANCE.....</b>	<b>14</b>
6.1 Register with the ICO.....	14
6.1.1 Data Protection Impact Assessment .....	14
6.2 Policy.....	14
6.3 Inform Personnel.....	15
6.3.1 Contract of Service.....	15
6.3.2 Signage.....	15
6.2.2 Explain Why CCTV Monitoring (and Recording) is Required .....	15
6.4 Securing Recorded Data .....	16
6.5 Allowing Data Subject Access Requests .....	17
6.6 Deleting Data.....	18
6.7 Accessing Digitally Stored Material.....	18
<b>7.0 CONCLUSION .....</b>	<b>18</b>

### 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 4, 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

### 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 Konkurransesepisjon (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, detecting, recognising and identification. At offshore worksites, it is usually 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 during diving is captured and stored in different formats, usually 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, it is classed as personal data and must be treated as such.

The Data Protection Act is the law in the UK 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 kept on both manual and electronic records.

Using CCTV to monitor employees' actions has potential implications for 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 office onshore; however, the same care needs to be taken regarding CCTV during diving and offshore worksites. More control must be given to CCTV recordings obtained from diving (and deck) operations. 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, first issued in 2009, primarily concerns CCTV use during offshore diving projects. Since then, UK regulations regarding CCTV monitoring, recording, storage, and use of personal data have significantly changed. This report has tried to capture those changes; however, data protection law is a specialised field outside the author's field of 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 the use of CCTV during offshore diving projects. It provides guidance to ensure the company adopts the correct standard operating closed-circuit television cameras, monitors, and recordings.

The report offers an overview of the legal responsibility of any recordings/images. It establishes who controls them, to whom they may be disclosed, and who is allowed access. Lastly, it assists managers in collecting, maintaining, and storing personal recorded data on board a ship by legislation.

### 1.4 Aims

The aims of this report are:

- ◆ Highlight the methods used offshore to capture images/recordings and provide good practice and advice for those responsible for operating images/recordings gained from CCTV 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 regarding how CCTV footage can be gathered and used 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 monitoring workers with closed-circuit television surveillance in private workplaces in the UK. Still, where monitoring involves collecting or storing data, it has to be done in a way that complies 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 Commission'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.

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

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

The DPA creates obligations for organisations and gives individuals rights, such as access to their details and claims compensation if they suffer damage.

The GDPR clarifies that CCTV footage is personal information and includes several specific requirements regarding how personal information is stored and processed. It also requires those who hold this data (i.e. employers) to disclose it based on data subject access requests (DSAR) from employees.

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

Individuals whose images are recorded have a right to view them and be provided with 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 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 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 on behalf of, and only on 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 provisions of 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 equipment and recommends how to meet 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 broadest and most fundamental piece of legislation governing the use of CCTV cameras. Article 8 of the HRA outlines a person's right to privacy, which extends to 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 state the limits of the monitoring.

### **2.5 Freedom of Information Act**

Individuals whose images are recorded have a right to view the pictures of them and be provided with a copy of the photos.

## 3.0 MONITORING, RECORDING AND STORAGE REQUIREMENTS

### 3.1 Monitoring with CCTV Cameras

UK legislation unambiguously allows employers to deploy CCTV cameras in the workplace. Cameras can be deployed wherever there is a legitimate business or security requirement as long as their deployment is proportionate and necessary and addresses a pressing need that other means cannot address. However, the use of CCTV in the workplace is governed by extensive privacy and data protection legislation, which aims to ensure that everyone's fundamental human rights to privacy and dignity are upheld, regardless of occupation and status.

Employers are not allowed to monitor workers everywhere (not in the toilet, for example). 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 its details 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 the benefits of that monitoring.

The assessment should consider targeting the monitoring only at the areas of particular risk, confining it to places where people's expectations of privacy would be low, using video and audio monitoring separately, operating it only when necessary rather than continuously, whether less intrusive methods can obtain comparable benefits and what adverse impact it may have on workers.

### 3.3 Informing Those Being Monitored

Employees should be notified that the monitoring is being carried out, where it is being done, and why it is being done. Recording anybody without telling them is illegal. You can only record workplace conversations by ensuring all individuals on site know the recording when it is active, and why it is in place.

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

Other people who may be captured by the monitoring, such as third-party contractors, visitors, and members of the public on the quayside, should also be made aware that such monitoring is in operation and why.

A prominent sign can satisfy the notification requirements. This sign must state the organisation responsible for the monitoring, when, where, and why it is being done, 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 should clearly and comprehensively outline 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 about CCTV use in the workplace

It is essential to use the correct camera equipment and locations, which achieve the purposes for which CCTV is being used and stated in the policy.

### 3.4 Access to Stored Recording

Data protection laws do not exhaustively list who can view CCTV footage. It is up to the CCTV operator to decide who is authorised to access the recordings. The DPA requires that access to the images be restricted only 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—it's also, more often than not, good operational practice.

Anyone can be offered access to CCTV footage in which they appear upon request. Employees can ask to see footage of themselves but cannot be granted access to CCTV footage of someone else. In addition to granting access when required, the DPA requires the employer to record all access to CCTV footage and document all access requests, along with the reasons for denials.

Disclosure of images from the CCTV system must be controlled and consistent with its purpose. For example, if the system is established to prevent accidents, it would not be appropriate to disclose images of identifiable individuals to the media or post them on the Internet.

Suppose images/recordings are disclosed to a third party and contain identifiable individuals, and those persons have not given their consent. In that case, the company should know the extent of any possible claim.

The method of disclosing images should be secure to ensure they are only seen by the intended recipient.

Establish 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 onboard diving support vessels record voice communication and/or are visually monitored and/or recorded. International legislation, national legislation, best practices, or local requirements govern 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 by the International Maritime Organisation 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



The data is stored on the Voyage Data Recorder (VDR). The length of the ship denotes the capacity and type of monitoring. The VDR is very similar to an aircraft's 'black box'. It stores the data typically for 30 days and either floats off the vessel or is ROV retrievable.

Although personnel are recorded 24 hours a day on the bridge, which inevitably will include 'private' conversations, this is not a concern. The reason for the recording is to investigate the accident.

The Maritime Accident Investigation Board is the only organisation that is allowed access to the data. Under maritime guidance, the Maritime Coastguard Agency audits and tests the VDR annually.

## 4.2 Gangway Area

When a vessel is alongside, the gangway area is recorded by CCTV as part of the International Ship and Port Security (ISPS) requirements. A ship is audited and certificated to achieve this requirement.

## 4.3 Working Deck Area

The ship's working deck areas are remotely monitored to allow the bridge crew and dive supervisors to view deck operations, cranes, lifeboats and upper workstations. They are not usually recorded unless wired into 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 communication to be recorded during diving operations. All of these standards require the recording of voice/audio communication between the diver and the supervisor; however, NORSOK and IMO require **video and voice** 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 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

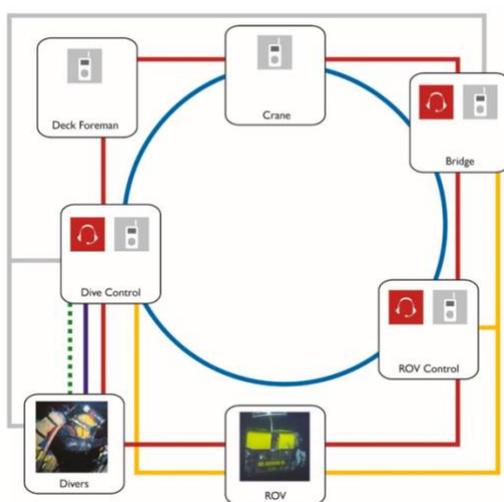
The same regulations, international guidance, codes of practice, and company policies that require recording communications during diving operations also provide a minimum retention period for voice recordings. None of these standards state a maximum retention period or security of recorded material.

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 that communications during diving operations be recorded also require visually monitoring 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 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 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 principles set out in data protection legislation

### 6.1 Register with the ICO

The first step is registering with the Information Commissioner's Office and paying 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 conduct their activities concerning the privacy of their employees.

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 being carried out.

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

Clear and prominent signs are vital, especially when the cameras are very discreet or in locations where people might not expect to be under surveillance. As a general rule, signs should be more prominent and frequent where it would otherwise be less obvious to people that they are on CCTV. All areas being recorded/monitored should display prominent signs conveying this information. (Bridge, deck chambers, dive control, gangway and quayside areas and 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 that the monitoring is being carried out, where it is being done, and the reasons why it is being done; 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, remembering that no regulations, international guidance, codes of practice, or standards require the recording and storage of moving images.

#### 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 all personnel could potentially have an accident or 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 set up to view the occupants. Is it vital to monitor the occupants continuously? 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 a heightened expectation of privacy, such as chambers and chamber wet pots during showering and toilet areas, cameras should only be used in the most exceptional circumstances where it is necessary to deal with 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 with an identifiable person (visual and/or audio) collected must be stored securely. Recorded images with 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.

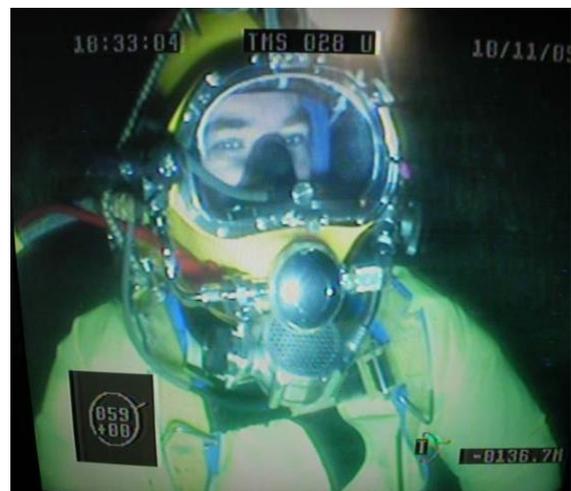
Internet sites have many CCTV images of identifiable divers at work, taken from deck cameras, ROV, diver-mounted cameras, chamber cameras and bell internal cameras. The CCTV images belong to the 'data controller', the diving contractor. These images containing identifiable individuals are 'personal data' and should have been treated as such. Employers can, however, be held 'vicariously' liable for the actions of their employees when they use company data such as CCTV recordings that appear on internet sites such as "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 by 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 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 OCM. The data controller should be the only person accessing the HDD play-back download function.
3. Diving contractors and vessel operators should review existing presentations for identifiable personnel and ensure images/recordings could not cause 'damage or losses to that individual.
4. Appropriate technical and organisational measures should be taken against the unauthorised or unlawful processing of personal data (e.g., images/recordings posted on internet sites) and against accidental loss.
5. Appropriate technical and organisational measures should be taken to safeguard images and recordings when vessels leave the European Economic Area unless that country or territory ensures adequate protection for the rights and freedoms of data subjects regarding the processing of personal data. For example, when vessels intend to work overseas, all images and recordings should be deleted.
6. Any procedure and policy should be subject to internal and external audit.

## 6.5 Allowing Data Subject Access Requests

Regard should also be given to the fact that anyone who is captured and is recognisable on CCTV will have a right to access that footage. Persons captured are entitled to make a Data Subject Access Request, which an employer has to respond to within a month. The request can be verbal or in writing. The procedure through which employees can request access to CCTV footage of themselves should be transparent and available to everyone without any unnecessary hurdles.

## Considerations

1. Does the diving contractor and the vessel operator have an internal procedure for a data subject access request?
2. Does 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 don't prescribe specific minimum or maximum retention periods for all systems or footage. Instead, retention should reflect the organisation's purposes for recording images. The maximum retention period should be stated in the CCTV policy. The vessel's data controller should delete/erase material at the indicated period and log what was deleted.

### Considerations

1. Diving contractors and vessel operators should only keep images for a short time to meet their purposes for recording them. Therefore, images should not be kept longer than the diving industry's stated duration or regional requirements, typically 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 handling moving images relating to individuals is no different. It is vital to prove who controls the images, for example, deciding what is to be recorded, how the photos should be used and to whom they may be disclosed. The body which makes these decisions is called the data controller and is legally responsible for compliance with the Data Protection Act. Diving contractors are, therefore, 'data controllers'.

### Considerations

1. Diving contractors should develop (if not already in place) a restriction on using private still and moving image devices such as mobile phones. Images and recordings are uncontrolled and can be freely uploaded to social media within minutes.
2. Disclosure of images from the CCTV system must be controlled and consistent with the purpose for which the system was established. The CCTV Policy should state the reason, and images should only be used for that purpose.
3. During some 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 is ashore.
4. Suppose images/recordings are disclosed to a third party and contain identifiable individuals, and those persons have not given their consent. In that case, the company should know the extent of any possible claim.

## 7.0 CONCLUSION

Diving contractors record the required voice communications and moving images through custom and practice. The diver wears a camera so the diving supervisor can give directions. It is common sense to capture the moving pictures and voice simultaneously. This practice was used long before data protection and human rights were in force.

IMO and NORSOK both require video recording.

CCTV surveillance at work is a relatively new field with potential pitfalls for employers. They must walk a fine line between possible liability for abuse of company facilities on the one hand and their employees' privacy and human rights on the other.

It is now possible to have an offshore accident/injury/fatality posted on an internet site before next of kin is informed.